CYBERSPACE:

MALEVOLENT ACTORS, CRIMINAL OPPORTUNITIES, AND STRATEGIC COMPETITION

Phil Williams and Dighton Fiddner, EDS.

UNITED STATES ARMY WAR COLLEGE PRESS
Carlisle Barracks, PA
STRENGTH and WISDOM

The United States Army War College

The United States Army War College educates and develops leaders for service at the strategic level while advancing knowledge in the global application of Landpower.

The purpose of the United States Army War College is to produce graduates who are skilled critical thinkers and complex problem solvers. Concurrently, it is our duty to the U.S. Army to also act as a "think factory" for commanders and civilian leaders at the strategic level worldwide and routinely engage in discourse and debate concerning the role of ground forces in achieving national security objectives.

The Strategic Studies Institute publishes national security and strategic research and analysis to influence policy debate and bridge the gap between military and academia.

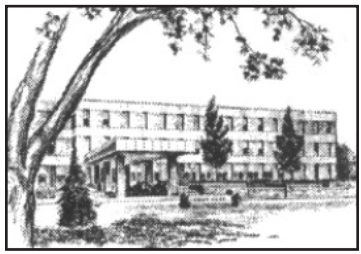
The Center for Strategic Leadership contributes to the education of world class senior leaders, develops expert knowledge, and provides solutions to strategic Army issues affecting the national security community.

The Peacekeeping and Stability Operations Institute provides subject matter expertise, technical review, and writing expertise to agencies that develop stability operations concepts and doctrines.

The School of Strategic Landpower develops strategic leaders by providing a strong foundation of wisdom grounded in mastery of the profession of arms, and by serving as a crucible for educating future leaders in the analysis, evaluation, and refinement of professional expertise in war, strategy, operations, national security, resource management, and responsible command.

The U.S. Army Heritage and Education Center acquires, conserves, and exhibits historical materials for use to support the U.S. Army, educate an international audience, and honor Soldiers—past and present.

STRATEGIC STUDIES INSTITUTE



The Strategic Studies Institute (SSI) is part of the U.S. Army War College and is the strategic-level study agent for issues related to national security and military strategy with emphasis on geostrategic analysis.

The mission of SSI is to use independent analysis to conduct strategic studies that develop policy recommendations on:

- Strategy, planning, and policy for joint and combined employment of military forces;
- Regional strategic appraisals;
- The nature of land warfare;
- Matters affecting the Army's future;
- The concepts, philosophy, and theory of strategy; and,
- Other issues of importance to the leadership of the Army.

Studies produced by civilian and military analysts concern topics having strategic implications for the Army, the Department of Defense, and the larger national security community.

In addition to its studies, SSI publishes special reports on topics of special or immediate interest. These include edited proceedings of conferences and topically oriented roundtables, expanded trip reports, and quick-reaction responses to senior Army leaders.

The Institute provides a valuable analytical capability within the Army to address strategic and other issues in support of Army participation in national security policy formulation.

Strategic Studies Institute
and
U.S. Army War College Press

CYBERSPACE: MALEVOLENT ACTORS, CRIMINAL OPPORTUNITIES, AND STRATEGIC COMPETITION

Phil Williams
Dighton Fiddner
Editors

August 2016

*****

Comments pertaining to this report are invited and should be forwarded to: Director, Strategic Studies Institute and U.S. Army War College Press, U.S. Army War College, 47 Ashburn Drive, Carlisle, PA 17013-5010.

*****

*****

*****

At the end of October 2012, a few days after Hurricane Sandy hit the East coast of the United States, the Ridgway Center for International Security Studies, the University of Pittsburgh, hosted a conference funded by the Strategic Studies Institute (SSI), U.S. Army War College, on Malevolence in Cyberspace.

The editors of the volume would like to express their appreciation to all those at SSI who facilitated the conference. Particular thanks go to Professor Douglas Lovelace, SSI Director, Dr. John Deni, and Lieutenant Colonel John Colwell for their

invaluable assistance, support, and participation. At the Ridgway Center, Beverly Brizzi handled the logistics and organizational arrangements with her usual flair and consummate skill.

After a long gestation, the presentations given at that conference, supplemented by some additional papers designed to fill certain gaps, have resulted in the current volume. This has been a long process, and the editors greatly appreciate the patience of the contributors. A special thank you goes to Sandra Monteverde, the Ridgway Center administrator, who played an enormous and indispensable role in the process of preparing the manuscript, taking it from conception to implementation in her own inimitable way. She and the editors would also like to thank Steve Worman and Aaron Attridge for their assistance with critical editorial tasks.

Phil Williams would also like to thank his international security colleagues—Michael Kenney, Luke Condra, Ryan Grauer, Taylor Seybolt, and Dennis Gormley—as well as Dean John Keeler and successive Associate Deans, William Dunn and Martin Staniland, for their continued enthusiasm and support for Ridgway Center activities

Dighton Fiddner would like to thank, first, the IBM Center for The Business of Government for generously funding the foundational research that resulted in his chapter and the contributions to the introduction and conclusion in this volume. Secondly, he wishes to thank sincerely all the participants in the collaborative (research) roundtable discussions he has organized since 2007: Davis Bobrow, Graduate School of Public and International Affairs, University of Pittsburgh; David Chambers (Moderator), Department of Political Science, Indiana University of Pennsylvania; Michael Driscoll, Indiana University of Pennsylvania; Casey Dunlevy, formerly BAE Systems; Waleed Farag, Department of Computer Science, Indiana University of Pennsylvania; Michael Fowler, Roger Williams University/Naval War College; Steve Jackson, Department of Political Science, Indiana University of Pennsylvania; Benoît Morel, Engineering and Public Policy, and Physics, Carnegie Mellon University; Isaac Porche, RAND Corporation; and Phil Williams, University of Pittsburgh. A special debt of gratitude is owed to those involved since the beginning of the research process and first round table in October 2007.

ISBN 1-58487-726-X

CONTENTS

Foreword.....xiii

1. Introduction.....1
Phil Williams and Dighton Fiddner

Part I: Concepts and Trends in Cyberspace

2. Defining a Framework for Decision-Making in Cyberspace.....29
Dighton Fiddner

3. Emerging Trends in Cyberspace: Dimensions and Dilemmas.....53
Nazli Choucri

4. Technologies That Will Change Your World.....75
Rick Hutley

5. Big Data Challenges, Failed Cities, and the Rise of the New 'Net.....101
Jeff Boleng and Colin P. Clarke

Part II: Challenges and Threats in Cyberspace

6. Cyberterrorism in a Post-Stuxnet World.....131
Michael Kenney

7. China's Reconnaissance and System Sabotage Activities: Supporting Information Deterrence.....173
Timothy L. Thomas

8. Information Warfare A La Russe.....205
Stephen J. Blank

9. The Adaptive Nature of Crime: Co-opting the Internet.....273
Shawn C. Hoard, Jeffrey L. Carasiti, and *Edward J. Masten*

10. Digitally Armed and Dangerous: Humanitarian Intervention in the Wired World.....319
Ronald J. Deibert and *John Scott-Railton*

11. The Threat from Inside . . . Your Automobile....369
Isaac R. Porche III

Part III: Responding to Threats in Cyberspace

12. Reflections on Cyberdeterrence.....391
Martin Libicki

13. Framing Cyberwar and Cybersecurity: Compelling Metaphors and Dubious Policy Templates.....417
Davis B. Bobrow

14. Identifying the Real and Absolute Enemy.....457
Rob van Kranenburg

15. Could the United States Benefit from Cyber-Arms-Control Agreements?.....477
Benoît Morel

16. Transnational Organized Crime and Digilantes in the Cybercommons.....513
Kelsey Ida

17. From Cybercrime to Cyberwar: Indicators and Warnings.....545
Timothy J. Shimeall

18. Crisis Management in Cyberspace and in a "Cybered" World.....571
Phil Williams

19. Cybered Ways of Warfare: The Emergent Spectrum of Democratized Predation and the Future Cyber-Westphalia Interstate Topology.....603
Chris C. Demchak

20. Conclusion 641
Dighton Fiddner

About the Contributors.....661

FOREWORD

The emergence and evolution of cyberspace has contributed to globalization, the creation of a new global commons, the rapid spread of knowledge and ideas, the development of global markets for local products, and the empowerment of individuals and small groups. Yet, cyberspace creates new opportunities for criminality, provides new avenues for terrorist recruitment, and adds a new playing field within which geopolitical rivalry among great and not so great powers plays itself out. Dependence by societies on cyberspace also creates new vulnerabilities. Cyberspace has brought new potential and promise—yet simultaneously it has also become a domain in which malevolent actors pursue selfish interests, spy, steal, extort, bully, and stalk.

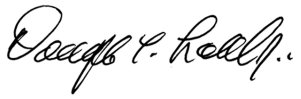
The problems are intensified by the fact that although cyberspace has become a ubiquitous feature of modern life, it is poorly understood. One approach often adopted by many members of the national security community is to treat it as a fifth strategic domain, joining land, sea, air, and space. Yet, cyberspace also permeates these other domains, and indeed, has permeated society as a whole. Perhaps one of the most significant features of cyberspace, however, is that it is becoming a risky place for the entire spectrum of users: nation-states, non-governmental and transnational organizations, commercial enterprises, and individuals. Yet it is also a space of opportunities—for benevolent, neutral, and malevolent actors.

It is against this background, that the Ridgway Center for International Security Studies, the University of Pittsburgh, and the Strategic Studies Institute

(SSI) of the U.S. Army War College (USAWC) held a conference entitled "Cyberspace: Malevolent Actors, Criminal Opportunities, and Strategic Competition." This volume contains the revised papers from that conference, along with several additional chapters that were commissioned after the conference. Accordingly, this volume has three parts: the first focuses on cyberspace itself; the second on some of the major forms of malevolence or threats that have become one of its defining characteristics; and the third on possible responses to these threats. Each section focuses on conceptual and analytic issues as well as the implications for policy and strategy.

The following chapters raise major and enduring questions about the conceptual and analytic challenges posed by the unique nature of cyberspace; differences between cyberthreats and more traditional challenges to national security; the range of possible responses to cyberthreats, ranging from the development of codes of conduct in cyberspace to strategies of deterrence and denial, and even the development of offensive cyberwar capabilities; and the relevance of traditional concepts such as crisis management and escalation to potential confrontations in cyberspace. This volume is designed to inform and provoke, as well as assist civilian and military national security, commerce, public sector, and academic decision-makers in understanding the sheer complexity and dynamism of cyberspace itself. Moreover, the authors identify and assess the challenges and threats to security that can arise in cyberspace because of its unique nature. In the final section, the authors discuss a variety of responses, with some suggesting that the most favored options being pursued by the United States are poorly conceived and ill-suited to the tasks at hand. The

intent is to provide food for thought to decision-makers as they confront this "new" medium and respond to its challenges and opportunities.



DOUGLAS C. LOVELACE, JR.
Director
Strategic Studies Institute and
U.S. Army War College Press

CHAPTER 1

INTRODUCTION

Phil Williams
Dighton Fiddner

In a highly prescient analysis written just prior to the end of the Cold War, James Rosenau argued that we were moving from a world of dichotomies to a world of paradoxes, from a world where something was either A or B to a world where A and B coexist and interact, albeit often uneasily.[1] Cyberspace is an excellent example of this world of paradoxes and complexity. The emergence and evolution of cyberspace have been an enormously positive force, contributing to globalization, the creation of a new global commons, the rapid spread of knowledge and ideas, the development of global markets for local products, and the empowerment of individuals and small groups.

Yet, cyberspace also facilitates intensified government surveillance of its citizens, creates new opportunities for criminality, provides new avenues for terrorist recruitment, and adds a new playing field within which geopolitical rivalry among great and not-so-great powers plays itself out. Dependence of societies on cyberspace also creates new vulnerabilities, which can be exploited by those with few scruples to inhibit their behavior. Indeed, at the same time that cyberspace has brought new potential and promise to millions of people, it has also become a savage domain in which malevolent actors pursue selfish interests, spy, steal, extort, bully, and stalk. In short, cyberspace has become a high-risk venue and medium for the entire spectrum of users: nation states, nongovernmental

and transnational organizations, commercial enterprises, and individuals. Key attributes of cyberspace, such as the low cost of entry, ubiquity, and relative anonymity (with the high degree of impunity that results), provide unique opportunities for malevolent actors and actions. Many of the same characteristics that make cyberspace so attractive—access to encyclopedic knowledge, flourishing commerce, ease and speed of communications and transactions, and the capacity to act as a force multiplier—also make it highly vulnerable to disruption and exploitation.

What makes this all the more problematic is that cyberspace is constantly evolving and expanding in numbers of users, types of users, points of access, means of access, degrees of connectivity, and forms of connectivity. At the same time, governance mechanisms lag far behind. Consequently, it is important to examine more fully the nature of cyberspace, the kinds of threats that it brings, and the range of possible responses to these threats. Accordingly, this volume has three parts: The first focuses on cyberspace itself; the second on some of the major forms of malevolence or threats that have become one of its defining characteristics; and the third on possible responses to these threats. Each section centers on conceptual and analytic issues as well as on the implications for policy and strategy. As one ponders and explores the very nature of cyberspace and what makes it so unique and distinctive, for example, questions about the differences between cyberthreats and more traditional challenges to national security become inescapable. The same kinds of questions arise in relation to the range of possible responses to cyberthreats: how useful are codes of conduct in cyberspace as opposed to strategies of deterrence and denial, and even the

development of offensive and defensive cyberwar capabilities? In the same vein, what is the relevance of traditional concepts such as crisis management and escalation to potential confrontations in cyberspace? Is cybercrime simply an old crime in new bottles, or have some crimes become so pervasive and far-reaching that they are qualitatively different from anything that went before? Conversely, how useful and relevant are new concepts such as digilantism? While this volume seeks to provide answers to such questions, it also challenges some of the answers that have become fashionable or convenient. Its starting point, however, is the sheer complexity and dynamism of cyberspace itself.

CONCEPTS AND TRENDS IN CYBERSPACE

In Chapter 2, "Defining a Framework for Decision-making in Cyberspace," Dighton Fiddner describes the nature and structure of cyberspace and teases out some of the ramifications for security. Because decision-making and strategies for cyberspace transcend the technical realm and incorporate multiple conditions, the definition of cyberspace needs to include individuals, organizations, and interrelated physical and cognitive components that involve information collection, processing, dissemination, and action. As such, cyberspace brings together the cyber and physical spheres of activity. Threats that begin in cyberspace now can jeopardize any level of security (personal, collective, and national), and can lead to a wide range of possible response options in either the physical or cybersphere of interaction.

Fiddner also argues that cyberspace is first and foremost a strategic domain (a sphere of activity, con-

cern, or function) similar in some respects to the traditional land, air, sea, and space domains. If cyberspace is a fifth, separate, and independent strategic domain, however, it is structured and operates differently than the other four traditional domains. Moreover, cyberspace encompasses the other four strategic domains and, as such, can have a direct causal and catalytic effect on activity that occurs within them. The threat and/or response vectors in cyberspace could come from either the cyber or physical sphere. However, in addition to being a strategic domain, cyberspace shares the characteristics of both a dimension and instrument of national power.

Because cyberspace is man-made and already in place, government decision-makers must work within the existing cyberenvironment and understand both specific risks and threats within the cyberspace domain and its relationship to the broader strategic environment. Response management in cyberspace is not a narrow technical challenge, but also involves fundamental issues of politics, strategy, security, interstate relations, bargaining, and escalation dynamics and control.

What makes these challenges all the more formidable is the novelty of cyberspace. In her highly trenchant analysis found in Chapter 3, "Emerging Trends in Cyberspace: Dimensions and Dilemmas," Nazli Choucri highlights the ways in which international relations in the 21st century differ from the international relations environment in the 20th century and the importance of cyberspace in contributing to these changes. Not only does cyberspace provide an unlimited opportunity for power, but it also is a source of vulnerability that continues to create major disturbances in the traditional legacy system of the 20th century. In this connection,

Dr. Choucri highlights seven disconnects between traditional and familiar conditions and current realities. These disconnects are temporality, physicality, permeation, fluidity, participation, attribution, and accountability. The result, she suggests, is that old ways of visualizing the pursuit of political and/or economic power have been rendered passé, if not obsolete, by diffuse, decentralized, diverse, and different types of interactions. "Cybervenues are critical drivers of the on-going realignments and the means by which all actors . . . pursue their goals."[2]

Moreover, cyberspace adds an important element of complexity to a power calculus, which has shifted from a polar to a highly distributed structure characterized by asymmetries in power and capability, and the creation of new vulnerabilities and challenges for national security. Choucri goes on to describe those complexities by providing a comparison of the old and new realities and the emergent trends in cyberspace. In her view, policymakers now have to contend with new sources of vulnerability (cyberthreats) and new dimensions of national security (cybersecurity), coupled with uncertainty, fear, and threat from unknown sources (attribution problems). In addition, the empowerment of new actors—some with clear identities and others without—as well as the wide range of asymmetries, contribute to an environment with greater potential for malevolence.

One of the difficulties recognized by Choucri, but more fully elucidated by Rick Hutley in Chapter 4, "Technologies That Will Change Your World," is that cyberspace itself is constantly morphing and expanding as a result of a continuing exponential explosion of technology innovation. The remarkable growth of digital data, continued increases in bandwidth stor-

age capacity, and improvement of raw computing power have all had a profound impact on societies. In effect, technology has become so integrated into the contemporary world that life would become chaotic without it. Hutley also focuses on some of the more promising current and future technologies (3D printing, designer pharmaceuticals, continued miniaturization, augmented reality, and high fidelity) to provide a glimpse of the likely future environment. In his view, the march of innovation now allows us to know (almost) everything about (almost) everyone, (almost) instantaneously through the Internet of Things (the connection of everything to the Internet). Paradoxically, with these enhanced capabilities come enhanced risks to personal, corporate, and national security; the possibility for malevolent use from each emerging technology is as great as (if not greater than) the possibility for benevolence. As Hutley says, "While these technological innovations have brought us heretofore unimaginable capabilities and benefits, they have also exposed us to a whole new breed of threats."[3] These threats will not go away, because humankind no longer has the ability to survive without technology. In order to mitigate them, it is necessary to focus not on the security capabilities of any one piece of technology, but rather on the overall security **architecture** of a technology infrastructure. As he argues, a "cohesive, holistic architecture that addresses security as a foundational design element"[4] is essential. That argument is all the more relevant because of the kinds of threats that have emerged in cyberspace.

One of the surprises in all of this is that, in much of the developing world, technology is also having a profound impact. That impact is one of the themes in Jeff Boleng and Colin Clarke's Chapter 5, "Big Data

Challenges, Failed Cities, and the Rise of the New 'Net." Boleng and Clarke focus on growing urbanization, particularly the continued growth of slums in developing countries, and examine the impact on cyberspace through the development of what they term "the new net." The new net has emerged in large part through the proliferation of feature phones throughout large parts of the developing world. Noting that 5.9 billion Subscriber Identity Module (SIM) cards are registered to active users globally, the authors emphasize that even people who live in relative poverty value the connectivity and services mobile devices provide. The prevalence of feature phones rather than smartphones has contributed to the creation of a new type of information environment. Information generated and consumed on these mobile devices is largely composed of multilingual text jargon, voice, images, and video, especially 6-second vines. Nevertheless, the creation and sharing of information in this new environment is staggering. It is also disconcerting, not only because of the likelihood of failing cities, but also because U.S. military forces might have to engage in contingencies in a range of unstable and chaotic urban environments. The challenge of the new net is particularly formidable because of the demanding physical environment and the equally demanding information environment. As Boleng and Clarke note:

> [T]his new net does not resemble the Internet and World Wide Web that we are accustomed to operating our cyber operational and intelligence forces in. It creates new challenges of multi-lingual, multi-media content that is highly intermittent and transient in nature. We must be able to rapidly gather intelligence and apply automated means to add context and connections to this vast sea of largely non-textual data.[5]

In other words, cyberspace has had new forms as well as serious new challenges. Indeed, it is only a small step from the valued connectivity of the new net to considering more explicitly the forms of malevolence and threats to security that can arise from its connections. These threats are the subject of Part II of this volume.

CHALLENGES AND THREATS IN CYBERSPACE

In Chapter 6, the first of the chapters dealing with threats in cyberspace, Michael Kenney critically examines the prospects of cyberterrorism. He concludes that the threat is overhyped, not least because the concept of cyberterrorism remains poorly understood. Confusion over cyberterrorism stems, in part, from recent attempts to stretch the concept to include hacktivism and terrorists' use of the Internet to facilitate conventional terrorism. Although the United States and other countries have experienced thousands of cyberattacks in recent years, none has risen to the level of cyberterrorism. Consequently, Kenney argues, it is important to dial down the rhetoric on cyberterrorism. He does this very emphatically by explaining how cyberterrorism differs from cyberattacks, cyberwarfare, hacktivism, and terrorists' use of the Internet. The most immediate online threat from terrorists lies in their ability to exploit the Internet to raise funds, research targets, and recruit supporters rather than engage in cyberterrorism. The skill with which the Islamic State has used Twitter to spread its message, to mobilize support, and to flaunt its victories underlines the arguments presented in this chapter. As Kenney notes, cyberterrorism might well occur in the future, but at present, online crime, hacktivism, and cyberwarfare are more pressing virtual dangers.

In Chapter 7, "China's Reconnaissance and System Sabotage Activities: Supporting Information Deterrence," Timothy Thomas examines how and why the Chinese so aggressively probe and enter global networks. His chapter goes beyond simply describing the cyberactivities that China employs to gain an advantage in economics, business, military competition, and political bargaining, to elucidate the Chinese use of cyberactivities for truly strategic purposes. China's objective is to "win victory before the first battle" by mapping the opponent's digital "terrain."[6] Much of this behavior is driven by Chinese beliefs that the United States maintains hegemonic power over global cyberspace, that information superiority is a key component of national power, and, therefore, China is at a strategic disadvantage in any conflict with the United States. From this perspective, strategic digital reconnaissance is particularly important, because it provides the Chinese with knowledge of the digital landscape, or virtual *shi,* allowing more effective offensive and defensive activities if needed. Active offense (system sabotage) is the preferred strategy of the Chinese for winning a cyberconflict. This offense entails damaging or disrupting the adversary's material and technical foundations, thereby making it impossible for the adversary to adjust to problems on the battlefield. Strategic digital reconnaissance locates the critical nodes to be destroyed.

Chinese strategic writers also foresee much merit in "information deterrence" through cyber-reconnaissance and cybersabotage. Several Chinese strategic thinkers view "the information umbrella as more utilitarian than the nuclear umbrella." By controlling information, China would leave its opponent in the dark about what is going on, thereby rendering it "impos-

sible to turn war potential into actual capabilities for engaging in war."[7] Thomas also emphasizes that Chinese strategic thought does not foresee information deterrence acting alone, but as coordinated with nuclear deterrence, conventional deterrence, and space deterrence. Moreover, he postulates that the Chinese may even develop political, economic, or cultural information deterrence to provide a strategic advantage in future conflicts. His analysis in this chapter and elsewhere is an important guide to China's concepts about cyberconflict—thinking that is both highly innovative and integrates ideas about cyberspace with broader considerations concerning geopolitical competition, strategy, and conflict.

As Stephen Blank discusses in Chapter 8, "Information Warfare A La Russe," Russia also views actions and policies in cyberspace as part of a more comprehensive strategy. This strategy consists of cyberwar, economic sanctions, domestic and international public information campaigns, manipulation of youth organizations or gangs, and the penetration of key sectors of the economy and subversion of politicians. This strategy takes the place of large-scale military capabilities that are unavailable or simply not usable. The Russian experience in both Estonia and Georgia indicates that Moscow operationalized a strategic information war to achieve victory by paralyzing a target country's social infrastructure networks, i.e., what might be called its central nervous system.

Russia appears to have employed this strategic concept with attacks on the cyberinfrastructure of Estonia (one of the world's most "connected" governments and societies at the time), which jeopardized that state's ability to function, let alone retaliate in cyberspace.The attacks on Estonian socioeconomic and

political institutions were allegedly coordinated with organized crime structures like the Russian Business Network. This offensive was also combined with economic warfare, as well as attempts to incite domestic violence in Estonia and attack its embassy in Moscow through violent demonstrations orchestrated by *Nashi* (one of the "official" Russian youth organizations). In Blank's view, the cyberattacks appeared to have been long planned to disrupt the Estonian government and society, and to demonstrate the North Atlantic Treaty Organization's (NATO) inability to protect Estonia against this novel form of attack.

For the first time, Georgia seemed to combine warfare in cyberspace with more conventional forms of warfare in traditional military domains. Russia attacked Georgian command-and-control and weapons systems, while also launching information-psychological attacks against media and communications targets. The perpetrators of the cyberattacks were recruited through the Internet and social media, and they were aided by Russian organized crime, which provided botnets and other malware that were used in the first wave of attacks. The second wave of attacks seemed to be based—in a sophisticated way—on postings containing both cyberattack tools and lists of suggested targets for attack. Once Russian troops had established positions in Georgia, the attack list expanded to include many more governmental and news media websites, financial institutions, business groups, educational institutions, and a Georgian hacking forum to preclude any effective response to the Russian presence and induce uncertainty about what Moscow's forces might do. These attacks significantly degraded the Georgian government's ability to deal with the invasion by disrupting communications,

stopping many financial transactions, and causing widespread confusion. The clear objective of the cyberstrikes was to support and further the goals of the military operations. Beyond this, the cybercampaign was part of a larger information battle between the Russian media and the Georgian and Western media for control of the narrative. In sum, Blank's analysis of Russia, rather like Thomas's analysis of China, suggests that, in contrast to actual or potential adversaries, the United States has embraced a rather narrow technocratic approach to cyberspace and the ways it might be used as part of a geopolitical competition.

In addition to threats in cyberspace that emanate from geopolitical competition and the pursuit of power and security in the fifth domain, there are other forms of malevolence that are linked to the profit motive. Cybercrime has become pervasive, simultaneously exploiting, challenging, and eroding the use of cyberspace for commerce and business. Although there were early indicators of this in 1994 when a Russian criminal was able to electronically steal $10 million from Citibank, the situation began to change more fundamentally in the late-1990s. In a little-reported episode in August 2000, a few months after the "I Love You" virus infected thousands of computers worldwide, a variant of the virus was used to acquire information from banks.[8] Since then, as Shawn Hoard, Jeffrey Carasiti, and Edward Masten indicate in Chapter 9, cybercrime has exploded with criminal use of the Internet. Their analysis reveals how cyberspace has not only facilitated new ways of carrying out old crimes, but also has created criminal opportunities, including new methods of money laundering. The chapter contains a series of highly illuminating case studies that provide strong support for the notion that cybercrime has become a major threat in its own right.

A less obvious set of threats targets the nongovernmental organization community and humanitarian initiatives in crises and conflicts. As Ronald Deibert and John Scott-Railton point out in Chapter 10, "Digitally Armed and Dangerous: Humanitarian Intervention in the Wired World," social media has penetrated armed conflict just as it has penetrated most other aspects of life in a world in which cyberspace looms increasingly large. As they point out:

> humanitarian groups, aid organizations, and conflict prevention and peace-building bodies use tools and data sources like Ushahidi and other crowd-sourced maps to anticipate, predict, and respond to crises and organized violence.[9]

Indeed, there is enormous enthusiasm about the potential use of digital technologies to boost both conflict prevention and humanitarian relief. Reflecting this potential, the authors identify important milestones in the evolution of digital humanitarianism, describe key approaches and technologies, and suggest a trajectory of where the field is headed. Yet, they also recognize the potential downside, noting the growing "risks to digital humanitarianism . . . as armed protagonists increasingly become more adept at exploiting these technologies for malignant ends." In fact:

> nonstate actors—such as organized criminals, rebels, insurgents, and rioters—have proved as adept at exploiting digital technologies for their ends as have the governments that monitor them. Thus, the spread of digital technologies need not necessarily result in increased access to information, opportunities to better tailor humanitarian relief, or tools to employ in the struggle against authoritarian governments. Rather, increased access to ICTs offers new avenues for non-

> state actors to engage in escalated violence against citizens and the state as well as for state repression of opposition and insurgents.[10]

Protagonists in armed conflicts can pollute information streams and spread disinformation or they can set up honeypots or malicious websites to infiltrate social networks, and even locate and arrest or murder individuals and groups. Crowd-sourced data can be used to entrap people or identify protests and take action against protesters. Drawing from recent Citizen Lab research, this chapter outlines some of the ways that humanitarianism is at growing risk from unintended consequences of its embrace of digital technology. In other words, Chapter 10 provides a vivid example of how cyberspace can be used for malevolence and coercion just as easily as for benevolence and humanitarianism. Those who exploit technology can also be threatened by it and with it.

The same theme emerges in Chapter 11, contributed by Isaac Porche, which moves from sources of threats in cyberspace to potential targets that could be attacked through cyberspace. His central theme that automobiles have a cybersecurity risk is both compelling and disturbing. The vulnerabilities of automobiles stem from the abundance of software, computers, and networks that were initially designed for automobiles several decades ago and have become much more salient, important, and vulnerable since then. Onboard diagnostic connectors, wireless communication connections, and the interaction between the Internet and the vehicle all provide additional sources of vulnerability that could be used to disable a vehicle or to override the commands of the driver, with potentially disastrous consequences. Using some very plausible

scenarios, Porche highlights the extent of the risks involved not only in the automobiles themselves but also in the transportation infrastructure (traffic lights, for example), which is also susceptible to both degradation and manipulation. Moreover, like the vulnerabilities in cyberspace more generally, automobile-based vulnerabilities are likely to persist. Enhanced security standards, stronger federal motor vehicle regulations, and a new patching regimen by car owners will all be needed to help mitigate the risks. Until then, however, it is not hard to imagine a day when a portion of the American automobile fleet is taken over by nefarious actors. Even then, as smart cars and self-drive cars become more common, new vulnerabilities are also likely to arise. In sum, Porche identifies an important area of vulnerability that very few people think of, and that has clearly been given insufficient attention, despite its ubiquity. He also provides examples that suggest the danger is both clear and present.

RESPONDING TO THREATS IN CYBERSPACE

Having examined the challenges and threats in cyberspace, this volume considers a variety of responses, with the authors suggesting that some of the most favored options being pursued by the United States are poorly conceived and ultimately inadequate and ill-suited to the tasks at hand. In Chapter 12, "Reflections on Cyberspace," Martin Libicki considers the possibility of cyberdeterrence as a major option for the United States. Libicki had long argued that the "difficulties associated with attributing attacks meant that the threat of retaliation, and hence cyberdeterrence, could not be expected to play a strong role in defending the United States from cyberattack." He revisits the theme

of cyberdeterrence, focusing on four key issues: the possibility of attribution; consideration of whether or not deterrence can work to prevent "obnoxious" behavior in cyberspace and not just an attack; the way in which third parties view the credibility of attribution; and whether a comparison of attribution in cyberspace with attribution in real-world attacks should discourage a deterrence policy for a cyberattack.

In an analysis with a great deal of subtlety and nuance, Libicki notes that attribution of an attacker who actively wishes to "avoid blame offers different and far less promising attributes for attribution than a repeated persistent intrusion set whose aim is to exfiltrate large amounts of data." Consequently, "attribution against the kind of attack that would merit retaliation has not gotten significantly easier." He also suggests that it is difficult to deter lesser actions such as cyberespionage. As Libicki suggests, "It is difficult to eradicate a practice, regardless of how obnoxious, in which the winners gain more than the losers lose."[11] Libicki also casts doubt on the notion that a cyberattack should be treated as a *casus belli:*

> Retaliation may lead to counter-retaliation and a tit-for-tat cycle which may stay in cyberspace or not, . . . which gets to the core dilemma of any deterrence policy—worthwhile as long as it serves to reduce the odds that others will misbehave, but problematic if it has to be carried out, particularly against a country with the capability to strike back.[12]

In the final analysis, therefore, Libicki concludes that deterrence is still not a viable option against possible cyberattacks.

In Chapter 13, Davis Bobrow comes to a similar conclusion, albeit by a very different route. In Bobrow's

view, much of U.S. cyberpolicy has been driven by the experience of Pearl Harbor, HI, and subsequently, the development of nuclear strategy—what he calls "the odd couple" (TOC):

> Those two templates . . . already have been shaping general U.S. conceptions of cyberwar and cybersecurity as well as more specific choices about how to pursue them. The consequences (actual and perceived) have and will affect how the rest of the world chooses to treat cyberwar and cybersecurity.[13]

Bobrow challenges the wisdom of these dominant frames. He elucidates the considerations that make them appealing but casts doubt on both the historical accuracy and completeness of their prevailing construction, noting that the dominant nuclear strategy was supplemented by the reciprocal reassurance measures such as the hot line and arms control agreements. Bobrow compares this with cyberspace, where "the preconditions for giving a serious push to hedges involving self-restraint and multilateral mechanisms seem to be only embryonic and lagging far behind the evolution of threats."[14]

Perhaps most importantly, however, Bobrow emphasizes the dissimilarity between nuclear weapons and cybertechnologies, concluding that it is doubtful that "even an improved version of TOC illuminates more than it distorts coping with prospects for cyberwar and cybersecurity."[15] Yet these differences seem to have little impact on the odd couple framework as a guide to U.S. policy and strategy. The danger, as he notes, is that both Pearl Harbor and the nuclear frame:

> . . . will reinforce self-damaging policy illusions. Those will carry with them substantial direct economic

> and security costs associated with a cyber-arms-race marked by leapfrogging defense and offense measures and counter-measures. Directly and indirectly, those competitive patterns increasingly will undercut proclaimed U.S. goals of a tolerant and cooperative cyberworld marked by individual informational freedom and mutually beneficial, peaceful cross-border flows. They will further motivate others to modify or organize alternative international cyberinstitutions with different priorities than those of currently American controlled bodies.[16]

Rather like Bobrow, in Chapter 14, Rob van Kranenburg postulates that the existing models of thinking about security in cyberspace are not necessarily the most appropriate or useful. In contrast to Bobrow's focus on U.S. security policy, van Kranenburg argues broadly and philosophically that the emerging Internet of Things, with its "automated systems interacting in the physical world," is altering the very basis of society. It is also altering the way society has organized itself economically, politically, and in relation to security, etc. and, as a consequence, the "nature of power" itself. He makes a distinction between the "real" enemy who can "redefine all that you hold normal, dear, and take for granted" and the "absolute" enemy that is more threatening because one is unable "to change convictions, alliances, and opinions" or one's "ontologies: what you are, what you hold yourself to be, what you believe to be 'normal,' 'just,' 'fair'." The absolute enemy is difficult to confront, partly because there is "no clear definition of what a victory would mean—other than having things not happen," but most importantly because there is no context or markers "to make an informed choice about the kinds of weapons that could either be used for defense or offense."[17]

Van Kranenburg argues that this change in ontological perception requires a change in how one makes decisions about the emerging digital world—moving from "analog" cause and effect to decisions made by negotiating "a network of varied and widely diverging skill sets that allow for conflict inside the network." To do this, he advocates constructing a "new conceptual space" with "new notions of privacy, security, assets, risks, and threats, tailored to a reality of today, not a reality of yesterday or longer."

Moreover, this is an urgent task and whoever succeeds first will dominate:

> when it is time to act out of a deep knowledge that the current situation is untenable. Unfortunately, the analysis of the situation leaves different stakeholders with different timeframes.[18]

In Chapter 15, in a trenchant and often controversial analysis, Benoît Morel offers another critique of existing approaches to cyberspace. He also examines whether the United States should seek cyber-arms-control agreements at either a bilateral or multilateral level. Morel's answer is a clear no. In his view, there is no good framework for multilateral negotiations, while he argues that bilateral negotiations with China should also be avoided, primarily because the United States simply would be negotiating from a position of weakness. Indeed Morel is extremely critical of the political establishment, the policy community, and the national security community—particularly the military—in the United States for not adapting to the peculiar and novel demands of cybersecurity. Instead, he argues, the military has simply rehashed old concepts that applied in the real world but are not readily applicable in cyberspace.

Morel also emphasizes that the cyberthreat is a composite of very different threats and that:

> cybersecurity is not served in debates mixing up privacy, cybersabotage, cyberespionage and cybercrime. They are very different subjects calling for very different answers. Privacy should enter in that kind of debate as a binding constraint.[19]

Rather, like the earlier authors considering responses to threats and challenges in cyberspace, Morel argues that appropriate responses require a conceptual change and a real change in culture. As he notes, however:

> The adjustment to a new culture tends to be a slow and protracted process. If one compares the situation as it was a few years ago, there has been progress. By way of analogy, it is a bit like the grass growing. Progress is not immediately visible; it takes place only very slowly. This reflects the slow penetration of the 'culture' of cybersecurity in the U.S. government and military.[20]

Unfortunately, this process is as vital as it is slow and incremental.

Instead of focusing on government responses to malevolence in cyberspace, Kelsey Ida in Chapter 16, "Transnational Organized Crime and Digilantes in the Global Cybercommons," suggests that there might be bottom-up emergent responses, particularly to transnational organized crime and its digital and real-world activities. After examining how the digital age has revolutionized transnational organized crime by providing "a means of conducting profit-generating activities with greater efficiency and an extraterritorial capacity,"[21] Ida considers the role of the transnational public in efforts to curb transnational crime.

She highlights the unique features of cyberspace and argues that bottom-up regulation by digilantes is not far-fetched after all:

> In the absence of a legitimate state to govern the virtual world, agency arguably flows to those individuals that can best manipulate the virtual environment. This amounts to those individuals with high cyberknowledge (i.e., encryptions skills, coding skills, hacking skills, programming skills, etc.), or . . . 'smart power.'[22]

The two major examples considered are the "419 digilantes," who take steps to counter the "Nigerian Advance Fee" or "419" fraudsters, and "Anonymous," which has confronted the highly violent Mexican criminal organization, the "Zetas." The 419 fraudsters derived their name from the relevant Nigerian constitutional criminal code dealing with fraud. Although Ida acknowledges that there is a possibility that some digilantes might be seduced into using their skills to exploit the plethora of criminal opportunities in cyberspace, she suggests that social frameworks, values, and the traditional notion of the superhero, by and large, will work to prevent this.

The prevalence of cybercrime also provides the background against which Timothy Shimeall in Chapter 17, "From Cybercrime to Cyberwar: Indicators and Warnings," considers how to distinguish between different kinds of attacks in cyberspace and the ways certain groups might move from crime to war. Shimeall identifies a variety of behavioral shifts as groups of malicious actors transition from profit-oriented cybercrime activity to politically oriented cyberwar activity. These changes include those of motivation, aggression, methods, and impact. Each shift is discussed in depth, along with possible indicators related to that shift. While it is difficult to identify a transition in

activity from any single shift, in combination, a clear pattern may emerge. Using the shifts as a basis, indicators for each stage of attack are profiled. The attack stages are drawn from the "cyber-kill-chain model."[23] He concludes with discussions of the limitations of network-traffic analysis and strategies for dealing with these limitations. In addition to providing considerable technical details about the shifts, Shimeall begins the process of identifying those attacks that constitute acts of cyberwar.

These acts are the starting point for Chapter 18 by Phil Williams, which focuses on "Crisis Management in Cyberspace and in a 'Cybered' World." After a period of inattention during which crisis management appeared to be little more than a Cold War relic, Williams argues that the crisis in Ukraine, along with growing tensions in the Pacific, revelations about how close the Cuban Missile Crisis came to war, and the hundredth anniversary of the Sarajevo crisis that led to the First World War, have combined to place the possibility of great power crises back on the agenda. He suggests that there is an important distinction between crises that begin in cyberspace with a major cyberattack, and those that are precipitated by events in the real world but are played out in a world in which cyberspace is an additional and important strategic domain.

After identifying some of the characteristics of crises and the nature of crisis management, Williams names some of the major challenges likely to confront policymakers who have to manage a crisis in cyberspace. He considers how cybercrises might differ from traditional crises and looks at the particular problems likely to arise in several key areas: decision-making, communications, crisis bargaining, making sound intelligence assessments, and maintaining control over events. Drawing on both the work of Herbert Lin on

escalation in cyberspace and that of Forrest Morgan and his co-authors on escalation dynamics, Williams elucidates some of the dangers. He also looks at the problems of crises that begin with a traditional geo-political flashpoint, but that have to be managed in a context within which cyberspace looms very large. Finally, Williams provides a set of recommendations to enhance the capacity for crisis management both in cyberspace and in a cybered world.

The notion of a cybered crisis is an extension of the idea of cybered warfare developed by Chris Demchak, who provides the concluding chapter in this volume. In Chapter 19, "Cybered Ways of Warfare: The Emergent Spectrum of Democratized Predation and the Future Cyber-Westphalia Interstate Topology," Demchak provides a view of future cyber-conflict, given the "disequilibrium" of the interstate system. Weak international institutions for cybergovernance have produced a hypervirtual anarchic system in which individual self-interests reign supreme. As a consequence, "every major conflict among states will involve cyber means that seminally influence the outcome of the conflict"; what Demchak calls "cybered conflict."[24]

In Demchak's view:

> cyberspace has spread as a highly insecure, open 'substrate' under the world's major communities, with systemic characteristics democratizing anonymous predation globally and overwhelming established state and societal controls.[25]

In response to this situation:

> states and organized groups are now engaged in a transition era to sort out where the new societal and interstate controls on predatory behavior will be

placed and enforced in the slowly emerging future 'Cyber-Westphalia' interstate system.[26]

The institutions that are created during this transition "will strongly influence which states are robust or weak 'cyberpowers' when cyberspace's topology stabilizes." As for long-term outcomes at the end of this transition, Demchak identifies three major possibilities: (1) "a system of fractious atomized states with varying degrees of cyberpower and responsible behaviors;"[27] (2) a system dominated by the rise of an illiberal superpower and the decline of liberal globalization; and (3) a system of many various balancing responses dominated by new or renewed technologically integrated regional alliances of like-minded, like-structured, or like-threatened nations. Which of these scenarios becomes dominant will do much to determine the future of malevolence in cyberspace.

ENDNOTES - CHAPTER 1

1. James N Rosenau, *Turbulence in World Politics: A Theory of Change and Continuity,* Princeton, NJ: Princeton University Press, 1990.

2. Nazli Choucri, Chapter 3 in this volume.

3. Rick Hutley, Chapter 4 in this volume.

4. *Ibid.*

5. Jeff Boleng and Colin Clark, Chapter 5 in this volume.

6. Timothy L. Thomas, Chapter 7 in this volume.

7. *Ibid.*

8. Joe Wilcox, "New Strain of 'Love' Virus Steals Passwords," CNET News, August 17, 2000, available from *news.cnet.com/2100-1023-244593.html*.

9. Ronald Deibert and John Scott-Railton, Chapter 10 in this volume.

10. *Ibid*.

11. Martin Libicki, Chapter 12 in this volume.

12. *Ibid.*

13. Davis Bobrow, Chapter 13 in this volume.

14. *Ibid.*

15. *Ibid.*

16. *Ibid*.

17. Rob van Kranenburg, Chapter 14 in this volume.

18. *Ibid.*

19. Benoît Morel, Chapter 15 in this volume.

20. *Ibid.*

21. Kelsey Ida, Chapter 16 in this volume.

22. *Ibid.*

23. Timothy Shimeall, Chapter 17 in this volume.

24. Chris Demchak, Chapter 19 in this volume.

25. *Ibid.*

26. *Ibid.*

27. *Ibid.*

PART I

CONCEPTS AND TRENDS IN CYBERSPACE

CHAPTER 2

DEFINING A FRAMEWORK FOR DECISION-MAKING IN CYBERSPACE

Dighton Fiddner

INTRODUCTION

The author thanks the IBM Center for The Business of Government for generously funding the foundational research that produced this chapter. An earlier version of the chapter appeared as the report "Defining a Framework for Decision Making in Cyberspace" to the IBM Center for The Business of Government, and was presented at the CISS, Jagiellonian University Millennium Conference 2015: Interdisciplinary Approaches to Security in the Changing World, Krakow, Poland, June 18-20, 2015.

About the Research Project.

This report is intended to provide cyberspace decision-makers with a more comprehensive, clearer description of cyberspace, which they can use to manage and make decisions about cyberspace programs to improve the effectiveness of government in this critically important area. The report offers an assessment of and recommendations focused on the unique characteristics of cyberspace, which were initially designed without much focus on security or risk management. Improving the definition of cyberspace will improve the current understanding of how to address cyberissues strategically, as well as how, when, and what tools decision-makers should use to respond to cyberevents.

The Political Science Department at Indiana University of Pennsylvania (IUP) initiated this project with the support of the IBM Center for The Business of Government. The project brought together an interdisciplinary panel of experts in national security, international relations, U.S. foreign policy, information system network and security, public policy, and computer science. They were asked to apply their individual and collective expertise to develop an integrated understanding of strategic decision-making for cyberspace activities.

The panel of experts met in two collaborative roundtable meetings, during which participants deliberated about a series of questions to frame and inform the issue. The second roundtable's questions were derived from and informed by the findings of the first panel's deliberations. These meetings allowed the researchers to further the goal of defining, describing, and explaining problems that hinder successful management in cyberspace, now that cyberspace is an integral part of the security environment. Each roundtable was videotaped for reference, archival purposes, and possible future use as edited digital instructional material.

The report summarizes the roundtables and adds context based on the roundtable participants' experience and research into cyberspace. The following sections present:

- A general discussion of the need to define cyberspace as a tool to help the government manage cyberactivity more effectively, both directly and across traditional strategic domains of land, sea, air, and space.
- A taxonomy of the range of cyberthreats for which effective responses can be framed, using context created by the definition of cyberspace and determining the consideration of cyberspace as a separate strategic domain.

- A set of recommendations for the government to consider in deciding whether to adopt the proposed definition and then implement an effective framework that can help frame cyberspace management in a security context.

GOALS OF THE RESEARCH PROJECT

First, roundtable participants wrestled with the lack of an accepted definition of cyberspace. This lack stems, in part, from how the perspectives of "technologists" (the people who focus on the hardware that operates the systems) differs from those of "information scientists" (the people who focus on both information and software). Cyberspace decision-making and strategy transcend the technical realm and incorporate multiple conditions, as do other national and enterprise security issues, necessitating solutions that extend beyond a purely technical environment. Therefore, roundtable discussions addressed multiple dimensions of cyberspace, including individuals, organizations, and interrelated physical and cognitive components that involve information collection, processing, dissemination, and action.

The roundtables next addressed the notion of cyberspace as a strategic domain. Traditionally, strategic domains have been divided into four categories: land, air, sea, and space. The participants concluded that cyberspace is best defined as a separate and independent fifth strategic domain that is structured and operates differently from the other four traditional domains. However, participants also acknowledged that cyberspace encompasses the other four strategic domains and, as such, can have a direct causal and catalytic effect on activity that occurs within them. In addressing the impact of cyberspace for a government, decision-makers across all dimensions must

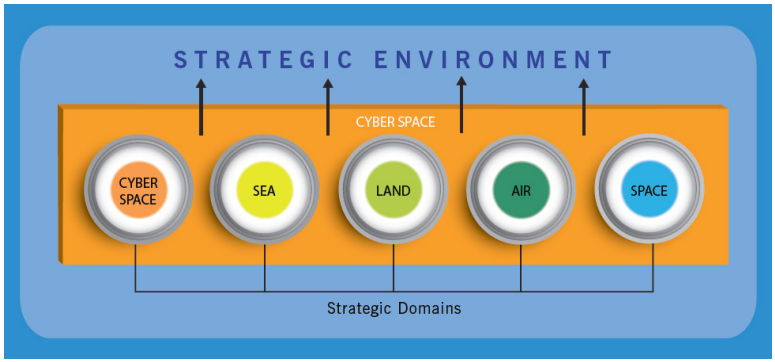
understand both specific risks and threats within the cyberspace domain and its relationship to the broader strategic environment.

In taking this approach to devising a definition for cyberspace, roundtable participants had to address the lack of a definition for "strategic domain." The researchers referred to a strategic domain as a sphere of activity, concern, or function.[1] Strategists traditionally have found that an activity, concern, or function could occur in four separate, independent domains (land, sea, air, and space). Based on the assessment that cyberspace provides a fifth domain in which an activity, concern, or function can occur, roundtable participants defined "cyberspace" as:

> A man-made global strategic domain, dimension of national power, and instrument of the dimension of national power within the information environment, consisting of the interdependent network of information technology infrastructures and resident data—including the Internet, telecommunications networks, computer systems, and embedded processors and controllers—for the production and use of information by individuals and organizations.[2]

UNDERSTANDING CYBERSPACE AS A STRATEGIC DOMAIN

Cyberspace, like the other four domains, can independently serve as the locus of activity, concern, or function, and each could trigger activity, concern, or function in the other domains. Figure 2-1 presents the five strategic domains.



NOTE: Cyberspace is a separate, independent domain that permeates the entire strategic environment and also encompasses the other strategic domains.

Figure 2-1. Strategic Domains.[3]

In addition, cyberspace as a strategic domain has three unique properties:

1. It has no physical boundary, which means cyberspace permeates the entire strategic environment;
2. It occupies the same space as the other four domains; and,
3. It can generate activity as a dimension and instrument of national power. This means that actions in cyberspace can:
    - Occur solely in the cyberspace domain
    - Move to one or more of the other traditional domains
    - Simultaneously affect activity in one or more of the other domains, either through human activity or automation.

Unlike the air, sea, land, or space strategic domains, cyberspace is not geographically constrained. Much like the space strategic domain, cyberspace is a global com-

mon good; no one country controls space, but instruments of national power can exist within the domain. In addition, unlike the other strategic domains, cyberspace simultaneously occupies the space of the other strategic domains. As a result, activity within cyberspace can have a direct causal and catalytic effect on activity in the other strategic domains. It is an **uber-strategic** domain that can involve the other four domains.

Cyberspace also brings together the cyber and physical spheres of activity. The threat vector and the response in cyberspace could come from either the cyber or physical sphere. This has tremendous implications, which influence how government manages and makes decisions involving cyberspace.

As mentioned earlier, the roundtables also found that cyberspace shares the characteristics of both a dimension and instrument of national power. As a **dimension** of national power, a nation can leverage cyberspace as it does any other strategic dimension, using it to persuade, entice, coerce, deter, or compel an entity to act in a certain fashion. As an **instrument** of national power, cyberspace includes key components, such as interdependent networks of information technology infrastructures and resident data, including the:

- Internet
- telecommunications networks
- computer systems, especially software,[4] and
- embedded processors and controllers.[5]

This conceptualization of cyberinstruments is analogous to examples of the other dimensions of national power displayed in Figure 2-2. This figure presents the four dimensions of national power and provides examples of each.

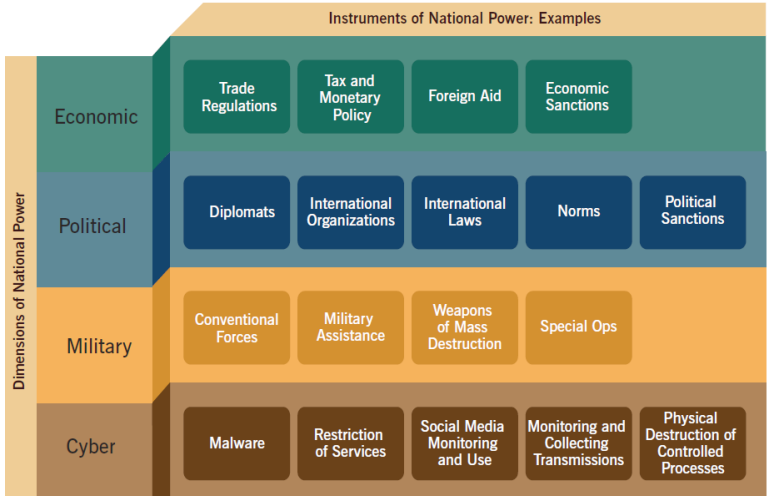


Figure 2-2. Dimensions and Instruments of National Power.[6]

Because cyberspace is man-made and already in place, government decision-makers must work within the existing cyberenvironment. This existing environment is of concern because certain properties or characteristics of cyberspace were deliberately designed without a specific focus on security or risk management. These properties include the network topography of cyberspace, which inherently introduces risk into cyberactivities. This risk reinforces the need for a commonly accepted framework that defines cyberspace so that risks can be addressed within a relevant context.

THREATS AND POTENTIAL RESPONSES IN CYBERSPACE'S DIFFERING SPHERES

Introduction.

The properties discussed in the previous section magnify the impact of cyberspace threats. Threats that begin in cyberspace now can jeopardize any level of security (personal, collective, or national), and can lead to a wide range of possible response options. In contrast, traditional security threats and responses emanate from the same sphere of interaction—for example, in the traditional physical sphere of interaction, a response would most likely have come from the same sphere from which the initial threat emanated.

Figure 2-3 includes horizontal rows that represent the sphere of interaction (cyber, physical, or merged cyber-physical), and vertical columns that show activity at differing levels of physical or economic security (individual, national, and global). The roundtable discussions inspired the framework shown in Figure 2-3. The framework is intended to describe threats in cyberspace, based on the context set out by the group's definition of that term as discussed in the previous section.

The following discussion addresses each component of the cyber-threat-and-response framework. The scenarios reinforce the need to develop a strategic context for managing activities in cyberspace—in which specific, general, and collateral impacts and their scope, as well as attribution, can vary widely and change rapidly, posing challenges for legitimate actions by government. Using the context delineated by the roundtables and described earlier in the report, and the recommendations presented in the next section, government can enhance its ability to make effective decisions about how best to address a wide range of cyberthreats.

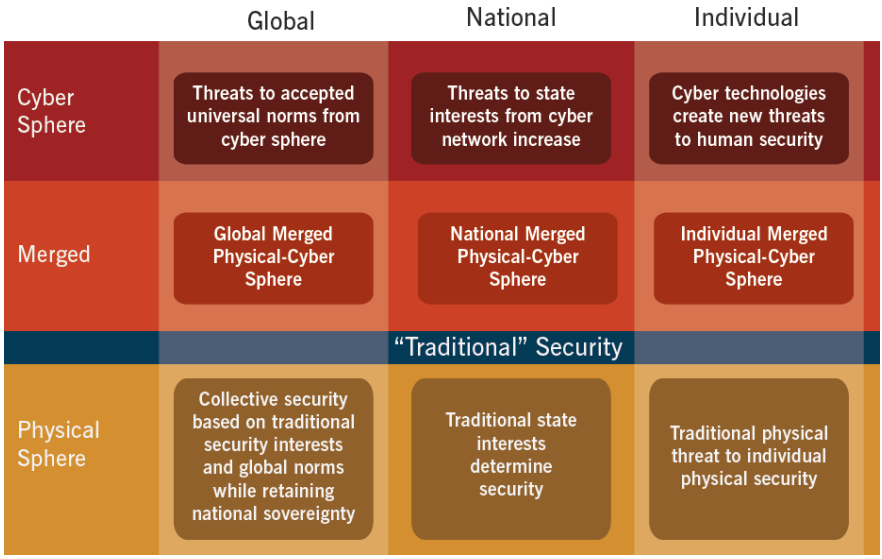


Figure 2-3. Threat Vectors.[7]

CYBERSPHERE OF INTERACTION

The initial threat vector involves cyberactivity in the cybersphere.

Global Cybersphere (Top Left Square).

A threat to cybersecurity could take the form of a risk to global cyberinfrastructure or a violation of globally accepted norms of content. Response to this threat in the cybersphere would usually be constrained to that sphere, which could consist of removing the links to offending websites. Additional responses, such as issuing a warning to remove harmful content from servers or shutting down services, could be implemented if the initial response(s) was not successful in deterring or stop-

ping the threat. This threat vector can also move to the physical sphere of interaction through some action (e.g., an unwarranted release of names of people—be they innocent bystanders or people who hold sensitive and undisclosed positions, thereby jeopardizing personal, organizational, or national security, or the security of other collective groups). In such scenarios, a response could still occur within the cybersphere of interaction; one example would be to degrade the perpetrator(s') cyberinfrastructure.

Nation-State Cybersphere (Top Center Square).

Threats in this sphere of interaction emanate from the cybersphere; the response also would occur primarily within the cybersphere, but these could be combined with threats from the physical sphere. Strategy for this vector does not involve information deterrence alone, whether in cyberspace or with other forms of information. Timothy Thomas wrote, "Informatized warfare can increase its deterrent power capable of achieving strategic objectives when combined with nuclear deterrence capabilities."[8] Actions in this space may also leverage conventional deterrence, space deterrence, and information deterrence as a "cocktail" for use in future conflicts.

Practitioners in the nation-state sphere of interaction view cyberspace as an asymmetric entity, in which cyberconflict, economic actions, a domestic or international public information campaign, or other measures, supplement large-scale military activities that may be unavailable or simply not usable. Most behavior in this sphere is driven by the belief that information superiority is becoming a key component of national power.

As a result, states and other participants can probe aggressively and enter global cybersphere networks to gain

a competitive advantage in economics, business, military, and political bargaining for strategic reasons; for example, by conducting strategic reconnaissance to "win victory before the first battle" by mapping the opponent's digital "terrain."[9] Strategic digital reconnaissance will provide knowledge of the digital landscape to permit more effective military activity. In this context, proactive responses in cyberspace can be a preferred strategy for winning a cyberconflict. Such actions seek to damage or disrupt the critical nodes that comprise the material and technical foundations of the opponent's cybersystem.

Individual Cybersphere (Top Right Square).

The individual threat vector is completely in the cybersphere and involves a violation of individual cyberinfrastructures of globally accepted norms regarding content that is published in cyberspace. The response would initially be confined to the cybersphere of interaction, but could migrate to the physical sphere if the desired result is not achieved through cybersphere response(s).

PHYSICAL SPHERE OF INTERACTION ("TRADITIONAL" SECURITY)

The physical sphere of interaction—the traditional focus of security concerns—addresses the physical or economic well-being of the individual, formal organization, or state. Traditional security threats come from within the physical sphere, and the response was and often is delivered in that sphere as well; however, the cybersphere can be used to augment a physical sphere response.

Global Physical Sphere (Bottom Left Square).

International security often involves activities in the global physical sphere. States collaborate to enforce an accepted global norm, which is typically also in their own interests. Although primarily physical, instruments of the cyberdimensions of national power increasingly are being used in conjunction with physical military instruments and other dimensions of national power to provide an even greater comparative advantage.

National Physical Sphere (Bottom Center Square).

This sphere represents the historical, realist notion of national security: a state acting within the physical sphere of interaction for its own self-interest, generally employing the military dimension of national power. Activity within the cybersphere of interaction can greatly enhance both the physical sphere's initial instruments of military power, as well as any subsequent activity.

Individual Physical Sphere (Bottom Right Square).

Often, people who live in dangerous areas and desire physical safety and the basic necessities of life turn to anyone who can provide them. Although the cybersphere of interaction could be involved, both the principal threat and response generally reside in the physical sphere of interaction. When authorities do not provide safety for those in jeopardy, unofficial groups might emerge to provide a physical (or cyber) response.

MERGED PHYSICAL-CYBERSPHERE OF INTERACTION

In the global merged sphere, the threat to a specific level of security—and a potential response—initially could appear from either the physical- or cybersphere of interaction. Any subsequent risks could arise from any or all spheres. In this scenario, it becomes difficult to locate the sphere in which activity is most prominent. Of course, there is always the potential for a physical threat to the cyberinfrastructure. The physical-cyber merged sphere seems to be the perfect example of the ability of cyberspace to impact the four traditional strategic domains, encompassing many aspects of physical- and cyberspheres.

Global Physical-Cybersphere (Middle Left Square).

The risk in the global-merged physical-cybersphere of interaction may initially be strategic, economic, or political (involving reconnaissance and intelligence gathering), and may lead to more direct action in the future. Alternatively, information derived from reconnaissance conducted by governments, embassies, research firms, trade and commerce organizations, aerospace, military installations, energy providers, or critical infrastructures could include geopolitical data for use by nations, or it could be traded underground and sold to the highest bidder. A collective response would generally fall in the cybersphere—but if the risk and loss of data were serious enough to jeopardize vital interests, then the response could move to the physical sphere.

National Physical-Cybersphere (Middle Center Square).

This sphere of interaction represents an integrated merging of the traditional dimensions of national power (political, economic, military, etc.) with the cyberdimension. Countries now view the use of the cyberdimension of national power as a supplement to other more traditional dimensions of power. They may use any and all interchangeably to achieve their preferred outcome(s) as a normal course of action, with the cyberdimension used to attack command-and-control and weapons systems directly and indirectly to disrupt various civilian functions. Cyberactivity can also be used independently to damage objects in the physical sphere.

Individual Physical-Cybersphere (Middle Right Square).

This sphere of interaction involves actions in cyberspace that jeopardize individual physical or economic security and lead to cyber- and physical responses. The initial response is generally through the cybersphere, but can migrate to the physical if the desired outcome is not forthcoming through cyberactivity. Vigilantism (or digilantism, the cyberequivalent of vigilantism) might occur in the physical and cyberspheres of interaction if an appropriate, effective response from recognized authorities is absent; this could also occur in the other two individual levels of security (cyber and physical).

GENERAL CONSIDERATIONS

Response management in cyberspace could prove to be much more problematic than it was during the Cold War because of the ontology of cyberspace and its

complex threat and response vectors—especially when definitive attribution of activity is difficult because the perpetrator strives to go undetected. However, managing security in cyberspace is not a narrow technical challenge; it involves fundamental issues of politics and strategy, nation-state relations, bargaining, and escalation dynamics and control. An understanding of the technological domain and strategic environment is imperative for developing effective responses to deliberate threats to cyberinfrastructures.

Without a solid conceptual foundation, a cyberconflict would pose significant management challenges. Even with more comprehensive scenario development and contingency planning, there is a strong potential for miscalculations and misunderstandings, which provoke an out-of-control escalatory spiral in the absence of a commonly understood definitional framework to help frame strategic and tactical choices.

The roundtables did not attempt to resolve the debate over the internal ontology of cyberspace. Such an attempt would have taken the group's attention away from the impact of a definition for cyberspace informing strategic choices by the government. Rather, roundtable participants tried to clarify the structures of the strategic environment within which cyberspace exists and operates.

Understanding the role of cyberspace in the strategic environment is crucial to making optimal decisions about cyberactivity, especially during a crisis. The roundtable discussions revealed that cyberspace is a more complex strategic domain than the other four strategic domains (air, land, sea, and space), and, therefore, demands more complex response calculations. Cyberspace is a separate independent strategic domain, much like the traditional four domains, while at the same time

encompassing those four domains. This fact presages significant difficulty for strategic planners and decision-makers who seek to accurately identify the true locus of the threat, attribution of the perpetrator, time available to respond, and response options. The roundtable participants recommend that government decision-makers be flexible and adaptable, and approach solutions with open minds within an agreed-upon strategic framework.

RECOMMENDATIONS

Recommendation One: The Federal Government Should Agree on a Definition of Cyberspace.

The roundtables believe that cybersecurity management would be more effective and efficient if the term were more clearly defined. Such a definition could replace the one now used by the Department of Defense (DoD) in Joint Publication 1–02: *DOD Dictionary of Military and Associated Terms*.[10] Based on roundtable discussions, the following definition is recommended:

> Cyberspace is a man-made global strategic domain, dimension of national power, and instrument of the dimension of national power within the information environment, consisting of the interdependent network of information technology infrastructures and resident data—including the Internet, telecommunications networks, computer systems, and embedded processors and controllers—for the production and use of information by individuals and organizations.[11]

This definition incorporates all of the aspects of cyberspace (functions, components, and uses). Roundtable participants found the recommended definition to be both comprehensive and practical.

Considerations regarding the proposed definition of cyberspace in a security context.

Several aspects of the proposed definition of cyberspace merit consideration by government decision-makers:

- Cyberspace simultaneously influences three different functions: global strategic domains, dimensions of national power, and instruments of national power. These three functions complicate cyberspace activity considerably because cyberspace has a variety of impacts, depending on the context in which it is used across these three functions. Decision-makers need to consider specifically which of those functions involves cyberactivity and which function should be used in responding to a threat if warranted.
- Cyberspace is a system composed of hardware, digital data, and human beings. It is a man-made system, with inherent vulnerabilities stemming from its design and construction, especially its network structure—which continues to evolve in a scale-free fashion with little overall organization or function.
  - Decision-makers should identify and prioritize cyberspace vulnerabilities (especially to critical infrastructures) according to the risks posed by a targeted attack on the continued well-being of U.S. national and economic security.
  - Methods or strategies to reduce or eliminate those prioritized structural vulnerabilities can either be taken or become a research priority, to enhance the continued operations that support national security.

- Cyberspace exists to facilitate human activity and is subject to human decision-making with all of its foibles; people must be involved in cyberspace operations, creating or initiating even automated cyberactivity, which then operates without direct human intervention. Human decision-making is not formulaic; it is based on different individuals' sometimes idiosyncratic assessments of costs and benefits, beliefs about fundamental issues of politics and strategy, skills in bargaining, and escalation dynamics. Cyberspace-based responses should be made by human decision-makers, not predicated solely on an algorithmic response, given that these decision-makers created the circumstances that require a response.

Recommendation Two: Government Should Apply the Definition of "Strategic Domain" to Managing These Domains.

The relationship between cyber- and the four other spheres, and the unique nature of cyberspace's strategic domain, involves both an independent space in which cyberactivity takes place and the other four strategic domains. This makes national security decisions involving cyberspace extremely complex. An increase in knowledge about the cyberdomain and its role and function in the strategic environment will allow decision-makers to identify different strategic options and should lead to more sophisticated anticipation of threats, as well as more nuanced and effective responses that account for the costs and benefits of various choices.

Particular efforts should be devoted to identifying the domain from which the cyberactivity originated. Making decisions in the strategic context of cyberspace

is as much about managing uncertainty across multiple domains that cyberspace activity affects as it is about achieving a specific goal. Successful strategic decision-making and management in cyberspace involves:

- Clear identification of goals;
- A profound (or deep) understanding of the relevant strategic environment;
- A clear assessment of the comparative advantages offered by one proposed solution over another, as they affect the entire environment; and,
- A calculation of costs through an objective appraisal of the effect of an action on national resources.

Effective government cyber decision-making will provide management between the internal cyber-domain-environment and the external domain environments, with an understanding of the goals and values, resources and capabilities, structure, and systems—and will identify the range of options of cyberspace's domains that it would be helpful for decision-makers to understand.

Questions to Consider in Applying Cyberspace within a Strategic Domain.

- At what point does the degradation of cyber- and other critical infrastructure systems become so serious that it jeopardizes the nation's ability to act in response to threats?
- In what instances should government ignore problematic activity against cyberinfrastructure? The level of risk acceptance across critical infrastructure sectors should be identified and prioritized to determine what constitutes a

national security risk as opposed to a "nuisance" (i.e., cyberactivity that is annoying or interferes with the operation of the national cyberinfrastructure, but does not rise to the level of threatening its existence or operability). Identification and prioritization of risks relevant to a critical infrastructure could lead to the establishment of a typology of activity based on risk acceptance, which could assist decision-makers in deciding how best to respond to the cyberactivity.

- When is an escalation of cyberactivity in response to a threat or a preemptive action warranted?
- What activity would prompt movement across strategic domains? What could those linkages be, and how might they shape a cyberconflict? Should escalation into other domains be sequentially ordered? What are acceptable parameters for the following:
  - **Authority:** Who acts, where, and when?
  - **Response:** What actions to take? What are the rules of engagement?
  - **Resources:** What are the scope and scale of the following actions:
    - Which dimension(s) of national power to use, and in what mix?
    - Which elements of national power to use, and in what mix?
    - Which domain(s) to act within?
  - **Impact:** What are the likely consequences of a response?
  - **Crisis:** When does cyberactivity become a crisis (e.g., given an unexpected occurrence, time constraints, widely unacceptable degree of risk, or high importance of a decision)? Crisis

management and cyber-incident-response can be challenging, especially when the perpetrator of a hostile act seeks to go undetected. What level of threat and other internal and external forces (e.g., type, severity, internal dynamics, range of outcomes) could impede adequate management of a cybercrisis?

Recommendation Three: Educate Practitioners about the Nature of Cyberspace, to Help Government Effectively Manage Across the Range of Cyber-Risks and Response Options. Training Can Provide Important Context to Frame Actions in the Event of a Cybersystem Degradation or Shutdown, especially a Cyberevent that Jeopardizes the Nation's Health and Welfare.

Understanding the nature of potential impacts across cyberspace and related domains will improve the capacity of government to anticipate and act in the face of these threats. Anticipation, built through training, will diminish the risk of miscalculations and misunderstandings that could provoke an escalating spiral of actions harmful to security. Such training should include:

- A series of scenarios that could be developed to depict different cyberthreat/risk situations in all the spheres of interaction, along with calculations threat-and-risk impact, so that decision-makers and operators have the benefit of existing knowledge and practice to hone their ability to confront these risks. Such scenarios could address answers to the questions above and be framed to accommodate:
  - Results
  - Time
  - Attribution error

  - Precedent-setting activities
  - Type and extent of responses.
- More sophisticated scenarios that could be generated to depict two- or multi-factor risk/threat situations to assess possible actions proposed to introduce asymmetric risk (an investment involving uneven gains and losses). Such scenarios could be made more realistic through simulations that involve both nation-state decision-makers and those who jeopardize nation-states, by generating activity in both the physical and cyberspheres of interaction.
- Estimates of the probable effectiveness of responses to a given scenario that could be modeled, providing decision-makers with a tool to understand the potential impacts of these types of decisions.
- Digitized training, which could be developed to involve "gamifying" different situations using video techniques to reflect cross-domain impacts.

ENDNOTES - CHAPTER 2

1. The author thanks Colonel Matthew C. Molineux, U.S. Air Force, Director, Aerospace Studies and the Eisenhower Series College Program, U.S. Army War College, for his diligent research to identify the lack of a definition of "cyberspace" and his work to provide the one used here.

2. Dighton Fiddner, *Defining a Framework for Decision Making in Cyberspace,* Strengthening Cybersecurity Series Report, Washington, DC: IBM Center for The Business of Government, 2015.

3. *Ibid*., p. 8.

4. Computers (or software) are now automatically constructing malware independently without intervention by humans. National Public Radio, 2013.

5. U.S. Joint Chiefs of Staff, *Information Operations,* Joint Publication 3-13, Washington, DC: U.S. Joint Chiefs of Staff, November 20, 2014, considers cyberspace one of 14 different information related capabilities (instruments of national power) that contribute to information operations.

6. Fiddner, p. 10.

7. *Ibid*., p. 12.

8. Timothy L. Thomas, Chapter 7 in this volume.

9. *Ibid.*

10. "[A] global domain within the information environment consisting of the interdependent network of information technology infrastructures, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers." U.S. Joint Chiefs of Staff, *Department of Defense Dictionary of Military and Associated Terms*, Joint Publication 1–02, Washington, DC: U.S. Joint Chiefs of Staff, 2011.

11. Fiddner, p. 6.

CHAPTER 3

EMERGING TRENDS IN CYBERSPACE: DIMENSIONS AND DILEMMAS

Nazli Choucri

This chapter was originally funded by the Office of Naval Research under Award Number N00014-09-1-0597. Any opinions, findings, and conclusions or recommendations expressed in this publication are those of the author(s) and do not necessarily reflect the views of the Office of Naval Research.

INTRODUCTION

Almost everyone everywhere recognizes that cyberspace is a fact of daily life. Created by human ingenuity with the Internet at its core, cyberspace has become a fundamental feature of the 21st century. Almost overnight, interactions in this virtual domain have catapulted into the realm of high politics and are at the forefront of nearly all key issues in international relations. However, today, this domain has become a source of vulnerability—posing potential threats to national security and a disturbance of the familiar international order—and a major arena of unlimited opportunity for various forms of power and potential. The rapidly shifting configurations of interactions in this virtual domain—with expanding actors and actions with diverse causes and consequences—continue to create major disturbances in the traditional system, a major legacy of the 20th century.

The vocabulary of world politics has already accommodated these new realities by signaling refer-

ences to cyberconflict, cyberpower, cyberintrusion, cybercooperation, and cybersecurity, to name only a few. The early concepts were put forth in hyphenated terms (such as cyber-security); now these are increasingly framed in one word (notably, cybersecurity). At first glance, such differences might seem trivial, but the shifts point to an explicit recognition of a new phenomenon, one that is no longer captured by the hyphenated concepts imported from the familiar politics of 20th-century international relations.

The purpose of this chapter is to highlight the salience of cyberspace's characteristic features, which are so fundamentally different from those of the traditional realities we are already accustomed to. Emergent trends on the Internet reflect significant shifts of actors and actions in the cybersphere and reveal the reconfigurations of interests and influence in the virtual domain of world politics. We begin by signaling some of the distinctive features of cyberspace and cyberpolitics, which create disconnects between traditional and familiar conditions and the current realities.

CYBERSPACE AND CYBERPOLITICS

Of the many critical disconnects between the new cyberarena and the traditional domain of international relations, we focus on seven of the most problematic for all actors in world politics—state and nonstate, formal and informal. Individually, each feature is at variance with our common understanding of social, political, and economic realities. Jointly, they signal a powerful disconnect between contemporary understandings of international relations.[1] These pertain to:

a. **Temporality**, in the sense that chronological time is replaced by near instantaneity in the realization of action and potential reaction.

b. **Physicality**, meaning that activities undertaken or decisions made are not constrained by geography, spatial consideration, or sovereign boundaries.

c. **Permeation**, which refers to communication and activities that penetrate state boundaries and sovereign jurisdictions. As we shall indicate, however, the sovereign state is trying increasingly to control access, with varying degrees of success.

d. **Fluidity**, which refers to the ease with which shifts in patterns of interactions take place, with attendant configurations and reconfigurations and the emergence of new actors and modalities of interaction.

e. **Participation,** in the sense that access to cybervenues has already shown how barriers to activism and political expression can be reduced, and the wide range of effects that could then occur.

f. **Attribution,** where the basic property of cyberspace in this connection refers to the obscurity of identity for actors as well as the difficulty of linking actors to specific actions.

g. **Accountability,** which refers to the absence of mechanisms of responsibility, due most largely to the lack to attribution possibility.

Any one of these factors alone creates serious dilemmas for the conduct of international relations. Jointly, they suggest that cyberpolitics in this domain cannot be reduced to a mirror image of interactions in world politics as conventionally understood—given the historical record and the tradition of empirical analysis, on the one hand, and our conceptual and theoretical tools, on the other.

In this context, **cyberpolitics**, a recently coined term, refers to the conjunction of two processes or realities—those pertaining to traditional human interactions (**politics**) surrounding the determination of **who gets what**, **when**, and **how**, and those enabled by the uses of a virtual space (**cyber**) as a new arena of interaction with its own modalities, realities, and contentions.[2]

OLD LEGACIES AND NEW REALITIES

The traditional systems of international relations, such as those with bipolar, multipolar, or unipolar structures—generally characterized by hierarchical power relations—are being replaced by new structural configurations characterized by the diffusion of power, decentralization, diverse asymmetries, and different types of power relations. Together these new features co-exist with, if not replace, the well-known vertical structures of power and influence. Cyberspace may be relevant to all these, but it did not create them.

Legacies of the 20th Century.

By definition, the legacies of the 20th century shape the basic parameters of the 21st century. Some of these legacies will prove to be transient; others are definitional in setting the contours of 21st-century international relations power and politics. Most notable among these is a large number of new states, formed by the decolonization process coupled with the periodic reframing of sovereignties and territorial boundaries. Somewhat related, with a logic and dynamic of its own, is the growth in the number of international institutions and the expansion of scale and scope of their activities.

We also must recognize the explosion of profit-seeking private sector activities and the consolidation of global reach permitted and propelled by technological innovations, market conditions, and emergent opportunities. With persistent expansions, the corporate structure of investment activities took on worldwide risks and responsibilities to investors of various kinds. The use of "private" may be somewhat misleading in this context, as state-based or state-owned firms should not be ignored. With the nationalization of resource extraction enterprises, for example, the state replaced the private (and usually foreign) investor in ownership as well as in operations and management.

Slow at first, and then more rapid—eventually occuring at an accelerated pace—is the growth of voluntary, not-for-profit entities in international relations. Initially, they appeared largely for the purpose of expanding religious faith. Gradually and almost imperceptibly, they adopted a wide range of causes, pursuing an ever-expanding set of activities and interests. Some of these non-profits were encouraged by the state system; others by the profit-seeking sector. But all pursued a target-based agenda driven by specific interests, even when these were defined in broad terms. With the increasing politicization of science and technology worldwide, the scientific community supports a wide range of research activities organized around particular knowledge interests. Over time, it became clear that the post-World War II major powers no longer held the monopoly of control over the global political, social, or economic policy agenda. By the 1980s, the international policy priorities, consumed by the conjunction of developmental and environmental challenges, framed what was arguably the first, most comprehensive global approach

to policy imperatives—at all levels of development and all forms of political aggregation. The concept of "sustainability" was framed to become as salient as "security," as conventionally understood in world politics.

None of these developments were due to the construction of cyberspace.

Realities of the 21st century.

When we factor in the construction of cyberspace—especially the dramatic expansion of cyberaccess worldwide, the growth of "voicing," global civil society, and the new economic and political opportunities afforded by the Internet—cybervenues appear to be more than enablers of power and influence. They are critical drivers of the ongoing realignments, the means by which all actors, at all levels of analysis, pursue their goals and objectives. Furthermore, they have assumed constitutive features of their own.

Constructed by human ingenuity, cyberspace is a domain of interaction enabled by new forms of communication venues. Almost overnight, human beings—who now recognized the salience of the natural environment and its life-supporting properties to be fundamental to survival and well-being—were interacting in a new environment whose properties were yet to be fully understood.

This particular reality of the 21st century did not replace, reduce, or eliminate the effects of 20th-century legacies. It created added complexities—augmenting, rather than reducing, the impact of the features noted above. The "new" reality altered key traditional dynamics of world politics and shaped many new features that were largely unprecedented but profoundly

pervasive in scale and scope. To begin with, the 21st century witnessed the effects of changes in the traditional power calculus. The old "polarity" framework in international relations was replaced by a highly distributed structure. This shift, a legacy of the 20th century, must be viewed in conjunction with critical elements of the new realities.

Among these are the powerful asymmetries in power and capability in traditional (kinetic) and new (cyber) terms. Stated differently, almost overnight, many states—large and small—expanded their cyber-based capabilities in ways that were not contingent on their position in the traditional power-based system. Equally important, if not more so, is the clear dominance of the private sector in the management of the cyberdomain. The fact is that the state system is a latecomer with respect to governance and the operation of cyberspace. Thus, we have increasing complexity in cybermanagement coupled with growing politicization. The management system put in place by the United States early in the cyberera was being contested by states with alternative visions and interests, such as China, Russia, and others.

For the state system as a whole—as well as for individual countries—many features of cyberspace, such as those noted above, created new vulnerabilities and new challenges for national security. Cybersecurity is now fundamental to the security of states, firms, organizations, institutions, and individuals. The challenge now is to provide this new imperative with robust theoretical and empirical foundations, which would at the very least enable the formation of robust policy responses.

All of this is due to the construction of cyberspace.

The Net Results.

Almost by definition, new forms of conflicts have emerged—for state and nonstate entities—supported by new instruments, tools, and weapons. These new conflicts are political and economic in nature, driven by the pursuit of power and the pursuit of wealth—in both legitimate and nonlegitimate venues. To be fair, international law for cyberspace is at the early stages of development; the rules for legal cyberconflict and competition and the acceptable venues for cybercontention are at their earliest stages.

Concurrent with the growth of conflict in cyberspace—or uses of cybervenues for the conduct of traditional conflict—are diverse international efforts to develop rules of cyberconduct; norms for cyberbehavior, laws, and regulations; and institutions for cybersecurity. Since the state is the only entity enfranchised to speak or act in the international system on behalf of its citizens—or people within its borders—it leads the formal cyber-related discussions and represents both private and public interests.

In the most general terms, we can identify two specific and overarching outcomes for the international system of 20th-century legacies and 21st-century realities. The first is an increasingly "close coupling" between traditional- and cyberpolitics in international relations, reflecting the growing interconnections between two initially distinct and separate arenas of interactions. By definition, "close coupling" does not necessarily imply mirror-image dynamics. That in itself in an empirical question. The second is the evolution of "hybrid" policies, generally in response to particular dilemmas rather than to reasoned policies based on robust principles.

Table 3-1 summarizes the differences in strategic international context "then" and "now."

THEN: 20th-Century Power-Politics Only the Major Powers	NOW: 21st-Century Cyberpolitics Anyone & Everyone
Bipolarity	Multiplicity & Diversity
Structural Power Balance	Structural Instability and Volatility
Clear Deterrence Calculus	Complexity in Deterrence Calculus
Recognized Symmetry	Uncertain Asymmetry
Known Actor Identity	Obscured Actor Identity
Shared Aversions	Varied Avoidance
State Dominance	Loss of State Dominance
Known Paths & Outcomes	Unknown Paths & Outcomes

Table 3-1. Strategic Context—Then and Now.

EMERGENT TRENDS IN CYBERSPACE

We now turn to cyberaccess and patterns of cyberparticipation. If we consider mobile signals as a notable indicator, then Figure 3-1 reminds us that by 2010, only 10 percent of the world's population did not have access to a mobile cellular signal. For all practical purposes, almost the entire globe was covered. However, this statistic in itself obscured many important features of cyberparticipation. See Figure 3-1.

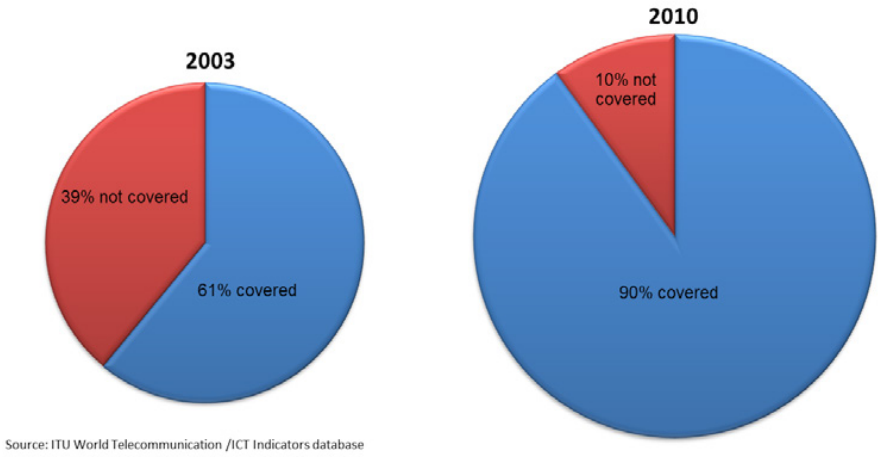


Figure 3-1. Percentage of the World's Population Covered by a Mobile Cellular Signal, 2003 Compared to 2010.[3]

Distribution of Users.

We show in Figure 3-2 that in 2012, Asia hosted the largest percentage of users worldwide. The regional distribution for that year illustrates an interesting disparity anchored, not only by differences in population size, but also in rapid growth in cyberaccess.

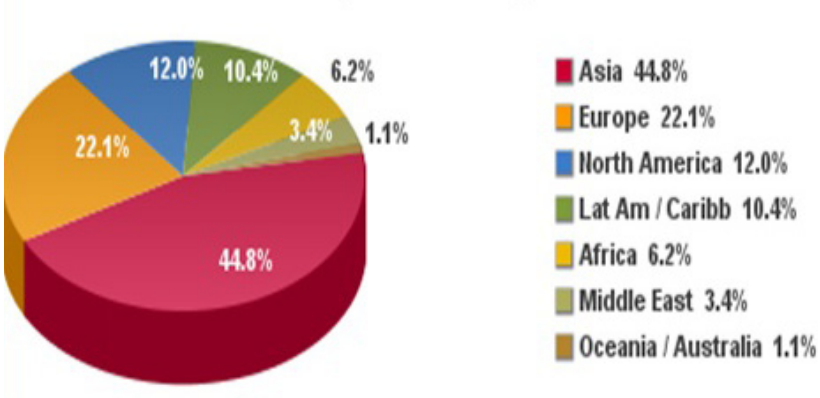


Figure 3-2. Internet Users in the World, Distribution by World Regions, 2011.[4]

Figure 3-3 presents a different view of cyberparticipation, one that focuses on the number of individual users and thus draws attention to new features of international relations. We consider this indicative of "people power," in the sense that the individual is now able to articulate preferences and voice interests. None of this can guarantee results, but it must be recognized as a notable feature of cyberdemography.

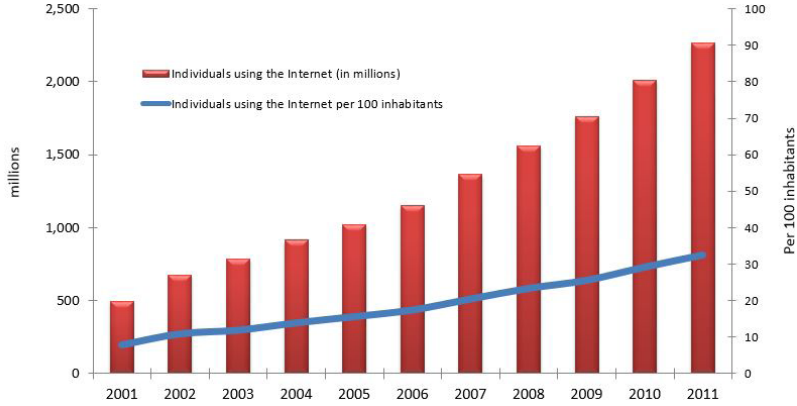


Figure 3-3. Global Numbers of Individuals Using the Internet, Total and Per 100 Inhabitants, 2001-2011.[5]

Yet another perspective on the political demography of cyberspace is based on the 2010 Internet User statistics worldwide. If we consider total Internet users, note, for example, the differences between the United States (227 million) and China (298 million): these figures represent 74 percent of the total U.S. population, but only 22.4 percent of China's population. Invariably, the character of cyberspace is influenced by shifts in the composition of users. With this demographic contour of cyberspace, new complexity follows.

New Complexity.

Nowhere is the influence of cyberdemography more evident than in the languages used on the Internet. While English continues to dominate, Chinese is a close second. The other notable languages shown in Figure 3-4 trail behind significantly. These are all

absolute figures, which reflect the accumulation of language use over time. They provide little insight into differences in rates of change across languages. These differences shape much of what is observed at aggregate levels.

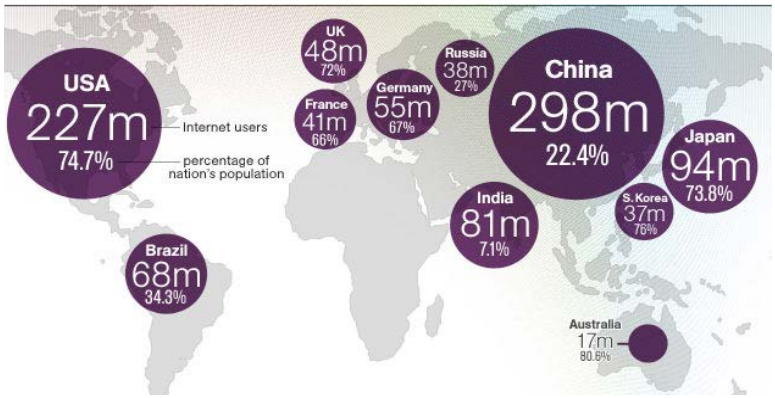


Figure 3-4. Internet Users by Country, 2009.[6]

Among the most significant features of the new political demography of cyberspace—the user, the language used, and the implications for the pursuit of power and the pursuit of wealth—is the variety we observe in rates of change. Figure 3-5 shows Internet usage by language for 2010. This figure "speaks for itself." Especially significant is the size of the representation of non-Western language. Such differentials may well enhance, rather than dampen, the politicization of cyberspace and the salience of "high politics."

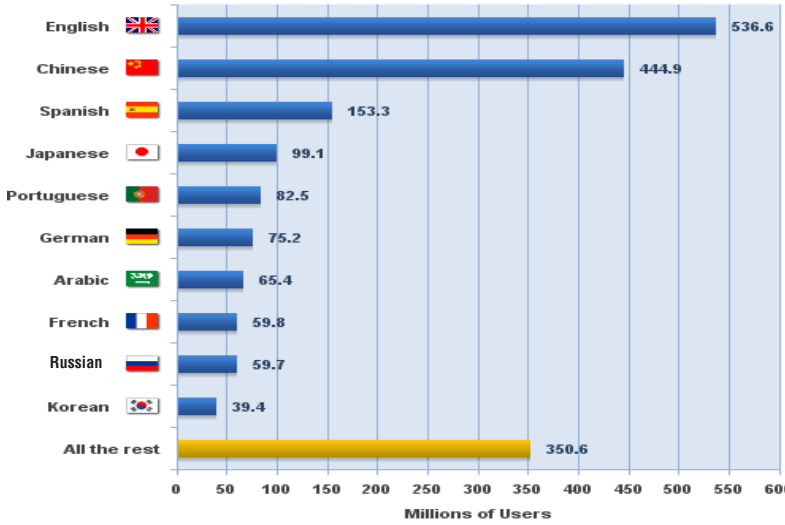


Figure 3-5. Top Ten Languages on the Internet, 2010, in Millions of Users.[7]

MALEVOLENCE AND THREATS TO CYBERSECURITY

We have focused so far on emerging trends in cyberspace. Characteristic features of cyberdemography and shifts in the configuration of users constitute "fundamentals" of this new arena of interactions. With the basics in place, we now turn to three forms of well-documented activities, namely: the denial of service, a variety of cyberattacks, and select facets of cyberespionage. These reflect different challenges to cybersecurity—by different actors, with different motivations, different instruments, and different stakes. However, these challenges are all driven by the basic primitives of international politics; that is, the pursuit of power and the pursuit of wealth.

Cyberattacks.

Cyberattacks have become an integral part of the entire cyberecology. The diffusion of damage-creating tools and the deployment of malevolence technologies, coupled with the growth of markets for malware, put cybersecurity at the forefront of national and international concerns in almost all parts of the world—threatening sovereign states as well as private entities and individual as well as organizational users.

Figure 3-6 shows the growth of cyberattacks, the originating country-location, and the number of organizations affected by different tools of malevolence. Clearly, from the country of origin, we cannot conclude that the government itself is responsible for the attacks. The originating country refers to the physical location of the attacker, but does not imply that government action was the source. In the most general terms, this growth further reflects the "power of the individual" unrestrained by sovereign jurisdiction of conventional territorial boundaries.

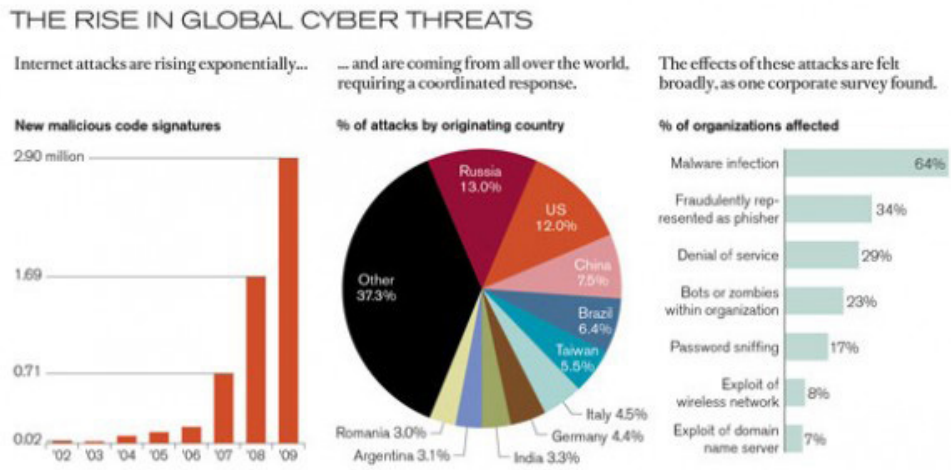


Figure 3-6. Cyberattacks: The Rise in Global Cyberattacks.[8]

Denial of Service.

The foregoing notwithstanding, at the same time, the state does not remain inert. We see the hand of government in the denial of service. Denial of service is a prerogative of the state, with formal authority, legitimacy, and regulatory capability. Figure 3-7 shows denial of service requests to Google, indicating how often governments request content removal, and how often Google agrees to the requests. The figure also indicates the reason stated for the request. To note the obvious, the diversity of requests is remarkable, as is the distribution of requests. Of course, there are considerable differences in government systems and national and social priorities, capabilities, and cyber-access. To note only the three most obvious cases—Brazil, Germany, and South Korea—the size and reasons

illustrate salient issues at the state levels. By contrast, if we consider India and Libya, the drivers of requests in the then-authoritarian state (Libya) are far greater and more varied than in the democratic state (India). Interestingly, India features prominently in another dimension of cybermalevolence, namely, as a target of espionage from China.

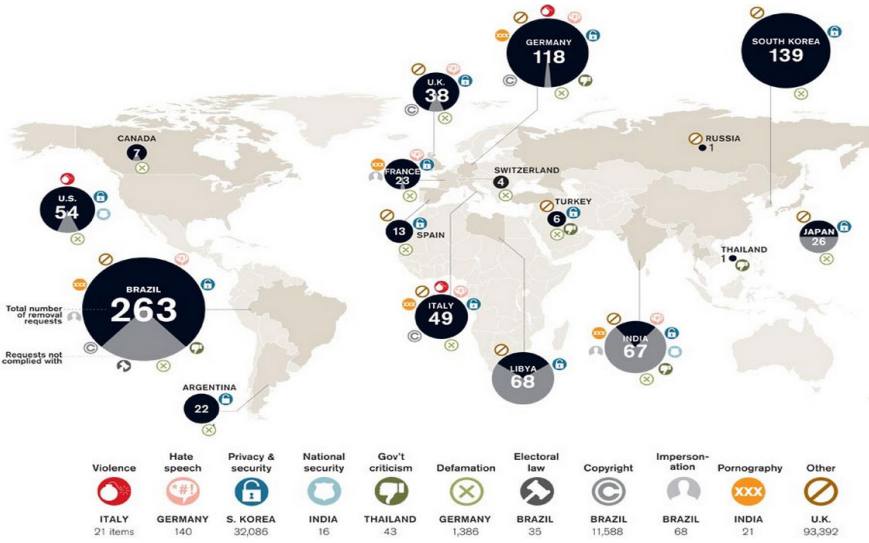


Figure 3-7. Denial of Service.[9]

Cyberespionage.

Given the fluidity of the emergent cyber-based vocabulary, it is often difficult to distinguish between "attack," "penetration," and "damage" as forms of behavior just like it is difficult to differentiate among instruments and tools or "malware" or other types. Of course, motivations are usually attributed to, rather than announced by, the actor or country-source.

With these considerations in mind, Figure 3-8 shows one representation of computers "compromised" with China as the source. This representaation, put forth in the *MIT Technology Review,* reflects the reach of computer penetration and compromise origination from China. Unexpected in Figure 3-8 is the salience of India as a target country—compared to other targets that are depicted. Either India's cyberdefenses are weaker than those of other state-locations, or India holds a greater attraction for penetration by users from China.

None of the data in Figure 3-8 have the precision or the empirical foundation of the 2012 Mandiant report, but they do provide a sense of the attributed Chinese penetration.[10] The general view is that such penetration is largely in the form of industrial or corporate espionage. By international standards, such penetration is a form of illegitimate "technology-leapfrogging," one that is manifested through venues not exactly advocated for by development analysts.

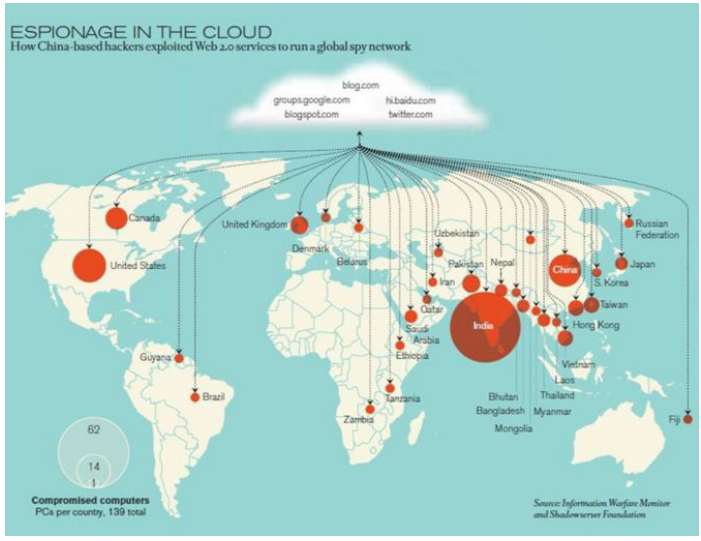


Figure 3-8. Espionage in the Cloud.[11]

EPILOGUE

The state-based international system, anchored in the traditional Westphalian concept of sovereignty, is increasingly influenced by the construction and expansion of cyberspace. Among the many effects, the following are among the most notable: First are the new challenges to national security, with new sources of vulnerability (cyberthreats) and new dimensions of national security (cybersecurity), coupled with uncertainty, fear, and threat from unknown sources (attribution problem). Second is the empowerment of new actors, some with clear identities and others without—but all with opportunities for growth. Among these are national actors created to exercise access control or denial, nonstate commercial entities with new products and processes, entities operating as proxies for state actors, and novel criminal groups, often too anonymous to identify, too varied to list, and too difficult to locate—all shaping new and unregulated markets. Third is the wide range of novel types of asymmetries that shift power relations and create new opportunities to exploit the advantages afforded by cyberanonymity. For example, such opportunities allow for weaker actors to threaten stronger ones, or for criminals to expand their activities, or for individuals to challenge the power of the state system—to note some of the most obvious possibilities.

Developments such as these are all breeding grounds for **malevolence** in its various forms, which create unprecedented threats to the stability and security of the state system, business enterprises, and activities of not-for-profit nonstate actors. The militarization of cyberspace, potentials for cyberwarfare, threats to critical infrastructures, and so forth are

among the explicit and evident threats. Equally, and perhaps more damaging, is the multiplication of computer-penetration activities that appear to be in the realm of industrial and technological cyberespionage. Given the mounting evidence of such malevolence, the international community is beginning to recognize the salience and significance of this threat trajectory.

While not the focus of this particular chapter, the issues addressed in this monograph all point to an increasingly critical global dilemma surrounding the governance of cyberspace. At its core, the dilemma is framed by two countervailing trends—on the one hand is the growth of an increasingly strident demand for governance mechanisms regulating conduct in cyberspace; on the other is the consolidation of international cleavages over the policy principles upon which to construct the supply of mechanisms for cybergovernance. This dilemma, noted here in the idiom of the marketplace, is fundamentally one of power politics—a worldwide struggle over new opportunities for the pursuit of power and wealth as well as gains in strategic and market contexts—made possible by the fluidity of the cybersphere.

ENDNOTES - CHAPTER 3

1. Nazli Choucri, *Cyberpolitics in International Relations*, Cambridge, MA: MIT Press, 2012; David Easton, *The Political System: An Inquiry into the State of Political Science*, New York: Alfred A. Knopf, 1953.

2. For this concept of politics, see Harold D. Lasswell, *Politics: Who Gets What, When and How*, New York: McGraw-Hill, 1958; David Easton, *A Systems Analysis of Political Life*, New York: Wiley 1965; and Easton, *The Political System*.

3. Data from ITU World Telecommunications/ICT indicators database.

4. Internet World Stats, Copyright 2001-11, Miniwatts Marketing Group, available from *internetworldstats.com*.

5. Data from ITU World Telecommunication/ICT Indicators database.

6. A News.com.au graphic of Internet users by country as of 2009, July 29, 2009, Sydney, New South Wales, Picture by Simon Wright, Newspix, available from *internetpromotion-australia.com.au/internetpromotionblog/?p=250*.

7. Internet World Stats.

8. Tommy McCall (Infographics.com) in David Talbot, "Moore's Outlaws," *MIT Technology Review*, Vol. 113, No. 4, July/August, 2010, p. 43.

9. Mike Orcutt and Tommy McCall, in Brian Bergstein, "Going Offline: Google reveals how often governments ask it to banish things from its services and how often it complies." *MIT Technology Review*, Vol. 114, No. 6, November/December 2011, pp. 30-31.

10. Mandiant, "APT1: Exposing One of China's Cyber Espionage Units," available from *intelreport.mandiant.com/Mandiant_APT1_Report.pdf*.

11. Talbot, pp. 36-43.

CHAPTER 4

TECHNOLOGIES THAT WILL CHANGE YOUR WORLD

Rick Hutley

INTRODUCTION

Regardless of which industry you work in today, what pastimes you have, or where you live, your world is dominated by technology. There is almost nothing we do today that does not depend upon technology somewhere along the line. Even rural farmers who live off the land depend upon technology to deliver the water or package the seeds.

We have all seen a wide variety of technological innovations in our lifetimes, and all of them have played their part in transforming our world. Some of their impacts have been relatively subtle but nonetheless pervasive, such as the humble battery; while others, such as the telephone or the computer chip, have made dramatic changes in our world. Human ingenuity and innovation are truly remarkable. What is equally surprising is that they have been remarkably consistent. Ray Kurzweil, one of the world's leading futurists, has shown that human innovation closely follows an exponential growth curve—approximately a 45-degree upward sloping line on a logarithmic scale![1] Nothing has slowed our rate of innovation—not the Great Depression or even two world wars—and over the past 100 years or so, most of that innovation has involved technologies of various kinds.

While technological innovations have brought us heretofore unimaginable capabilities and benefits,

they have also exposed us to a whole new breed of threats. At their core, these threats can be summarized in the realization that humankind no longer has the ability to survive without technology. Our world would be thrown into utter chaos if we were to lose our technologies, and it is critically important that we consider the implications of any threat to our technological foundations.

Technology has changed our lives beyond all recognition, and it will change our lives again and again—but not always for the better.

A WORLD WITH FEW LIMITS—THE ERA OF BIG DATA (ACTUALLY, BIG EVERYTHING)

We live in an increasingly complex world driven by an exponential explosion of technological innovation. Stop for a moment and consider that word "exponential." We have all seen the graphs; you probably use that word quite regularly, but have you ever considered what it truly means?

There is a famous legend from India regarding the literal power of exponential growth. A local king who was fond of chess would offer anyone who could beat him any prize that person wished. One lucky winner simply asked for rice—to be added to the chess board in the following manner: one grain on the first square, twice as many (two grains) on the next, twice again on the third square (four grains), and so on. The king eagerly agreed, thinking it a small price to pay. There are, however, 64 squares on a chessboard and on the last the king would have needed to place 18,000,000,000,000,000,000 grains of rice. That equates to around 210 billion tons of rice—enough to cover the entire territory of India with a layer of rice one meter thick!

Exponential is a BIG concept.

We live in an era of truly exponential data growth. Some of the numbers are staggering:

- In 2009, mankind created more data than we created in the previous 5,000 years combined![2]
- Global mobile data traffic grew 70 percent in 2012, and that growth is accelerating.[3]
- We send over 2.4 million emails every second.[4]

These types of statistics abound. Consider communications bandwidth. In 1998, the cost of transporting Internet data was around $1,200 per megabit. These costs have steadily been reduced between 30 to 50 percent per year until today, when it costs around $0.50 cents per megabit.[5] That is a 240,000-percent price reduction. However, it is not just about cost. We can now transmit high-quality live video to most parts of the planet for viewing on everything from giant television screens to wristwatches.

Storage is another practically unlimited resource. In 1956, IBM introduced the first computer hard drive with a capacity of five megabytes. By 1980, IBM had increased this capacity to over one gigabyte at a cost of $140,000. Today, a thousand times that capacity (or one terabyte) can be purchased for as little as $60, and, through the magic of Internet storage—or cloud storage—unlimited amounts can be purchased for around $0.06 per gigabyte.

Perhaps the most remarkable improvement over time has been in raw computing power, which has seen a similar exponential growth. In 1949, J. Presper Eckert and John Mauchley developed the Electronic Numerical Integrator and Computer. It weighed over 30 tons and could perform around 5,000 additions

per second. The cost of this behemoth has been lost to the sands of time—probably for good reason. By 1997, IBM built Deep Blue, the first computer to beat a human at chess, and, in 2011, the corporation did it again when IBM's Watson computer soundly beat all human competitors on the TV quiz show, *Jeopardy*.

Computer processing power steadfastly has followed Moore's Law since 1965, when Gordon Moore first projected that the number of transistors (on a computer processor chip) would double every 2 years. In order to cram more and more circuitry into a single integrated circuit, the size of the individual components has shrunk and shrunk. Today a single chip can have up to five-billion transistors.

While these statistics are impressive, does it really matter? Put simply, yes, it does. These technologies mean that we could store every piece of information we could ever need, transmit it to anyone, anywhere at any time, and then process it faster than we could possibly imagine. These technological advances open up a universe of opportunities. From a security perspective, this also means that anyone with around $1,000 and an Internet connection can gain access to information on any topic from how to boil an egg to how to boil the ocean—and reach every person on the surface of the earth, instantly. That is both an exciting and scary development—and we have not even begun to explore the possibilities.

Some have projected the demise of Moore's law, pointing out that we are reaching the limits of electronic circuits imposed by the physics of electrical conduction. In other words, we are reaching the point where we will not be able to develop faster processors, or cram more storage into our devices. They are correct, but that has not prevented us from continuing our

inexorable ability to innovate our way to even greater heights. We are now in the process of developing an array of new computing techniques that will take us far beyond the physical limitations of traditional electronics, including photonic computers, DNA computing, and quantum computing.

Our capacity to innovate and create ever faster, more powerful technologies fortells an amazing (yet potentially alarming) future. Ray Kurzweil predicts that by 2040, we will have developed computers with the capacity to exceed the processing power of the human brain, and, by 2050, we will have developed a machine with more processing power than the entire human race![6]

Whether it is the power of computer chips, the speed of communications bandwidth, the amount of storage at our disposal, or data, the fact is there are almost **no practical limits** to our digital world.

THE CAPACITY OF THE INTERNET—AND THE INTERNET OF EVERYTHING

Consider the Internet itself for a moment. One way to think of the Internet is like a vast postal system, in which everything connected to it; including you, me, and our digital toys, all have a unique address. We can send information to those addresses to impart information, request information, or cause a device to take an action. In short, if we can give something an Internet address, we can see it, track it, and control it.

In 2008, the Internet ran out of addresses. That made things a little tricky. It would be a bit like telling everyone that no one else can have a house because we have run out of house numbers. Fortunately, the technologists saw this coming, so they developed a

new, bigger addressing system that had more numbers—a lot more numbers! The new Internet Protocol version 6 (IPv6) has an astronomical address range—to be precise:

340,282,366,920,938,463,463,374,607,431,768,211,456

In theory, that would allow every person on the planet to have 4.25 E^{28} addresses each—or 6.7 E^{19} addresses for every square centimeter of the earth's surface. Again, for all **practical** purposes, **everything** could have an IP address.

In 1995 (the beginning of the Internet as we know it today), there were approximately 16 million users. Within 10 years that number had grown to one billion users, and, by the middle of 2012, we had reached 2.4 billion. That is still only 34 percent of the human population, so we have a lot of growth to go yet.

However, the number of "things" that we are now connecting to the Internet will far surpass the number of people connected to the Internet. In 2008, we officially entered the **Internet of Things** era—the point at which there were more things than people connected to the Internet. Now, with the advent of the new IPv6 addressing range, we are entering the **Internet of Everything** era.

THE GARDEN OF GOOD AND EVIL—SECURITY IMPLICATIONS

By 2020, we estimate there will be over 50 billion devices connected to the Internet. So what are all these **things**? Some are what we might expect.

- **Computers:** We all use computers every day, but do you realize just how many computers you rely on for almost every aspect of your life, every day? For example, there are typically seven networks and up to 100 computers in a luxury car. These control everything from the entertainment system and global positioning system (GPS) to the anti-lock braking system. Your wristwatch is quite possibly driven by a computer chip, and so are your DVD player, television, microwave oven, etc. Prior to 2010, the word "computer" conjured up machines that ranged from the room-sized "mainframe" computers large corporations used—to desktop computers we had on our personal desks in the office or at home. If you were truly "on the edge," you might even have had a laptop computer so that you could travel from desk to desk as well. In 2010, that all changed when Apple introduced the first truly successful commercial tablet—launching the iPad. Now computers travel with you as easily as a newspaper.
- **Smartphones:** Today's smartphones are more powerful than yesterday's desktop computers. They can run a bewildering array of applications (apps) that are so cheap that anyone can afford to have as many apps as he or she wants. Computing is now truly affordable. Smartphones are powerful computers with small screens. One of the most powerful capabilities of today's smartphones (and tablets) lies in their accelerometers and gyros. These are simple solid-state chip devices that can communicate your exact location (via GPS), the direction you are walking, the speed at which you are walking, and even your gait. From information

like this, it is possible to detect whether or not you are walking normally, in a furtive manner, have a limp, are in a hurry, or maybe that you are feeling ill.

Add to that the modern phone's ability to capture voice, images, and video; store large amounts of information; and access an infinite amount of data online, and you have a very powerful mobile device indeed. One of my favorite apps is a business card scanner—but I could just as easily use the phone to photocopy documents or secretly record a meeting.

- **Televisions:** Make no mistake, modern televisions are computers. If smartphones are computers with small screens, then TVs are computers with really large screens. They can run apps and communicate with the Internet just like any other computer—and the next breed of TVs will have cameras, too. They will watch you and record and report on your behavior every bit as much as you watch them.
- **Door Entry Systems:** When you swipe your corporate passcard through the door lock you are providing a lot of useful information: who you are, the date and time you pass through the door, your access rights (or authority), etc. By recording this information, it is possible to build up a history of your entries and exits to and from specific buildings or rooms, how long you spend in given areas, and your typical work patterns. However, many of today's door locks now use Radio Frequency Identification (RFID) or Near Field Communications technologies to detect the badge. These badges can also be detected by other wireless detection systems and can do more than just track your

ingress/egress via doors. They can also detect your movement around the building, the time you spend between point A and B, the time you spend in any given location (e.g., a specific desk or in front of a photocopier), or the time you remain motionless.

- **ATMs:** The ATMs we are all familiar with at our banks are just one example of card readers and automated interface devices. Square even makes a card reader that plugs into the headphone socket of your smartphone so that you can conduct credit card transactions on the move *(www.squareup.com)*. These machines are, of course, connected to the Internet and communicate a broad range of information regarding who you are, the transaction you just performed, where in the world you are, and when you used your cards.
- **Cameras:** Once the domain of professional and high-end amateurs, camera technology today is incredibly cheap. Modern plastic lenses and single-chip camera-sensing technologies now enable good-quality cameras to be embedded into everything from phones to ballpoint pens. Cameras are everywhere. For example, there are an estimated 4.2 million surveillance cameras in the United Kingdom (UK)—one for every 11 people in the country—most of them privately owned and operated.[7] The growing number of cell phone and computer cameras in our everyday lives dwarfs this number. What many do not realize is that, unless security restrictions are put in place, these cameras can be accessed and controlled without your knowledge. For example, it is possible to access a

laptop computer remotely and turn on its camera—without turning on the little green light to let the user know it is recording!

There are, of course, many other traditional uses of technologies that could be mentioned. Almost everything today has some form of internal computer chip, from our washing machines to the remote controls for our TVs, and all of them either connect, or have the potential to connect, to the Internet. Once connected, you have almost no idea what the devices are saying about you. Rather than expound further on the "normal" technologies we all know and recognize, it is more useful to identify some of the less likely ways we are using technology to enrich the world around us today.

- **Pets / Animals:** Pets and animals are valuable. Whether for emotional reasons, such as that we love our pets, or commercial reasons, such as the animals that constitute a farmer's livelihood, pets and animals are important to us. When things are important, we tend to want to track them. As a consequence, a growing number of people have tracking devices embedded under the skin of their pets so that they can locate them and track their movements. Farmers have cattle, sheep, and pigs barcoded or RFID-tagged and can track every aspect of their livestock from the date and location of their birth, the food they eat, the trucks they are transported on, and the name of the shelf stacker who placed the final product on display in the supermarket.

- **Trees:** There is a talking tree in Europe that has more Twitter followers than most of us reading this chapter.[8] Why? Because information is a valuable and useful resource. Everyone—from environmental scientists to city planners, botanists to hobbyists—finds the information that this tree can provide useful in a variety of ways. For example, the tree can tell you the temperature, wind speed, vibration from nearby traffic, CO_2 levels, the number of hours of sunshine, and a whole lot more—and all for the paltry salary of $0.
- **Shoes:** If trees can tell us about our surroundings, shoes can tell us about our activities. Nike was one of the first companies to link your shoes to the Internet, informing you (and anyone else you choose—and maybe do not choose) about your every move—literally. You (and the world) can track your level of activity, how vigorously you exercised, or how frequently you jog or run.

Today you are also actively encouraged to share your information via social media. Often this comes in the guise of a **competition** of some form: challenge yourself, compare yourself to your friends, etc. By doing so, of course, you allow even more information to be gathered about you, such as who you ran with, how often you meet up with people, or where you went for coffee afterward (just because you stopped running does not mean your shoes turned off!).

- **Cardboard Boxes:** Think about the number of items you own or use every day that came in a cardboard box. The chair you are sitting on, the cereal that you ate this morning for breakfast,

even the bill for the electricity you consume reading this document came in a cardboard box (OK, a very flimsy piece of cardboard disguised as an envelope, but you get the idea). We have barcoded packaging material for years, and for more expensive items we have also been embedding RFID chips; but we are now starting to use much cheaper, smaller tracking devices that need less power. It would now be possible to track every single box, package, or even a single document not only in terms of their location, but also the range of temperatures they have undergone, the degree of vibration they have experienced, and when/where they experienced those extremes.

- **Clothing:** Sensors are now starting to be embedded into the very clothing you wear. We have, of course, applied tags to clothing in stores to prevent theft for many years, but what if those tags were deliberately woven into the fabric of the material so that the seller could continue to provide added services once you had left the store? Wearable computing is not science fiction—it is here now and ranges from smart wristwatches to clothes that can monitor your health. Like the shoes above, this information can be streamed on a constant basis over the Internet unless we take specific steps to prevent it.

These are just a few of the myriad things we are connecting to the Internet. Even so, over 99 percent of the things in our world remain unconnected at this time.[9] We are entering an era of unprecedented innovation and change that will dwarf even the impacts

we saw with the introduction of the Internet itself. The question is, what do you do with power like that? Or perhaps more importantly, what could someone else do with that power?

ADVANCE TECHNOLOGIES

Let me start this section by stating up front that I am not suggesting that the examples I cite below are real—or will ever become real—but they could. My point is, technologies exist or are being developed that would allow the following to occur, and history has shown that more often than not, what is possible is usually done by someone—eventually.

As explained earlier, the addressing scheme of the Internet is truly mind boggling. It opens up the possibility of attaching a unique address—a unique ID—to almost everything we could possibly have an interest in. Once we can address something, we have the ability to monitor it, track it, and control it. Furthermore, some of the new technologies now entering the marketplace will add significantly to the list of things we can connect and control via the Internet. Let us look at a few of these.

3D Printing.

When I was growing up, there was a popular TV cartoon series called "The Jetsons." This futuristic space-age family had some amazing tools at its disposal, one of which was a wonderful kitchen appliance that could create almost anything the Jetsons wanted: food, drink, whole meals—even the cups and plates the meals were served on. That has now become a reality. 3D printers are here today, and for a mere $1,200 you could have one at home.

3D printers enable the creation of a wide range of objects locally, literally printed in three dimensions in front of your eyes. Think of a traditional 2D printer that prints one layer of the object you are creating. Then it prints another layer, and then another, until eventually you can stack each of these layers one on top of the other to create a three-dimensional object. That is what 3D printers do. They can print in a wide range of materials, including plastics, nylon, metals, etc. What is more, the printing be done in millions of colors and high definition to create high-quality, photorealistic objects.

Not only do these printed objects look highly realistic; they **work** too! In fact, 3D printers can create objects that we cannot easily produce using traditional manufacturing techniques. Think of a bicycle chain. Traditionally we manufacture each link and then connect them together using pins to create a circular chain. With a 3D printing method, the entire chain is printed as one complete object in which each link is separate from the others and free to move, just as it is in a traditionally manufactured chain, but there are no joints. The parts are not produced individually and then assembled into a chain; instead, all of the parts are printed together into a single working object. With traditional manufacturing techniques, the weakest links (no pun intended) tend to occur at the seams, or where we join different components together. With 3D printing, there are no seams or joins.

Perhaps the most amazing 3D printing materials of all are human cells. We now have the ability to print up to 22 different human organs, from the skin to beating heart cells.[10] Furthermore, this is now leaving academia and the experimental stage and entering mainstream use. In June 2011, the first-ever human

procedure was conducted when a 3D-printed titanium jaw was implanted into a woman's face.[11]

This technology will fundamentally change many industries. For example, why go to the store to pick up a replacement part for your dishwasher when you could simply download the blueprint and print it yourself at home? The home repair industry will be forever changed. Imagine a world in which you could download the recipe for that Asian cuisine you have been wanting to try and have the 3D food printer produce it for you—perfectly, every time. Better still, why not ask one of the world's leading chefs to takeover the production of the entire meal:

- Ordering the ingredients at the right time so they arrive as fresh as possible.
- Printing personalized place cards and menus.
- Controlling the 3D printing of the before-meal cocktails to the after-dinner mints.
- 3D printing custom napkin rings and wine glass name tags.
- Even controlling the music selection and lighting.

The potential is endless.

The above scenario is, of course, an appetizing image of haute cuisine on demand (OK—pun intended this time), but there can be more sinister and disturbing uses of this technology, too. 3D printing could just as easily be used to print weapons of all kinds—from working guns to bacteriological devices. While we could monitor the Internet for those downloading blueprints for an automatic handgun or ordering radioactive isotopes, we would be hard pressed to detect some of the no-less-concerning activities. For example, it would be difficult to tell from the readily available

data whether a person ordering raw materials to print metal objects was intending to make guns or garbage cans. As for the blueprints themselves, with modern graphics software, it would be trivial for a skilled individual to compose an appropriate blueprint from **innocent** parts or simply from scratch. What is more, even if we could detect some of these things, it may be too late by the time we detect them: 3D printing enables real-time production. In short, someone could download the blueprint and then produce the guns in the space of hours or minutes.

Designer Pharmaceuticals.

One further example comes from Proteus Digital Health, which has developed pills that have an embedded IP chip inside them *(www.proteus.com)*. These chips are activated by the stomach's acid when ingested by the patient and send a short communication signal to a band-aid on the patient's arm. This, in turn, communicates with the local wireless network to inform the doctor, relatives, or other caregivers that the medications have been taken. In this way, computer chips have been embedded into the pill to augment its capabilities. We go to elaborate lengths to scan people as they pass through airports and security gates—but do you know if the pill you have just taken for a headache is only dulling your pain or perhaps going to cause you a great deal of pain in the future?

Miniaturization.

Not so much "a technology" but "a technological trend," miniaturization is occurring across the entire technology landscape. Think back to the first mobile phones—or bricks, as we all called them. They were an

amazing technological advance that, for the first time, untethered us from our desks and forever changed the nature of our business and personal lives. Think of the first "portable computers." The first one I used was from Compaq and was appropriately called a "Transportable" computer, as it was the size of a small suitcase and weighed more than I could carry beyond a few steps from the car to the desktop.

By comparison, we all walk around now with more computing power in our wrist watches than we had in many desktop computers not so many years ago. My wrist watch today (I have a Nike Fuel) not only tells me the time, but also monitors my walking habits, reports on my progress, calculates the calories I burn, and logs it all to the Internet for me. The power of the devices we carry has increased exponentially, and their size, weight, power consumption, and cost have all plummeted. So where are we at today, size-wise?

Smart dust is an excellent example of miniaturization at its best. Smart dust devices are micro-electro-mechanical systems—miniature millimeter-size devices such as sensors that can detect a broad range of inputs, including light, magnetism, temperature, pressure, etc. They have only rudimentary "intelligence," but have the ability to communicate with each other and with their main wireless controllers. Think of them as a network of sensors distributed across a wide area—maybe woven into the carpet you are standing on, or embedded in the wallpaper or paint in your office. Each one could be reporting a simple piece of information that in and of itself is quite innocent, but collectively provides a great deal of information about the world around them. Imagine, for example, that your office is impregnated with just one simple type of smart dust—one that can record pressure. From that information I could deduce:

- Where you are standing;
- Which way you are facing;
- How much you weighed when you entered the office and how much you weighed when you walked out (Did you leave something or pick something up?);
- How long you stood facing the wall with a given diagram on it;
- If you walked with certainty or in a furtive manner;
- What was your reaction when a given person entered the room;
- How fast you moved; and,
- Whether you were wearing new shoes, etc.

Information is a very powerful thing.

To get a sense of just how small and finely tuned our sensing capabilities are, scientists at Penn State University have developed flexo-electronic sensors that can detect the presence of a single atom. Measuring whether or not you picked up a piece of paper and walked out of the office will be trivial by comparison.

As further proof of how small and almost invisible we can make things—and harping back to 3D printing—the Vienna University of Technology recently used a technology called two-photon lithography to produce a 3D-printed racing car that can be seen only by using an electron-scan microscope.[12] A 3D racing car carries a great deal of information, and detecting its existence would be virtually impossible if you did not know where to look (unless you happen to have an electron-scan microscope handy).

However, let us get smaller still. DNA sequencing is one of the truly amazing accomplishments of the past few years. From the discovery of the DNA double helix in 1953, we have progressed to the point that we can not only sequence the entire human genome of 3.2 billion base pairs, but we also can now engineer a DNA sequence to our specific requirements. The 3.2 billion pairs of four components (computers use only two states—zero and one) enable us to encode an incredible amount of information into a single DNA strand. DNA can easily be replicated by the trillions, even by amateurs in their home kitchens, image-encoding secret information into a DNA strand and injecting that into an animal, say a homing pigeon or even a human.

We are not finished yet. As Richard Feynman once said, "There is a lot of room at the bottom."[13] Miniaturization is set to continue in almost every field for a long time to come.

Augmented Reality.

This technology is real today. In fact, you probably have an augmented reality app on your smartphone right now, but it is going to get a whole lot more interesting over the next few years. Augmented reality simply refers to the ability to add additional information (append) to the world around us (reality). The simplest example can be seen in a smartphone app such as "Around Me." This app allows you to see reality through the phone's camera (you simply see what the camera is seeing), but with additional information overlaid on top of that image—for example, to show the name, address, phone number of, and distance to the nearest coffee shop. As you rotate yourself and your smartphone camera around, you see the various coffee shop data pop up on the phone's camera image.

As another well-known example, fighter pilots have had Head Up Displays (HUDs) for many years; flight information is projected onto the helmet visor of the pilots so that they can see key information while continuing to look through the visor at the sky around them. The Armed Forces, of course, have been experimenting with augmented reality solutions for many years. Modern soldiers receive key information that can be superimposed on their night vision goggles, or "over the hill" information pertaining to enemy positions and armory placements. Augmented reality is increasingly showing up in nonmilitary areas as well. Modern cars are now appearing with HUDs showing key driving information, such as speed, superimposed on the windscreen of the car so that drivers do not have to take their eyes off the road.

This is a powerful concept. We can add additional information—any information—to enhance the world around us. Consider therefore the range of information at our disposal in today's electronic world, and imagine how it could be used to augment our lives. Satellites constantly scan every square inch of the planet on a nonstop basis—there is nowhere you can hide today. Wikipedia holds over 26 million articles on every conceivable topic, in 286 languages by over 100,000 active contributors.[14] Google's mission is to "store the world's information."[15] There is almost limitless information at our disposal, much of it available for free, and all of it could be used to augment the world around us.

Google Glass[16] is one of the exciting new technologies about to be made available to the world. Through this small pair of spectacles, somewhat reminiscent of Geordi La Forge's visor from *Star Trek,* Google will be able to project information so that the wearer, and only the wearer, of the glasses can see it. Imagine your

next customer meeting where key product information or customer order history data are projected into your vision only.

While we are on the topic of *Star Trek,* and linking back to sensors for a moment, in January 2012, Qualcomm announced a $10-million X-Prize Tricorder project.[17] Imagine a few years' time when your doctors have the ability to project all of your vital signs, such as blood pressure, temperature, etc., onto their glasses. Alongside your information could be information about specific drugs or treatments, along with the collective guidance from the world's specialists on your specific condition.

Of course, those are the good examples. We could equally envision terrorists using the same technologies to share up-to-the-minute information pertaining to security guard positions. This key information might be used to compromise the person you are speaking with—or maybe to convince that person you are someone he or she should trust, or even identify which of the security guards is feeling sleepy or emotional and is most susceptible to distraction.

High Fidelity.

On top of this ability to share unlimited information in real time and in a secure and/or secret manner, you also have to consider the fidelity of that information. Graphic displays and image-processing software today can produce results that are indistinguishable from reality in all but the most rigorous laboratory testing. Using a battery of sophisticated sensor techniques from light sensors and infrared sensors to ultrasonics and x-rays, we can reproduce materials with amazing accuracy. An individual's voice can be captured, analyzed, and sequenced such that we can cre-

ate audio files that are perfect in every detail. In short, we can make "you" say anything we want.

We even have technologies today that can model human behavior and mannerisms. For example, Cisco Systems has software that can monitor the conversations between a call center operator and a customer and indicate whether the customer is angry, frustrated, or elated. We can produce computer avatars that display human emotion in terms of their body language, facial expressions, and voice intonation.

Of course, 3D is commonplace today, and with the new 4K (and soon-to-be-released 8K) ultra-high-definition TVs and display with super-vivid Organic Light Emitting Diode, our ability to project highly detailed, highly realistic images is incredible. Next time you see one of these devices, look closely into the picture, and you may just see some information hidden deep within. For a sense of how imaging technology today can store a lot of information, take a look at the Gigapan high-resolution panoramic images *(www.gigaspan.com).* For less than $1,000, you could create an image that allows you to read the headlines of someone reading a newspaper on the steps of the U.S. Capitol Building from the Lincoln Memorial.

In short, it is getting harder and harder to tell what is real and what is computer-generated.

WHAT CAN WE DO?

It is clear from the preceding examples that technological advances offer us some amazing opportunities, but also present us with some significant challenges. The most important thing to remember is: **you cannot stop**. This point is so critical, I want to repeat it. You cannot afford to stop using these technologies or try to avoid them. Your adversaries will most definitely em-

ploy every technology they can obtain and use them in the most imaginative ways possible. Whether you represent an individual company or an entire country, you cannot afford to allow your competitors or enemies to outmaneuver you by using technologies you choose to avoid. We must not be frightened into inaction.

Security and privacy, of course, are very serious issues, and they must be treated as such. Good security needs to be architected into your world—it is not a bolt-on afterthought. This includes everything from the hardware and software you use to the processes and procedures your employees follow. Choosing your technology solutions is a critical step in your overall security strategy. Low-cost solutions may prove to be very expensive in the long run when critical information is leaked due to inadequate security capabilities of your information and communications technology infrastructure. Furthermore, it is not simply the security capabilities of any one piece of technology that counts, but rather the overall security **architecture** of your technology infrastructure. As the saying goes, you are only as strong as your weakest link.

Most corporations today are consolidating their technology infrastructure down to a few key strategic partners who have the breadth and experience to help them build a cohesive, holistic architecture that addresses security as a foundational design element. From a security standpoint, it is no longer safe to build a patchwork quilt of low-cost technologies that cannot be linked together to form a tight, secure platform for your critical business functions. Technology is no longer a small back-office capability reserved for a few specialists in finance—your technology infrastructure is the very foundation of every aspect of your company, and it has to be secure.

Chief among your technology concerns should be the corporate network. It carries **all** of your information—voice, data, video, sales, customer information, and security codes—every single piece of information your company runs across your network. A secure network can not only protect your company from security breaches while transporting information across the network, but can also provide critical security controls to all of the devices connected to the network. For example, you might use your network to detect aberrant behavior or malicious messages at the edge of your network and prevent such activities from entering your company. Building a secure network should, therefore, be one of your highest priorities.

Choose your technology partners well. Work with them to develop a robust, holistic technology platform that is founded upon a highly secure network with security designed in from the outset as an architectural capability. This is an imperative for both governments and corporations.

ENDNOTES - CHAPTER 4

1. Ray Kurzweil, "Ray Kurzweil Defends His 2009 Predictions," *Forbes*, March 21, 2012, available from *forbes.com/sites/alexknapp/2012/03/21/ray-kurzweil-defends-his-2009-predictions*.

2. Dave Evans, "The Internet of Things," Talk2Cisco, July 27, 2010, available from *ustream.tv/recorded/8552217*; see also Jamie Beckett, "Cisco Futurist Discusses Internet of Things, Tech Predictions, More on Talk2Cisco Broadcast," Cisco Blogs, July 30, 2010, available from *blogs.cisco.com/news/cisco_futurist_discusses_internet_of_things_tech_predictions_more_on_talk2c*; see also Telefoníca I&D 2011 Report.

3. Cisco Systems, Inc., "Cisco Visual Networking Index: Global Mobile Data Traffic Forecast Update, 2012–2017," February 6,

2013, available from *docslide.us/documents/cisco-visual-networking-index-global-mobile-data-traffic-forecast-update-2012-2017.html*, p.1.

4. See "Internet Live Stats," available from *internetlivestats.com/one-second/#email-band*.

5. "History of IBM Magnetic Disk Drives," Wikipedia, available from *https://en.wikipedia.org/wiki/History_of_IBM_magnetic_disk_drives.*

6. Kurzweil, "Ray Kurzweil Defends His 2009 Predictions"; see also Ray Kurzweil, "The Law of Accelerating Returns," March 7, 2001, available from *kurzweilai.net/the-law-of-accelerating-returns*.

7. David Barrett, "One Surveillance Camera for Every 11 People in Britain, Says CCTV Survey," *The Telegraph,* July 10, 2013, available from *telegraph.co.uk/technology/10172298/One-surveillance-camera-for-every-11-people-in-Britain-says-CCTV-survey.html*.

8. Steven Erat, "*Steven Erat's Blog | TalkingTree.com*," available from *talkingtree.com/blog/*.

9. Cisco Systems, Inc., "Cisco Consulting Thought Leadership," available from *cisco.com/web/about/ac79/index.html*.

10. Susan Young Rojahn, "Artificial Organs May Finally Get a Blood Supply," *MIT Technology Review,* March 6, 2014, available from *technologyreview.com/news/525161/artificial-organs-may-finally-get-a-blood-supply/*.

11. "Transplant Jaw Made by 3D Printer Claimed as First," BBC News, March 8, 2012, available from *bbc.com/news/technology-16907104*.

12. Clay Dillow, "Video: Super High-Res 3-D Laser Printer Prints at Five Meters Per Second," *Popular Science*, March 12, 2012, available from *popsci.com/science/article/2012-03/video-super-high-res-3-d-printing-technology-sets-speed-records*.

13. "There's Plenty of Room at the Bottom," Wikipedia, available from *en.wikipedia.org/wiki/There's_Plenty_of_Room_at_the_Bottom*.

14. See Wikipedia, available from *wikipedia.org*.

15. See Google, Company Overview, available from *https://www.google.com/about/*.

16. See Google Glass, available from *google.com/glass/start/*.

17. "Create a Star Trek Tricorder and Win $10 Million," TechJournal, January 10, 2012, available from *techjournal.org/2012/01/create-a-star-trek-tricorder-and-win-10-million/*.

CHAPTER 5

BIG DATA CHALLENGES, FAILED CITIES, AND THE RISE OF THE NEW 'NET

Jeff Boleng
Colin P. Clarke

INTRODUCTION

Approximately 40 percent of the global population currently uses the Internet, with that figure only expected to grow.[1] Indeed, by the end of 2015, both China and the Philippines will have outpaced the United States in Internet and social media usage on a percentage basis.[2] More than 1.35 billion people use Facebook, roughly equivalent to China's entire population and a significant portion of the world's.[3] Not only has the number of people using the Internet increased, but also the sheer number of devices that people use to access the Internet is also increasing. Now, more than ever before, these devices are becoming part of an "Internet of Things," which is, in turn, increasingly connected to cyberspace.

As the world moves into an era of big data, numerous opportunities present themselves to analyze emerging challenges in the international security environment. One of these challenges is dealing with the proliferation of urban slums. The world population topped 7 billion in October 2011 (7.125 billion as of 2015) and is predicted to be around 8.3 billion in 2030,[4] with well over half the population living in Asia and Africa[5] and over 50 percent living in urban areas.[6]

In 2012, the GSM Association reported that over 6.8 billion Subscriber Identity Module (SIM) cards have been issued, with 5.9 billion actively assigned to human users.[7] Many of these mobile subscribers live on an average of $2 per day, spend up to 2 months' salary on a mobile phone, and pay up to 10 percent of their income for basic connectivity.[8] To put this in perspective, imagine an American consumer spending $600 per month for a mobile phone plan and up to $8,000 to purchase a mobile device (based on a reported median annual income of $50,000).[9] Furthermore, 70 percent of all phone shipments worldwide are feature phones,[10] and the most popular phone in the world is the Nokia 1100 series feature phone.[11] Finally, mobile phone penetration rates in countries with three of the most prominent underdeveloped city neighborhoods (from here on referred to as slums)—Kiberia Nairobi, Kenya; Mumbai, India; and Jakarta, Indonesia—are 74 percent, 76 percent, and 92 percent, respectively.[12] In fact, nearly 62 percent of the population of Mumbai reportedly lives in slums.[13] Clearly, even people who live in relative poverty value the connectivity and services mobile devices provide.

In an example of what the National Intelligence Council (NIC) labels a "tectonic shift," by 2030, the world's urban population will stand at approximately 4.9 billion of a projected total global population of 8.3 billion—roughly 60 percent. Much of this growth is expected to occur in China, India, Bangladesh, Brazil, the Democratic Republic of Congo, Nigeria, Pakistan, and other cauldrons of ethnic and religious strife.[14]

Indeed, according to Strategy Analytics, by the end of 2012, there were over 6 billion mobile phone subscriptions. This means that today, not to mention the future, we are living in a hyperconnected world.

Everyone is constantly communicating, but not always in a way that we can understand or that makes sense. For all the good that this increased connectivity has wrought, it also portends growth in a more nefarious side—the dark underbelly of society that leverages the convenience and anonymity of mobile phones for sordid purposes such as human trafficking, drug smuggling, and the financing of terrorism.[15] Mobile phones have vastly increased connectedness on multiple levels, between coastal cities and their hinterlands, between cities, and between domestic populations and global networks like refugee and diaspora populations living abroad.[16]

In essence, just as certain technologies enhance the exchange of information that can promote health and well-being, good governance, and foster collaboration, so too can they facilitate a range of criminal activity. Meanwhile, though, if the method of communication being used by these criminals is properly understood, it can be tracked, translated, analyzed, and eventually used as a critical component of multi-intelligence fusion.

Urban areas that are plagued by overcrowding and high crime are the most likely candidates to prove problematic for law enforcement authorities, since these areas will also be hyperconnected, retain the ability to spoof and maintain anonymity, and be potentially unhooked from the wider World Web. Since mobile phones can be used for a range of illicit purposes, from communicating or organizing mass attacks to detonating improvised explosive devices (IEDs), the challenges of tracking these devices are manifold. Consider the following statistic: between January and August 2012, 14,733 mobile phones were reported stolen in the city of Karachi, Pakistan (and that is simply

the number reported, so the actual number stolen is likely much higher).[17] Unregistered phones are hard enough to track. The challenge is compounded when these phones are stolen and end up in the hands of unknown users.

This data leads to the following conditions/conclusions:

- A majority of the population lives in urban areas, with significant numbers living in slums. Both these conditions are expected to increase in the future.[18]
- A majority of people, even in the developing world, have mobile phones, resulting in hyperconnectivity.
- The majority of the mobile phones in the world are feature phones, as opposed to smartphones. This inevitably makes them harder to track and attack.
- Literacy rates lag cell phone penetration rates, especially in slum environments.[19]

These conditions have created a new type of information environment. Information generated and consumed on these mobile devices is largely composed of multilingual text jargon, voice, images, and video. The pace of information creation and sharing in this information environment is staggering and increasing. Current capabilities of large-scale data analytics are heavily text-centric. As the world's population becomes more urban, as slums increase in size and number, and as information flow and news reporting continue to democratize, these urban environments and slums become a natural center of gravity for a crisis, natural disaster, or conflict. Future operations—whether humanitarian aid to civil authorities or mili-

tary operations—increasingly will be centered in these environments. The United States must begin to focus on the challenges presented by this new information environment in order to be able to gather intelligence from, operate in, and exert influence through this new 'Net.

SOCIOECONOMIC CHALLENGES OF SLUMS

Writing in the late-1700s and early-1800s, British scholar Thomas Malthus centered on the importance of demography and the political effects of poverty and resource deprivation. Today, the term "Malthusian" is synonymous with the feral cities of the near future—fetid, overcrowded, squalid, tribally governed, and dangerous. This is the place where life in 2015 still is, as once described by Thomas Hobbes, "short, brutish, and nasty," or, as the journalist Josh Eells remarked when visiting Lagos, Nigeria, in May 2012, "a Dickensian conurbation of overcrowded slums and nonexistent services."[20]

Failed and weak states are plagued by corruption, which attenuates the rule of law and makes police and border security officials more prone to bribery—increasing the porosity of borders and thus facilitating the flow of illicit goods into and out of the territory. Other challenges faced by failed cities are too numerous to list, but these include at least the following: insurgency, terrorism, energy insecurity, climate change, resource deprivation, brain drain, transnational crime, corrupt patronage networks, religious extremism and radicalization, piracy (both digital and maritime), cyberwarfare, weapons of mass destruction, global economic slowdown, and the spread of pandemics and disease.

From Mumbai to Mogadishu and from Caracas to Kinshasa, failed cities present a host of political, social, economic, and security challenges to any entity attempting to intervene in these environments. Weak cities contribute to weak, failing, failed, and collapsed states; which, in turn, then become a haven for terrorists and insurgents, nuclear proliferators, and transnational criminal organizations that engage in money laundering, kidnapping for ransom, counterfeiting, and the smuggling and trafficking of humans, weapons, and narcotics.

Case Study: Karachi, Pakistan.

While much has been made of failed states, the hand wringing curiously has not extended to a similar concern over the plight of failed cities. However, without question, failed states are made up of failed cities, towns, and villages. In the mega-slums of the near future, the challenges are herculean. For evidence, one need not look any further than the city of Karachi, Pakistan.

Karachi is a city of 23.5 million people with an average growth rate of 4.9 percent a year, the highest of any of the top 28 most populous cities in the world. Sometime in the early- to mid-1990s, the Pakistan Army was deployed to this sprawling megacity in Pakistan's Sindh Province to stabilize a city that had morphed into a hub of terrorist and gang activity. The arrival of Pakistan's Army transformed the city into an urban battlefield during Operation CLEAN-UP, fought in the streets and back alleys of Karachi. Unable to quell the violence, Pakistan's Army was replaced by an elite paramilitary ranger unit, which fought door to door against a panoply of criminals,

terrorists, and violent political parties, some of which used rocket launchers against the security forces.[21] Karachi was soon paralyzed by violence as the city quickly became ungovernable. Ordinary citizens took law enforcement into their own hands as the violence spread throughout the area.

Now imagine if a coalition comprised of Western nations is forced to intervene in such an environment. Never mind that Pakistan is a nuclear-armed nation, though that fact alone is sobering enough. Even for the most competent and capable of security forces, Karachi poses a nightmare of an operating environment. This is a city of unauthorized settlements (known as *katchi abadis*), rampant pollution, and daily blackouts that last for hours on end.

Violence is a fact of life, with bombings, kidnappings, riots, and murders the rule, not the exception. In 2009 alone, 1,747 people were killed in Karachi.[22] Following the U.S. invasion of Afghanistan, Karachi was a receiving station for al-Qaeda fighters and served as a rear base for militants to organize and plan attacks back across the border. Subsequently, it has emerged as a hub for insurgents from Tehrik-i-Taliban, a militant outfit fighting the Pakistani state.[23]

Tehrik-i-Taliban is an example of a nonstate actor that includes an array of adversaries, such as terrorists, insurgents, militias, warlords, transnational criminal organizations, and violent drug trafficking organizations. Some scholars have labeled this phenomenon BlackFor, or Black Force, defined as a "postmodern form of societal cancer," and as "a confederation of illicit non-state actors linked together by means of a network of criminalized and criminal (narco) cities."[24] Components of BlackFor are likely to be intertwined inextricably with, and indeed aided by, symbiotic

relationships with Mafia states. In these kinds of states, government officials enrich themselves and their cronies, while utilizing the "money, muscle, political influence, and global connections" of crime syndicates in order to pad their pockets and remain in a position of power.[25]

Where governments suffer from capacity gaps, legitimacy deficits, and functional holes, alternative sources of governance will fill the void. One form of alternative governance that often emerges in response to central political collapse, in which a government either cannot or will not provide its citizens with basic services, is the warlord. Warlords lead armed bands of up to several thousand fighters, hold territory (this could be as small as several city blocks), and act both financially and politically in the international system without interference from the state in which they are based.[26] These individuals flourish where cultural identities are fragmented, political space is in flux, and the absence of traditional governance mechanisms is apparent.[27]

The urban slums likely to become operational environments of the next decade are extremely poor, with high levels of unemployment and low levels of literacy. These cities also suffer the effects of "youth bulges" and "brain drain," which exacerbate the levels of inequality between the "haves" (landowners, retired military, and those with connections to the ruling elite and patronage system) and the "have-nots" (everyone else). The result is a legion of marginalized, frustrated, angry youth with the mobile connectivity to organize for violence and to do so surreptitiously. This same marginalized youth is likely to survive by participation in the illicit economy, in which various flavors of crime—from the smuggling and trafficking

of arms, humans, drugs, organs, endangered species, etc., provide the only means of income for an otherwise neglected subpopulation. In this world, a culture of lawlessness means that life is cheap, and everything is for sale. A decaying social fabric furthers the gap between expectations and opportunities and makes individuals prone to recruitment into terrorist groups and criminal organizations. Those who can afford it will outsource security to private firms. This will encourage a return to the dark ages of fiefdoms and accelerate the erosion of the Westphalian state, as the pendulum swings back in the other direction—thus encouraging a backlash against the concept of government as it currently exists.

Case Study: Mogadishu, Somalia.

Following a decade of insurgency from 1980 through 1991, Somalia began its rapid descent into state collapse, as warlords besieged the country's capital, Mogadishu.[28] Warfare between clans and subclans and the proliferation of violent nonstate actors—warlords, terrorists, militias, gangs, and pirates (to name but a few)—consumed the city and transformed Mogadishu into one of the most lawless zones of urban terrain in the world. Once the former dictator, Siad Barre, finally had been driven from the country, Somalia degenerated into "an orgy of uncontrolled violence," characterized by ethnic cleansing. The cities of Mogadishu, Baidoa, and Kismayu soon became known throughout East Africa as "the triangle of death."[29]

In some of the most odious violence in the contemporary era, warlords massacred orphans, systematically raped women from rival clans, slaughtered clan

elders, killed and mutilated pregnant women, indiscriminately bombed neighborhoods with mortars and rocket-propelled grenades, and used women and children as human shields.[30] Young men roamed the country wearing shirts that read in English, "I am the Boss," which came to reflect the stark reality that, in essence, every Somali was his or her own boss, which meant security for nobody and violence for all.[31] The Bakara Market in Mogadishu became known as one of the world's busiest bazaars for the exchange of arms, weapons, and ammunition.

Somalia has been without a functional central government since 1991, which is to date the longest recorded tenure of state collapse in post-colonial history.[32] The country has not held a civilian election in 44 years.[33] For most of the 2000s, Somalia held the dubious distinction of being ranked number one on *Foreign Policy* and the Fund for Peace Failed States Index. At the time of state collapse in 1991, about one-third of Somalia's population (estimated at between 8 and 10 million people) was internally displaced.[34] Somalia's economy remains among the poorest in the world, while its human development indicators also rank among the lowest.[35]

Failed Cities Make Failed States.

In the early-1990s, Mogadishu became the scene of violent looting and a humanitarian catastrophe, compounded by a lack of food, electricity, and clean water. Clan warfare, the control of resources, and the absence of governance exacerbated the zero-sum mindset of most Somali political actors.[36]

On December 9, 1992, the United States provided a quick reaction force to a peace enforcement mis-

sion dubbed Operation RESTORE HOPE, intended to bring humanitarian relief to Somalia. In the summer of 1993, following continued attacks on United Nations (UN) peacekeepers and a U.S. military police convoy by Mohammed Aideed's Somali National Alliance (SNA) militia, President Bill Clinton deployed Task Force Ranger to Somalia.[37]

Upon entering Mogadishu, U.S. forces used fire and maneuver, teams and squads leapfrogged one another, and infantry dismounted, moving on foot to provide the convoy with full cover.[38] Combatants routinely disguised themselves as civilians, hiding their weapons and then ducking behind cars and buildings before re-emerging to fire bursts of automatic gunfire from windows, doorways, and alleys. Somali militiamen constructed roadblocks, burned tires to alert others, and set up a defense covering 18 separate sectors across the city, connected through a primitive radio network. Within sectors, the communication method was even simpler. Gunmen with megaphones implored civilians to "Come out and defend your homes!"[39]

The Task Force, which included some of the most elite soldiers in the world—U.S. Army Rangers—became disoriented while attempting to navigate through the city's terrain. A dearth of intelligence about Mogadishu's structural conditions, street widths, and lack of clear landmarks for navigation contributed to soldiers getting separated from each other.[40] The battle made famous by the book (and subsequent movie) *Black Hawk Down* resulted in the death of 18 Army Rangers.

In their monograph *Street Smart: Intelligence Preparation of the Battlefield for Urban Operations,* Jamison Medby and Russell Glenn lay out some of the most

significant challenges posed by urbanized terrain, including underlying terrain, buildings, infrastructure, and, of course, people.[41] Urban areas, especially slums, are congested, polluted, decrepit, and packed with a dizzying blur of pedestrians, motorists, buildings, windows, streets, alleys, and tunnels. In dense urban environments, counterinsurgent or counterterrorism forces need to be prepared to respond to myriad challenges, ranging from counterfire radar to radio and global positioning system degradation.[42]

Knowledge of culture and people is a critical enabler in any urban operation. The Battle of Mogadishu between U.S. troops and Somali militiamen saw civilians protecting Somali gunmen by using their own bodies as shields. This posed a tactical challenge for U.S. troops, who were constrained by rules of engagement and the law of land warfare.[43]

The world has grown infinitely more complex since 1993. Over the past 2 decades, technology has proliferated with the spread of globalization and the broadening of access to previously isolated areas. While the U.S. military is certainly more technologically advanced than it was during the Battle of Mogadishu, so too has the patchwork of violent nonstate actors become adept at utilizing mobile phones, the Internet, and social media.

Somalia: 20 Years after the Battle of Mogadishu.

Of all the many challenges facing Somalia today, perhaps the most pernicious is the rise of Harakat al-Shabaab al-Mujahideen (aka Shabaab, or "The Youth"). Shabaab is a radical fundamentalist faction that split off from the Islamic Courts Union, which itself was the outgrowth of al Itihaad al Islamiya.[44] Although radical

Islam does not have a rich history in Somalia, over the past decade or so, the country has fallen within the "orbit of Wahhabist preaching" which, in turn, has led political Islam to become ascendant.[45]

Shabaab actively recruits Somali-Americans from the diaspora to come and fight with the insurgents in Somalia. In July 2010, Shabaab exploded bombs among revelers watching a World Cup soccer match in Kampala, Uganda, killing 74 people and injuring scores more.[46] The group has also claimed responsibility for horrific attacks such as the September 2013 Westgate Mall attack in Nairobi, Kenya, and the April 2014 Garissa University College attack in eastern Kenya. Religious extremists regularly target foreign aid workers and journalists in Mogadishu. Furthermore, for most of the last 2 decades, kidnapping has become endemic in Mogadishu, and those with wealth, family connections, or an employer thought to have deep pockets and an inclination to pay became prime targets.[47]

By 2005, Shabaab numbered somewhere around 400 fighters and expanded when Ethiopia invaded Somalia in late-2006.[48] Throughout 2007 and 2008, employing a range of ambush-style attacks, IEDs, assassinations, and bombings, Shabaab militants fought the Ethiopian military to a standstill.[49] The Ethiopians withdrew in early-2009. The fighting between Shabaab and Ethiopian forces, complemented by U.S.-backed militias, became known as the "dirty war," since both sides chose to eschew previously held norms regarding violence. Shabaab introduced suicide bombing to Somalia for the first time, while the Ethiopians responded by using white phosphorous bombs to clear out entire neighborhoods.[50]

Shabaab poses even more of a threat than Aideed's militia did back in 1993. Unlike the SNA, Shabaab relies heavily on digital video and social media to convey its messages, transmit propaganda, recruit new fighters, and counter security force interpretations of events.[51] Having to contend with a network composed largely of feature phones with intermittent connectivity sharing nontraditional, culturally specific text data and large amounts of non-text data would certainly pose immense challenges to security forces operating in Mogadishu. These challenges are in addition to the many other challenges already present when one is dealing with densely populated, urban terrain.

The case studies of Karachi and Mogadishu are intended to demonstrate the complexity of operating in failed cities and how technology and demographics serve to compound the challenge. Coupled with the threat of the diffusion of violent ideologies like that espoused by the Islamic State in Iraq and Syria (ISIS); and the convergence, in some cases, between terrorism, insurgency, and transnational organized crime, the operational environment is evolving rapidly and not in a manner favorable for the United States and its allies. The rise of the "New 'Net" will only further exacerbate these threats.

TECHNOLOGY CHALLENGES OF THE NEW 'NET

The technology challenges presented by the rise of this new network are considerable. Chief among them are multimedia content, multilingual content, and transient nature. As noted earlier, the data content produced, consumed, and exchanged in this new network largely will be voice, images, and video. Signifi-

cant content will also be exchanged as traditional text via short-message service, but it will be multilingual slang and leetspeak.[52] The nature and volume of the content place huge demands on U.S. analytical and intelligence capabilities for understanding and sense-making. We must expand research in automated methods for multimedia context mining and multilingual text understanding. Additionally, we must have the ability to deploy rapidly and focus systems with these capabilities in previously unforeseen locations around the globe.

Added to the challenge of determining the meaning and relative context is the transient nature of the network itself, both in terms of connectivity and participation. Reliance on battery power and the difficulty of recharging phones in slums where infrastructure is fragile, expensive, and often nonexistent have created an environment in which users power off phones when not in use. This creates a highly dynamic network with mobile devices disappearing from one location and reappearing in another. Tracking mobile devices becomes much more difficult, and the time windows available for fixing a device or gathering data from it are small and rare. New techniques for tracking and intercepting data from intermittently connected devices should be made a priority.

The urbanization of the population and increasing poverty have created numerous slums around the globe. These areas are dominated by hyperconnectivity and a new type of electronic network that has not been seen before. This new 'Net does not resemble the Internet and World Wide Web, where we are accustomed to operating our cyberoperational and intelligence forces. It creates new challenges of multilingual, multimedia content that is highly intermittent and

transient in nature. We must act to increase current understanding and define new areas of research that will provide us with the ability to operate effectively in these environments. We must be able to gather intelligence rapidly and apply automated means to add context and connections to this vast sea of largely nontextual data. Furthermore, we must ensure that our forces are able to leverage their technological capabilities even in locations that do not share the same infrastructure or resources they have become accustomed to or depend on.

The Challenges of (Really) Big Data.

As of 2012, 2.5 quintillion ($2.5x10^{18}$) bytes of data were created every day.[53] A quintillion bytes is referred to as an exabyte. It is estimated that there are approximately 10 terabytes ($10x10^{12}$) of data in the print collection of the Library of Congress, and all the words ever spoken by human beings may account for approximately 5 exabytes ($5x10^{18}$).[54] Even if these are rough estimates, the world creates about as much data every 2 days as the entirety of humanity has ever uttered, or about 50 million times the Library of Congress print collection every day. Additionally, the rate at which data creation increases is more than linear. According to the IDC Digital Universe Study, unstructured data will account for 90 percent of all data created over the next decade.[55]

How big a challenge is it to make sense of this magnitude of data? Even if we take out the 12 terabytes ($12x10^{12}$) of tweets created each day, we are still left with 2.499988 exabytes of something else. The majority of these data are voice, images, and video. Consider the challenge of just determining the

semantic meaning of the data in Twitter. From a data standpoint, much of this is exchanged via images and the growing use of 6-second Vine videos. However, as of May 2015, there were on average 6,000 tweets per second, which corresponds to over 350,000 tweets per minute, 500 million tweets per day, and around 200 billion tweets per year.[56] In order to analyze only the textual data in real time, we would need to process far more than 4,000 to 6,000 tweets per second. The current state-of-the-art algorithms can accomplish topic modeling on roughly 500 to 1,000 tweets per second; while sentiment analysis is somewhat more resource demanding, resulting in 100 or so tweets per second on a commodity processor. Scaling of these techniques to make use of multiple cores or multiple computers is not always obvious or possible with current algorithms. This performance can scale to handle the current volume of tweet texts, but may not scale to much more complex and longer text artifacts such as emails, etc. which require significantly more memory and processing to analyze. Additionally, the use of images and videos in tweets is growing substantially, and the demands to analyze these are not included here.

Let us turn our attention to the huge magnitude of leftover data. As a back-of-the-envelope calculation, assume these data are composed of roughly one-third each of voice, images, and video. Furthermore, assume a compromise data rate for voice and music encoding of 128 Kilo-base pair (common size images (1280x1024 resolution at 24 bits per pixel jpeg, or approximately 250 kilobytes per image), and standard definition television video (3.5 mega-base pairs). With these sizes, we will need to be able to process about 1.6 million years of conversation, 3 trillion images, and 60,000 years of video every day! These are extremely rough estimates, but even if they are off by multiple

orders of magnitude, the world is creating really big data. As fast and ubiquitous as modern-day computers have become, with current techniques, there is not enough computation for topic modeling and semantic analysis of this magnitude of unstructured data.

Of course, we could greatly reduce the amount of data processing required by focusing our efforts on the areas that may be most volatile. But where in the world are these places? We could focus on slums and developing countries. These areas produce relatively lower rates of data than industrialized countries. On the other hand, these areas are densely populated, and we have already seen that mobile devices are proliferating in every segment of society and the world. These mobile devices are all capable of producing audio, photos, and video at quality rates much higher than those considered above. Consider also that groups desiring to gain global influence will likely operate and strike in wealthier industrialized cities and countries.

What must be done, at least from a technological standpoint? First, mechanisms to access the data produced by mobile devices must be developed and expanded. This raises numerous societal and privacy concerns that are beyond the scope of this chapter. However, there will be instances in which access to mobile device data will be absolutely required. Second, we must increase investment in the research and development of algorithms and techniques to process unstructured data. The volumes of data being produced are beyond the capacity of any organization to analyze manually. We must be able to perform topic modeling and semantic and contextual analysis of huge amounts of streaming text, voice, image, and video data in near-real time to focus our attention rapidly on emerging events that could threaten our national interests around the world.

Making Progress with Data Analysis.

Through our engagements with public safety personnel and experimentation with publicly available social media data, we have discovered four types of interaction with data analysis to aid intelligence gathering in support of public safety and military operations. We identify these types of interaction:

- Forensic Analysis;
- Reactive Intelligence;
- Predictive or Actionable Intelligence; and,
- Preventive Intelligence or Influence Operations.

Recorded and archived data can be used in support of intelligence operations by applying data-mining techniques to the corpus of historical data in a matter informed by records of actual events. It is possible to recognize trends in disparate data channels, which can be used as indicators and warnings of the events that occurred. This level of analysis facilitates the development of algorithms and rules that can be applied to streaming real-time data. Additionally, archival data can be used as training and evaluation sets for machine-learning algorithms, which can also be used as computational filters for streaming data.

The preparation and training of the system through forensic analysis of the data have led us to a system that facilitates reactive intelligence. By this, we mean that real-time intelligence is gathered and analyzed as the situation is unfolding. This information is invaluable in informing reaction teams about the details of a situation while the teams are still en route to respond. By the time quick-reaction elements are in place to engage the situation, they

already have been informed of key details about the location; quantities of hostile, neutral, and friendly participants; terrain outlet; and other essential details to give them an information advantage over the adversary.

Our current endeavor is to refine our forensic and reactive capabilities continually through experience and more fine-grained training of the machine-learning algorithms. Employing our techniques in a wider variety of events and drawing from a more diverse set of available public and social media feeds, we are gaining invaluable experience that we are confident will lead to a predictive intelligence capability. A representative scenario with which we have experience is analyzing large amounts of social media data at a multiday music festival attended by 60,000 to 80,000 people. The initial system capabilities include topic modeling and sentiment analysis of Twitter streams related to the event. Based on the automated alerts and trends in the data, further manual analysis of associated Instagram, Vine, and selected publicly available Facebook data has proven promising in the pursuit of a predictive intelligence capability.

Perhaps most controversially, consider the ability to influence situations through the creation of data. In the near term, this implies the manual creation of information in an attempt to shape behavior. However, it is conceivable that a variant of the same machine-learning algorithms used to recognize a volatile event could also be used to inject orthogonal data automatically to inform the crowd or population in an opposite or calming manner. This capability can be understood as preventive intelligence when applied to situations involving groups of U.S. citizens. Strong safeguards must be in place to ensure that only factual informa-

tion is disseminated. In the Department of Defense context, this is more commonly known as "information" or "influence operations," and a much wider variety and array of information can be used to shape responses. If the data streams indicate the planning of a possible threatening event, one response mechanism is to deploy a significant and visible monitoring force to the suspected area in an attempt to dissuade the would-be perpetrators from carrying out their plan. In another context, extemporaneous incidents can expand at amazing time scales due to the rapid proliferation of social media and mobile data. As the ability to develop and efficiently analyze massive amounts of data in terms of context and semantics matures, it will also be possible to generate contextual and semantically accurate data to influence alternative behaviors in large numbers of data consumers.

As previously noted, efforts to date have focused solely on the use of textual data. Research is expanding, however, to focus on the real-time analysis of streaming voice, images, and video at scales sufficient to support operations in densely crowded urban environments. There is much work to be done, both architecturally and algorithmically, but efforts to date have shown promise and generated widespread interest from the public safety and national security communities. The applicability of these techniques to support ad hoc military engagements in areas with sparse intelligence preparation is clear.

ENDNOTES - CHAPTER 5

1. Salvador Rodriguez, "60 Percent of World's Population Still Won't Have Internet by the End of 2014," *The Los Angeles Times*, May 7, 2014.

2. Maya Shwayder, "One-Third of World's Population Using Internet, Developing Nations Showing Biggest Gains," *International Business Times,* September 24, 2012.

3. Caitlin Dewey, "Almost as Many People Use Facebook as Live in the Entire Country of China," *The Washington Post*, October 29, 2014.

4. U.S. National Intelligence Council (USNIC), *Global Trends 2030: Alternative Worlds,* Washington, DC: USNIC, 2012.

5. U.S. Census Bureau, "US and World Population Clock," available from *census.gov/popclock/*, accessed on May 14, 2015.

6. World Health Organization, "Urban Population Growth," available from *who.int/gho/urban_health/situation_trends/urban_population_growth_text/en/*, accessed on May 14, 2015.

7. GSM Association, "GSMA Announces New Global Research That Highlights Significant Growth Opportunity For The Mobile Industry," Press Release, October 18, 2012, available from *gsma.com/newsroom/press-release/gsma-announces-new-global-research-that-highlights-significant-growth-opportunity-for-the-mobile-industry/*, accessed May 17, 2013.

8. Erica Kochi, "How the Future of Mobile Lies in the Developing World," Tech Crunch, May 27, 2012, available from *techcrunch.com/2012/05/27/mobile-developing-world/*, accessed on May 17, 2013.

9. U.S. Dept. of Commerce, Economics and Statistics Administration, Amanda Noss, "Household Income for States: 2010 and 2011," Washington, DC: U.S. Census Bureau, September 2012.

10. Andreas Constantinou, "[Report] Mobile Megatrends 2012," Annual Report Series, VisionMobile, London, UK, May 31, 2012, available from *visionmobile.com/blog/2012/05/report-mobile-megatrends-2012/*.

11. Tarmo Virki, "Nokia Cheap Phone Tops Electronics Chart," Reuters, May 3, 2007, available from *uk.reuters.com/article/2007/05/03/us-nokia-history-idUKL0262945620070503*.

12. Communications Commission of Kenya, "Quarterly Sector Statistics Report—Third Quarter of the Financial Year 2011/2012," Communications Commission of Kenya, Nairobi, 2012; Telecom Regulatory Authority of India; "Telecom Subscription Data as of 30 Nov 2011, New Delhi, India," Telecom Regulatory Authority of India, New Delhi, India, 2011; Peter Evans, "2014 Indonesia—Telecoms, Broadband, Mobile and Forecasts," Budde Comm [online telecommunications research site], available from *budde.com.au/Research/Indonesia-Telecoms-Mobile-Broadband-and-Forecasts.html*.

13. Bhavika Jain, "62% of Mumbai Lives in Slums: Census," *Hindustan Times*, October 17, 2010, available from *hindustantimes.com/mumbai/62-of-mumbai-lives-in-slums-census/story-I3bUsll9w-5f6ePEfuXJEbM.html.*

14. "Global Trends 2030: Alternative Worlds," Washington, DC: National Intelligence Council, 2012.

15. Colin P. Clarke, *Terrorism, Inc.: The Financing of Terrorism, Insurgency and Irregular Warfare*, Santa Barbara, CA: ABC-CLIO, 2015. For a theoretical explanation of the phenomenon of the dark side of social capital, see Robert D. Putnam, *Bowling Alone: The Collapse and Revival of American Community,* New York: Simon & Schuster, 2000.

16. David Kilcullen, *Out of the Mountains: The Coming Age of the Urban Guerrilla,* Oxford, UK: Oxford University Press, 2013, pp. 32-33.

17. Aroosa Shaukat, "Education for all: Literacy rate rising, but Pakistan needs to do more," *The Express Tribune,* October 25, 2012, available from *tribune.com.pk/story/456401/education-for-all-literacy-rate-rising-but-pakistan-needs-to-do-more/*, accessed on May 22, 2013.

18. National Intelligence Council.

19. Henry Blodget and Tony Danova, "The Future of Digital: 2014," *Business Insider*, December 8, 2014, available from *businessinsider.com/the-future-of-digital-2014-slide-deck-2014-12*, accessed on May 22, 2013.

20. Josh Eells, quoted in Kilcullen, p. 16.

21. For more, see C. Christine Fair, *Urban Battlefields of South Asia: Lessons Learned from Sri Lanka, India, and Pakistan*, Santa Monica, CA: RAND Corporation, 2004.

22. Steve Inskeep, *Instant City: Life and Death in Karachi*, New York: Penguin Group, 2011.

23. Declan Walsh and Zia ur-Rehman, "Taliban Spread Terror in Karachi as the New Gang in Town," *The New York Times*, March 28, 2013, available from *nytimes.com/2013/03/29/world/asia/taliban-extending-reach-across-pakistan.html*, accessed on May 22, 2013.

24. Robert J. Bunker and John P. Sullivan, "Integrating feral cities and third phase cartels/third generation gangs research: the rise of criminal (narco) city networks and BlackFor," *Small Wars & Insurgencies,* Vol. 22, No. 5, December 2011, pp. 764-786.

25. Moisés Naím, "Mafia States: Organized Crime Takes Office," *Foreign Affairs,* Vol. 91, No. 3, May/June 2012, pp. 100-111.

26. Mark Duffield, "Post-modern conflict: Warlords, post-adjustment states and private protection," *Civil Wars,* Vol. 1, No. 1, 1998, pp. 65-102.

27. Philip G. Cerny, "Neomedievalism, civil war and the new security dilemma: globalisation as durable disorder," *Civil Wars,* Vol. 1, No. 1, 1998, pp. 36-64.

28. Collapsed states are characterized by the rule of the strong, a vacuum of authority, and a "dark energy" that has pushed the state into a veritable black hole where political goods can only be obtained through private or ad hoc means. See Robert I. Rotberg, "Failed States, Collapsed States, Weak States: Causes and Indicators," in Robert I. Rotberg, ed., *State Failure and State Weakness in a Time of Terror*, Cambridge, UK: World Peace Foundation, 2003, p. 9. For more on the anti-Barre insurgency in Somalia from 1980-1991, see Christopher Paul, Colin P. Clarke, and Beth Grill, *Victory Has a Thousand Fathers: Detailed Counterinsurgency Case Studies*, Santa Monica, CA: RAND Corporation, 2010, pp. 47-57. For a more updated case study on Somalia, see Christopher Paul, Colin

P. Clarke, and Chad C. Serena, *Mexico is Not Colombia: Alternative Historical Analogies for Responding to the Challenge of Violent Drug Trafficking Organizations: Supporting Case Studies*, Santa Monica, CA: RAND Corporation, 2014, pp. 151-166.

29. Walter S. Clarke and Robert Gosende, "Somalia: Can a Collapsed State Reconstitute Itself?" in Rotberg, ed., *State Failure and State Weakness in a Time of Terror*, pp. 146-147.

30. Kenneth Menkhaus, "Non-State Actors and the Role of Violence in Stateless Somalia," in Kledja Mulaj, ed., *Violent Non-State Actors in World Politics,* New York: Columbia University Press, 2010, pp. 372-373.

31. *Ibid*., p. 373.

32. Kenneth Menkhaus, "Somalia: Governance vs. Statebuilding," in Charles T. Call with Vanessa Wyeth, *Building States to Build Peace,* Boulder, CO: Lynne Rienner, 2008, p. 187.

33. Katrina Manson, "Welcome to Mogadishu," *Financial Times,* May 31, 2013.

34. Clarke and Gosende. p. 132.

35. Menkhaus, "Somalia: Governance vs. Statebuilding," p. 199.

36. *Ibid*., p. 189.

37. Task Force Ranger consisted of 130 Delta commandos, a Ranger company, and elements from the Army's special operations aviation unit. See Sean J. A. Edwards, *Mars Unmasked: The Changing Face of Urban Operations,* Santa Monica, CA: RAND Corporation, 2000, p. 13.

38. Edwards, p. 15.

39. *Ibid*., pp. 15-16.

40. Jamison Jo Medby and Russell W. Glenn, *Street Smart: Intelligence Preparation of the Battlefield for Urban Operations,* Santa Monica, CA: RAND Corporation, 2002, p. 29.

41. *Ibid.*, pp. 25-36.

42. For more on the challenges of operating in dense urban environments, see Russell W. Glenn, *Heavy Matter: Urban Operations' Density of Challenges,* Santa Monica, CA: RAND Corporation, 2000.

43. Medby and Glenn, p. 33.

44. Rob Wise, "Al Shabaab," AQAM Future Project Case Study Series, Case Study Number 2, Washington, DC: Center for Strategic and International Studies, July 2011, p. 3. For a more robust discussion of AIAI, see Kenneth J. Menkhaus, "Somalia and Somaliland: Terrorism, Political Islam, and State Collapse," in Robert I. Rotberg, ed., *Battling Terrorism in the Horn of Africa,* Cambridge, UK: World Peace Foundation, 2005, pp. 35-36.

45. Menkhaus, "Somalia and Somaliland: Terrorism, Political Islam, and State Collapse," pp. 23-24.

46. Sudarsan Raghavan, "Islamic Militant Group Al-Shabaab Claims Uganda Bombing Attack," *The Washington Post,* July 12, 2010.

47. Ken Menkhaus, "Local Security Systems in Somali East Africa," in Louise Andersen, Bjorn Moller, and Finn Stepputat, eds., *Fragile States and Insecure People? Violence, Security, and Statehood in the Twenty-First Century,* New York: Palgrave MacMillan, 2007, p. 77.

48. Ken Menkhaus and Christopher Boucek, "Terrorism Out of Somalia," Washington, DC: Carnegie Endowment for International Peace, September 23, 2010.

49. Wise, p. 3.

50. Kenneth Menkhaus, "Non-State Actors and the Role of Violence in Stateless Somalia," in Kledja Mulaj, ed., *Violent Non-State Actors in World Politics,* New York: Columbia University Press, 2010, p. 373.

51. Alexander Meleagrou-Hitchens *et al*., "Lights, Camera, Jihad: Al-Shabaab's Western Media Strategy," London, UK: The International Centre for the Study of Radicalisation and Political Violence, 2012.

52. "Leet," also known as "eleet" or "leetspeak," is an alternative alphabet for the English language that is used primarily on the Internet. It uses various combinations of ASCII characters to replace Latinate letters.

53. IBM, "What is Big Data?" available from *www-01.ibm.com/software/data/bigdata/*, accessed on June 30, 2013.

54. Margaret Rouse, "How Many Bytes For . . ." available from *searchstorage.techtarget.com/definition/How-many-bytes-for*, accessed on June 30, 2013.

55. "EMC Digital Universe Study with Research and Analysis by IDC," available from *www.emc.com/leadership/digital-universe/index.htm?pid=landing-digitaluniverse-131212,* accessed on June 30, 2013.

56. Internet Live Stats, "Twitter Usage Statistics" available from *internetlivestats.com/twitter-statistics/*, accessed on May 14, 2015.

PART II

CHALLENGES AND THREATS IN CYBERSPACE

CHAPTER 6

CYBERTERRORISM IN A POST-STUXNET WORLD

Michael Kenney

When Saudi Aramco, the world's largest oil producer, and several major American financial institutions, including JPMorgan Chase, Bank of America, and Wells Fargo, were pummeled by computer attacks in August and September 2012, it marked the beginning of a new wave of cyberattacks against the global oil and banking industries. What made the attacks stand out from earlier ones was that they were directed toward destroying information rather than stealing data or defacing websites, which are objectives typically associated with hackers and online criminals. In this respect, the attacks resembled Stuxnet and other cyberweapons the United States and Israel reportedly unleashed against the Iranian government to sabotage its nuclear development program by physically damaging the centrifuges used to enrich uranium. Indeed, as they learned more about the attacks against the U.S. banks, American officials became convinced they were carried out by the Iranian government in retaliation for Stuxnet and U.S.-led financial sanctions on the Iranian economy.[1] The cyberwar that RAND strategists John Arquilla and David Ronfeldt declared was coming almost 20 years before it was apparently at hand.[2]

The Barack Obama administration has remained conspicuously silent about Stuxnet, refusing to confirm or deny numerous reports describing the American role in the attacks. However, prominent officials

have expressed growing alarm over the wave of cyberattacks against U.S. financial institutions. In giving voice to their concerns, some observers have moved beyond trepidation to hyperbole. In a major speech referring to the attacks, Defense Secretary Leon Panetta warned that the United States faced a "cyber Pearl Harbor," whereby an "aggressor nation or extremist group" could use computer attacks to "derail passenger trains . . . contaminate the water supply in major cities, or shut down the power grid across large parts of the country."[3] If the Defense Secretary's scenarios sounded like something out of a *Die Hard* movie, some computer security specialists actually compared the recent attacks between the United States and Iran to the fourth film in the Bruce Willis franchise. In that film, terrorists send viruses that kill people by causing their computers to blow up, to suggest that what we are seeing today is not cyberwar, but "cyberterrorism" and "the beginning of the end of the [interconnected] world as we know it."[4]

While the covert actions between the United States and Iran represent a new threshold in cyberattacks, the breathless portrayals of these events by Panetta and others do not. Ever since the widespread adoption of the Internet in the 1990s, government officials, computer security specialists, and journalists have promoted frightening scenarios depicting a "digital Pearl Harbor" in which, as one long-time observer recalls, computer hackers "would plunge cities into blackness, open floodgates, poison water supplies, and cause airplanes to crash into each other."[5] The perpetrators behind these hypothetical attacks were often called "cyberterrorists," a term whose provenance dates back to the same period.[6] In popular accounts, cyberterrorists referred both to computer

hackers, who caused airplanes to fly into each other or brought down the nation's banking system; and terrorists, who used computers to kill, as in the Willis movie. Either way, Tom Ridge, then White House Director of Homeland Security, warned that the threat of cyberterrorism was immediate and palpable: "Terrorists can sit at one computer connected to one network and can create worldwide havoc . . . [they] don't necessarily need a bomb or explosives to cripple a sector of the economy, or shut down a power grid."[7]

There was only one problem with such dire warnings, the threats never materialized. While the United States experienced hundreds of thousands of cybercrimes and cyberattacks in the ensuing years, none rose to the level of cyberterrorism. Cyberterrorism is defined as computer-generated attacks against other computer systems that cause enough violence or physical harm against private citizens or property to generate fear in a wider audience in pursuit of a political, social, or religious objective. Instead, during any given year, a motley assortment of hackers and online criminals routinely broke into computer networks to probe for weak spots, steal information, vandalize websites, disrupt online services, and, more recently, sabotage computers and the machines they run. While some attacks were carried out by politically and socially motivated hackers who used nonviolent means to engage in digital protest politics, such incidents typically involved website defacements—the virtual equivalent of graffiti—or denial of service attacks, which temporarily disrupted websites. None of the thousands of computer intrusions physically harmed anybody, provoked fear in larger audiences, or seriously damaged critical infrastructures, such as major transportation and communication systems.

This chapter seeks to dial down the rhetoric on cyberterrorism by analyzing the concept along with similar phenomena with which it is often associated. While some scholars have previously drawn distinctions between these phenomena, others have recently "stretched" cyberterrorism's conceptual parameters—equating it with hacktivism, cyberattacks, and terrorist use of the Internet. In the wake of Stuxnet and Iran's retaliatory cyberattacks against American banks, along with the pugnacious virtual pranks and digital activism of Anonymous, a conceptual review appears in order. My inquiry proceeds from the assumption that precision is essential to this task: to understand what cyberterrorism is, we must be able to distinguish it from what it is not. To be sure, none of the concepts discussed below enjoy universally agreed-upon definitions, but each contains basic features that are essential to the phenomenon in question—characteristics that distinguish cyberterrorism from its cyber-companions. While my analysis is largely conceptual, I repeatedly draw on real-world examples to illustrate my arguments and observations. In a post-Stuxnet world, threats to our cybersecurity are real, but only by carefully distinguishing among them, separating fact from fantasy, can we best understand the dangers we face without inflating them.

CYBERATTACK

I begin high up the ladder of abstraction with the most general concept, one that provides a conceptual umbrella for the phenomena that follow. A cyberattack is a deliberate computer-to-computer attack that disrupts, deceives, degrades, or destroys computer systems or the information they contain.[8] There are

many different methods for conducting cyberattacks, including infecting computers and networks with viruses and worms that takeover, slow down, or damage computers; embedding malicious code, also called "Trojan horses," into otherwise legitimate hardware and software; using fake emails or websites to trick or "phish" people into sharing sensitive information; exploiting spyware to probe for network vulnerabilities or capture data; and conducting denial-of-service attacks, with or without the assistance of botnets, to overwhelm websites and networks by flooding them with junk communications.[9]

By definition, cyberattacks are computer attacks on other computers. They do not include physical assaults on computers using other weapons, such as destroying computers with hammers or explosives.[10] The immediate objective of a cyberattack may be to harm the targeted computer or system, steal information from it, or simply observe the computer in action in order to exploit vulnerabilities for subsequent attacks. The key is that the attacker conducts the intrusion with hostile, if not necessarily destructive, intent—and without the knowledge or consent of the target. Beyond this, cyberattacks do not contain a lot of discriminating characteristics, as we would expect in such a broad, general concept. The perpetrators of cyberattacks can be states or nonstate actors, the scale of the attack can be large or small, and the purpose for such intrusions can be to achieve any economic, political, social, or psychological goal.

Among the many cyberattacks that have been carried out in recent years, prominent examples include the "I Love You" worm, which caused billions of dollars in estimated damages among millions of computers in 2000; the "Slammer" denial-of-service virus,

which infected dozens of computer servers in 2003, including a 911 emergency response system in Washington State and the Davis-Besse nuclear power plant in Ohio; and the "Conficker" super worm in 2009, which created a massive botnet of millions of Windows-based personal computers, a botnet that was never activated, yet still infects many computers.[11]

CYBERCRIME

If a cyberattack is an overarching concept under which we can distinguish many different cyberphenomena, cybercrime is also a broad concept, referring to any criminal activity committed using a computer. Cybercrime encompasses a wide range of activities for which the computer is "the agent of the crime, the facilitator of the crime, or the target of the crime."[12] Some cybercrimes, such as "spamming," online piracy, and distributing child pornography, occur exclusively on the computer; while others, including cyberstalking and harassment, some forms of identity theft, and corporate espionage use the computer to facilitate crimes that are conducted largely offline. Many cybercrimes are perpetrated by individuals and small groups of hackers, rather than traditional organized crime groups or states.[13] In recent years, corporate cybercrime involving the widespread use of botnets and sophisticated espionage attacks that steal proprietary data has emerged as a major concern in the United States and Europe.[14]

Cybercriminals have a variety of tools at their disposal, including viruses, worms, Trojans, keystroke loggers, and other malicious software, along with phishing scams and social engineering tricks to elicit sensitive information from unwitting victims.[15] Cyber-

crimes may constitute cyberattacks, particularly when the act is undertaken with hostile intent and without the knowledge or consent of the target. But not all cybercrimes are cyberattacks. Some forms of cybercrime, such as online drug dealing, involve the cooperation of mutually consenting participants. For example, federal authorities in 2013 shut down Silk Road, a virtual underground marketplace connecting thousands of drug dealers with over 100,000 customers who regularly purchased marijuana, Ecstasy, LSD, illegal prescription drugs, and other illegal goods.[16]

As with offline criminality, the purpose of many cybercrimes is economic, to obtain money or other material resources rather than to achieve some political or social objective. However, some cybercrimes, including harassment, "life ruin" pranks, and "revenge porn," may be driven by psychological motivations, such as the desire to harm a perceived wrongdoer or merely have fun (lulz)[17] at another's expense.[18] Irrespective of the motivation, cybercrime has skyrocketed in recent years, with identity theft, online frauds, and other illegal computer intrusions becoming a regular feature of everyday life—costing the U.S. economy an estimated $100 billion dollars in losses each year.[19]

CYBERWARFARE AND STUXNET

Like conventional warfare, cyberwar is largely, though not exclusively, the domain of states. States, and the hackers they sponsor or support, wage war in cyberspace to deny their rivals the ability to use computer systems effectively while safeguarding their own ability to do the same. Cyberwarfare includes defensive operations that protect a state's computer networks from attacks by others and offensive operations

that damage and destroy their adversaries' networks or deter their opponents from attacking them.[20] Similar to kinetic warfare, cyberwar involves a sustained campaign rather than isolated attacks. Moreover, cyberwar generally occurs in the context of larger conflicts, including, but not limited to, low-intensity conflict and operations other than war.

Unlike cybercrime and cyberattacks more generally, there are not a lot of clear-cut examples of cyberwarfare in the real world. One oft-cited exception refers to the campaign of cyberattacks directed against the Georgian government in the lead-up to the Russian-Georgian war in 2008. Weeks before the fighting broke out, hackers believed to be acting on behalf of the Russian government carried out a series of distributed denial-of-service and website defacement attacks against websites run by the Georgian government. When Russian forces began bombing Georgia, the cyberattacks expanded to other targets, including government, media, and transportation company websites in Georgia. While the cybercampaign managed to shut down many websites temporarily, the significance of the attacks lay not in the damage they caused, but rather in the fact that it was the first time a documented series of cyberattacks acted as a force multiplier for one of the combatants in a real war, effectively opening another theater of operations for contemporary warfare.[21]

Although computer forensics investigators uncovered substantial evidence of Russian involvement in the attacks, the Russian government denied that it was responsible, illustrating another feature of cyberwar—the difficulty in determining whether clandestine perpetrators responsible for specific attacks are state agents or nonstate actors. The challenge of assigning

attribution makes it hard to distinguish some cyberwarfare incidents from cyberattacks more generally. The hackers who claimed credit for the recent cyberattacks against U.S. financial institutions called themselves the Izz ad-Din al-Qassam Cyber Fighters, in honor of a famous cleric who died while fighting British forces in Palestine during the 1930s. In several press releases posted on the Internet, the group claimed it attacked the banks in retaliation for an offensive video mocking the Prophet Mohammed.[22] However, American officials claim the group is merely a cover for the Iranian government, which they believe launched the attacks in retaliation for Stuxnet and other computer viruses allegedly unleashed by the United States and Israel against Iran's nuclear program.[23] Ironically, if these officials are right, the cyberattacks and counterattacks between the two countries may be viewed as cyberwarfare, particularly when seen through the lens of the recent history of low-intensity conflict between the two countries dating back to the Iranian Revolution and the U.S. hostage crisis in the late-1970s.[24]

Practitioners of cyberwar have a variety of weapons in their arsenals, including distributed denial-of-service attacks, spying malware, and viruses and worms. Because they are carried out or supported by states, cyberwar operations tend to be more complex than many cyberattacks carried out by nonstate hackers. While the Stuxnet worm may not have been as cutting-edge as the media hype surrounding the attacks suggested, it still set a new standard in weaponized malware.[25] Part of a larger U.S. cyberwarfare program called "Olympic Games," Stuxnet launched a series of attacks targeting industrial controllers used at Iran's uranium enrichment facility in Natanz. Industrial controllers are small computer systems that

run mechanical devices such as pumps, valves, motors, and thermometers by sending and receiving electrical signals.[26]

With Stuxnet, computer programmers created an intricate code capable not only of manipulating the industrial controllers who spun the gas centrifuges at the facility, but of secretly recording plant operations when the centrifuges were working properly, and replaying these signals back to plant engineers during the attacks, so that they thought the centrifuges were operating normally when they were spinning out of control.[27] After programmers developed and tested the Stuxnet worm against a replica of the Iranian facility using the same kind of gas employed at Natanz, individuals with access to the plant deployed the virus, wittingly or not, through infected jump drives. This allowed the United States and Israel to jump the air gap surrounding the facility, which was not connected to the Internet for security reasons. Once Natanz's computer systems were infected, the cyberattacks were periodically activated over the course of many weeks, deliberately altering the velocity at which the delicate gas centrifuges spun and causing them to slow down and speed up at intervals the machines were not designed to handle.[28] The intermittent nature of the attacks, in which the centrifuges returned to normal following each round of attacks, confused the plant's engineers. This allowed the operation to continue over an extended period of time before Iranian authorities temporarily closed the facility, setting back their country's nuclear enrichment program by months or even years.[29] Stuxnet marked a watershed in cyberwarfare, not only demonstrating U.S. willingness to engage in offensive cyberattacks against its most intransigent adversaries, but also revealing a level of destructive

power with computer code previously reserved for kinetic bombings and physical sabotage.[30]

The purpose of Stuxnet and other acts of cyberwarfare is inherently political. Countries engage in cyberwar to protect and advance their security interests. While private, "patriotic" hackers may actively support one belligerent over another, most cyberwarfare involves state adversaries, either the governments directly involved or state-sponsored or supported hackers acting on their behalf. In addition to the United States, Israel, and Iran, numerous countries have developed offensive cyberwarfare capabilities in recent years, including China, Cuba, France, Germany, India, Iraq, Japan, Libya, Syria, and the United Kingdom.[31] This list will likely continue to grow in the aftermath of Stuxnet, which so dramatically illustrated the firepower of today's most advanced cyberweapons.

HACKTIVISM

Hacktivism refers to politically or socially inspired cyberattacks carried out by private, nonstate hackers, either operating on their own or as part of larger collectives such as Anonymous. These politically motivated hackers, or "hacktivists," target different government agencies, business corporations, and even private individuals with distributed denial-of-service attacks, website defacements, viruses and worms, and data theft. In 1999, after the North Atlantic Treaty Organization accidentally bombed the Chinese Embassy in Belgrade during the Kosovo war, hacktivists from China attacked U.S. Government computer networks with website defacements and denial-of-service email attacks.[32] In 2006, hackers launched denial-of-service attacks and website defacements against numerous

websites in Denmark after the Danish newspaper *Jyllands-Posten* published cartoons lampooning the Prophet Mohammed.[33] Over the years, pro-Palestinian hackers and digital activists repeatedly have attacked government and private websites in Israel, as they did after the resumption of violent hostilities between Israel and the Hamas-controlled Gaza Strip in 2012.[34] These digital activists are driven by an assortment of political, social, and religious causes, representing new forms of direct action and civil disobedience that are reshaping contemporary protest politics.[35]

No collective has pushed the boundaries of this new form of digital activism more forcefully than Anonymous. Along with its numerous spin-off groups, including LulzSec and AntiSec, Anonymous has taken hacktivism to a whole new level, carrying out dozens of highly publicized denial-of-service attacks, website defacements, and life-ruining attacks against a sundry assortment of government agencies, private corporations, and individuals. Among the many targets of Anonymous are the American Israel Public Affairs Committee, the Central Intelligence Agency, the Federal Bureau of Investigation, Koch Industries, MasterCard, the Motion Picture Association of America, PayPal, the Public Broadcasting Service, Sony, Stratfor, *The Sun* newspaper, the Vatican, Warner Brothers Music, the White House, and the Westboro Baptist Church. What unites "Anons," as members of the hacktivist movement call themselves, behind their operations is an eclectic vision that embraces the free flow of information, the protection of human rights, and the "power of the individual" not only to participate in virtual civil disobedience, but also to agitate and amuse "just for the lulz," satisfying the participants' ironic, self-righteous sense of humor, often at the expense of others.[36]

Attacks carried out by Anonymous and other hacktivists have been disruptive, causing inconvenience, financial damage, and, in some cases, emotional distress to their immediate victims. In 2007, following the removal of a Red Army war monument from the center of Tallinn, the capital of Estonia, hackers used botnets to carry out distributed denial-of-service attacks against the former Soviet republic that temporarily blocked Estonians' access to online banking services and government websites.[37] Speaking at a public forum hosted by the Center for Strategic and International Studies shortly afterward, the Estonian Minister of Defense emphasized the "psychological nature" of the attacks, claiming they "caused intimidation . . . [and] created widespread confusion and miscommunication in the general public."[38] After being victimized by distributed denial-of-service attacks, website defacements, and other Anonymous pranks, the Church of Scientology issued a statement describing Anonymous as "a group of cyber-terrorists" carrying out "illegal assaults on Church web-sites."[39]

Ultimately, whether these incidents caused enough harm or fear in wider audiences beyond their immediate victims to be considered cyberterrorism rather than hacktivism is, as Dorothy Denning observes, "a judgment call."[40] Although some Estonian citizens may have been disturbed by the country-wide cyberattacks, they did not likely fear immediate physical harm. The website disruptions were temporary, online services were rapidly restored, and no critical infrastructures were targeted. "[T]he primary operational result of the attack," concludes the National Research Council in its assessment of the incident, "was inconvenience."[41] The distributed denial-of-service attacks and website defacements carried out against the Church of Scientology did not cause their victims any

physical damage. Nor have any Anonymous operations incited fear or intimidation in audiences larger than the immediate victims of the attacks, which is essential to terrorism. In sum, these incidents were politically and socially motivated cyberattacks designed to disrupt, inconvenience, and publicize their respective causes, rather than spread terror, cause physical harm, or degrade critical infrastructures. The attacks represent an aggressive form of digital protest politics and civil disobedience rather than terrorism, with or without the "cyber" prefix.

CYBERTERRORISM

Cyberterrorism refers to cyberattacks against computer systems outside of cyberwarfare, resulting in substantial physical harm or violence against civilian noncombatants intended to terrorize wider audiences for some political, social, or religious end. Unlike cybercrime, cyberterrorism is a political act, one that is committed in pursuit of a larger cause, be it overthrowing the capitalist economic system, reestablishing the Islamic caliphate, or creating a "racially pure" theocratic state based on Biblical scripture. Cybercrime may be violent, but it is not politically motivated, and the fear or intimidation it generates is limited to its immediate victims, contrary to the broader audience that terrorists seek to influence. In contrast to hacktivism, cyberterrorism is, by definition, a physically violent act, one intended to seriously harm or kill innocent human beings or cause substantial destruction to property or critical infrastructure. By way of illustration, Denning discusses specific examples of cyberterrorism, including attacks "that lead to death or bodily injury, explosions, plane crashes, water contamination, or severe economic loss," or "serious at-

tacks" against critical infrastructures that spread fear rather than "costly nuisance" attacks, which do not.[42]

To date, most cyberattacks have been disruptive, not destructive. To be sure, a small number of attacks have resulted in physical damage, at least against property. The most prominent examples are Stuxnet and a separate attack against a water treatment plant in Queensland, Australia, in 2000. The Queensland attack was carried out by Vitek Boden, a former employee of the software firm that installed the Supervisory Control and Data Acquisition (SCADA) system and industrial controllers that regulated the plant's sewage system.[43] After quitting the software firm and being turned down for a similar position on the local government council that ran the treatment plant, Boden used his expertise of the industrial controllers and SCADA system to remotely access and release 800,000 gallons of raw sewage into adjacent rivers, parks, and the grounds of a nearby hotel, destroying local marine life and creating a nauseating stench for residents.[44]

Both Stuxnet and the Boden attacks caused physical damage, in the latter case against critical infrastructure. They also caused puzzlement and confusion among plant operators, who struggled to understand what was happening to their respective facilities.[45] However, neither attack was accompanied by any public statements or admissions of responsibility from perpetrators threatening additional assaults, which would have made the attacks more intimidating had that been the perpetrators' intention. What distinguishes kinetic cyberattacks like Stuxnet and Queensland from cyberterrorism is that the violence of the latter has an inherently dramatic purpose: to provoke fear, dread, and terror in a wider audience, an audience extending well beyond the immediate

victims to a country's government or society at large.[46] Stuxnet was intended to sabotage and disrupt the Iranian government's nuclear program; Queensland was an act of vengeance by a disgruntled employee who wanted to get even with his former employer and the local government that refused to hire him. Neither attack was intended to provoke widespread fear in the areas they targeted.[47]

The attributes of cyberterrorism discussed so far—political motivation, physical violence against civilians or property, and coercion through fear and intimidation—are all found in terrorism proper. What makes an act cyberterrorism is the means by which it is conducted and the target of the attack. Unlike conventional terrorism, cyberterrorism refers to computer-generated attacks that target other computers and the information they contain.[48] With cyberterrorism, computer technology is both weapon and target. Significantly, the many examples of terrorists exploiting computers to prepare for conventional attacks, such as using the Internet to research potential targets, buy plane tickets, or email fellow conspirators, do not qualify as cyberterrorism. Nor do physical attacks on computer systems, such as using explosives to destroy a SCADA system that regulates the electricity grid of a large American city.[49] What would qualify as cyberterrorism is a computer-generated attack on a SCADA system or industrial controller that regulates critical infrastructure, provided the attack is politically inspired and causes enough violence and damage to provoke fear and intimidation in others beyond the immediate victims of the attack. Cyberattacks rarely produce this sort of physical violence. As Denning points out, this "may be one reason they have not yet become an instrument of terrorism."[50]

The four elements discussed above—physical violence, psychological coercion, political motivation, and computer generation—represent necessary, but not sufficient, conditions for cyberterrorism. The combination of these four elements suggests that cyberterrorism is defined both by its intent and its effects, rather than by one or the other, as some analysts suggest.[51] The intent of computer-generated violence must be to achieve some political, social, or religious goal, and its effect must be sufficiently harmful or damaging to generate a high level of fear, comparable to real-world terrorism. There can be no cyberterrorism without terrorism.

STATE OR STATE-SPONSORED CYBERTERRORISM

Do states engage in or sponsor cyberterrorism? The question is an important one because, as Stuxnet illustrates, state hackers or state-sponsored hackers possess the resources and expertise to carry out cyberattacks with the severity of effects needed for cyberterrorism.[52] Some researchers maintain that cyberterrorism is the exclusive province of nonstate actors. Maura Conway uses the U.S. State Department's definition of terrorism, which limits the perpetrators to "subnational groups or clandestine agents," as the basis for her definition of cyberterrorism. She defines the latter as:

> premeditated, politically motivated attacks by subnational groups or clandestine agents against information, computer systems, computer programs, and data that result in violence against noncombatant targets.[53]

Mark Pollitt does the same, arguing that analysts must be able to distinguish cyberterrorism from other concepts, such as information warfare. The first, he points out, is "an offensive and defensive function of governments," while the second is the work of "subnational groups or clandestine agents."[54] Similarly, Kelly Gable argues that states and state agents engage in cyberwarfare, while "individuals, groups of individuals, or organizations such as Al Qaeda" engage in cyberterrorism.[55]

Restricting cyberterrorism to nonstate actors is consistent with the views of some leading terrorism scholars, who insist that states do not conduct terrorism. According to this line of argument, states are sovereign actors who enjoy a monopoly on the legitimate use of violence within their national territories and who are bound by the Geneva, Switzerland, and Hague, The Netherlands, Conventions. States may commit war crimes against other states and "terror" against their own citizens, but they do not engage in terrorism. The latter is the domain of nonstate terrorists who scorn long-standing rules of warfare and international diplomacy by, among other things, taking civilian hostages; bombing embassies; and blowing up, shooting, and otherwise harming and killing innocent civilians and noncombatants.[56]

This view, however, is not shared by all terrorism scholars, many of whom insist that, since the French Revolution, the historical record is replete with examples of states and their agents carrying out violent acts against civilians outside of warfare that are intended to terrorize wider audiences for some political purpose, usually to coerce dissenters to submit to state rule.[57] Moreover, Bruce Hoffman and other established scholars, and even the U.S. State Department itself,

acknowledge that some contemporary governments engage in state-sponsored terrorism when they intentionally support nonstate terrorist groups, including groups that execute attacks to serve the sponsoring state's national security interests.[58] Whether analysts wish to call it "state terror" or "state terrorism," history suggests that some states have been implicated in terrorist attacks, either directly as perpetrators or indirectly as sponsors.

Consequently, Brian Michael Jenkins and others maintain that terrorism must be "defined by the nature of the act, not by the identity of the perpetrators or the nature of their cause."[59] When terrorism, and by extension cyberterrorism, is defined by the nature of the act, rather than by the identity of the attackers, it is no longer necessary or plausible to restrict it to nonstate actors. If all the definitional elements of cyberterrorism described earlier apply to the act in question and the act takes place outside of warfare between two or more belligerents, then the perpetrators behind the attack may be considered cyberterrorists, irrespective of whether they are states or nonstate actors.

Including states as possible agents or sponsors of cyberterrorism compels us to add a fifth component to our definition, which is necessary to distinguish cyberterrorism from cyberwarfare. Unlike cyberwarfare, cyberterrorism refers to peacetime cyberattacks against computer systems resulting in substantial physical harm or violence intended to terrorize wider audiences for some political, social, or religious end. While most acts of cyberwarfare committed to date have aimed to steal data from or damage computer systems rather than to intimidate or terrorize wider audiences, such a possibility is not inconceivable. Two belligerents engaged in a sustained campaign of

cyberattacks against each other as part of a larger, kinetic war between them may seek to intimidate or terrorize each other's civilian populations through extensively distributed denial-of-service attacks or SCADA attacks targeting critical infrastructures. So where do we draw the line between cyberwar attacks intended to terrorize and cyberterrorism proper? If such attacks occur during sustained hostilities between belligerents, including low-intensity conflict, they are cyberwarfare; if they occur during peacetime, they are cyberterrorism. Cyberterrorism, in sum, is the peacetime equivalent of what could be called cyberwar crimes or atrocities.[60]

For an act to be considered cyberterrorism, it must meet five conditions. First, as with cyberattacks more broadly, the act must be a computer attack that targets other computers, computer systems, or the information they contain. Second, the attack must be undertaken in pursuit of some political, social, or religious aim, as opposed to an economic one, which is associated with cybercrime. Third, the attack must result in physical violence against persons, property, or critical infrastructures. Fourth, the attack must cause fear or intimidation in a wider audience beyond the immediate victims of the violence. While cyberwarfare may also result in physical violence and widespread fear, such effects are incidental, not essential, as they are in cyberterrorism. Fifth, unlike cyberwar, the attack must occur outside the context of war or hostilities between two or more belligerents.

When analysts apply all five factors to the many thousands of cyberattacks that have occurred in recent years, attacks involving both state and nonstate perpetrators, they will find few, if any, instances of cyberterrorism. This stands in sharp contrast to the

other cyberphenomena discussed earlier, for which there are many examples. Table 6-1 summarizes the essential components for all five types of cyberactions discussed in this chapter and provides real-world examples for each, save one.

	Cyber-attack	Cyber-crime	Cyber-warfare	Hacktivism	Cyber-terrorism
Computer attack targeting other computers, computer systems, computer networks, or the information they contain	✓	✓	✓	✓	✓
Attack in pursuit of political, social, or religious aim			✓	✓	✓
Attack in pursuit of economic aim		✓			
Attack part of broader hostilities between belligerents			✓		
Attack outside of war or cyber-war between belligerents					✓
Attack produces physical violence against persons, property or critical infrastructure.					✓
Attack causes widespread fear or intimidation beyond immediate victims					✓
Examples	"I Love You" worm, "Slammer" denial of service attack, "Conficker" virus	"Silk Road" drug exchange, phishing scams, child pornography	Stuxnet, Russian cyber-attacks on Georgia	Anonymous attacks, "cyber jihad" against Danish newspapers	?

Table 6-1. Necessary Components of Different Cyberphenomena.[61]

THE PAUCITY OF CYBERTERRORISM

Cybersecurity has become a major concern among policymakers and practitioners in recent years, and rightly so, given the dramatic rise in cyberattacks and

cybercrimes, if not cyberterrorism. Indeed, what is perhaps most striking about cyberterrorism is that it has never occurred.[62] To date, not a single cyberattack has been carried out by either state or nonstate actors that meet the five conditions of cyberterrorism. This includes Stuxnet, the Boden attack in Queensland, and the operations of Anonymous and al-Qaeda, who have never carried out a major cyberattack, despite expressing a desire to do so.[63] None of the cyberattacks believed to be from state actors, including Stuxnet and the Iranian cyberattacks on American financial institutions, qualify as cyberterrorism because the attacks sought to disrupt or sabotage computer systems rather than terrorize wider audiences. None of the cyberattacks involving nonstate actors, including the hacktivism of Anonymous, qualifies because they did not involve physical violence. Or, if they did, like Boden's attack, they did not spread fear and intimidation among wider audiences, though some life-ruining attacks may have intimidated their immediate victims. Recent years have witnessed several complex cyberattacks by states, many more or less sophisticated but disruptive hacking attacks by nonstate actors such as Anonymous, and even more cybercrimes by economically motivated criminals, but not cyberterrorism.

This does not mean that terrorists and their supporters, including those affiliated with al-Qaeda, have not carried out cyberattacks.[64] In October 2001, a group of hackers called G-Force Pakistan announced the formation of the al-Qaeda Alliance and defaced the Department of Defense website devoted to Operation ENDURING FREEDOM.[65] Several years later, other hackers carried out attacks under the banner of what the media sometimes calls "cyber-jihad." After Euro-

pean news media started publishing cartoons of the Prophet Mohammed in 2006, hackers vowed to take revenge by launching denial-of-service attacks against the Danish news websites held responsible for these acts of "blasphemy."[66]

Significantly, none of these attacks resulted in the violence and fear that are necessary for cyberterrorism. The distributed denial-of-service attacks caused, at best, temporary disruptions to public websites, often lasting only a few minutes. The website defacements, which typically posted anti-Western text and photos on the hacked sites, were the online equivalent of spray-painting the side of a building.[67] Users visiting targeted websites during such attacks may have been frustrated and inconvenienced, as the sites they sought to access were temporarily unavailable or displayed offensive messages. But they did not likely feel the dread of violence and physical intimidation associated with terrorism, despite exaggerated claims of cyberterrorism made by a few computer security professionals after some of these attacks.[68]

To be sure, some al-Qaeda members and supporters have expressed interest in conducting more damaging attacks against computer systems, attacks that could, if they were executed, approximate the widespread fear and intimidation necessary for cyberterrorism. In 2002, Omar Bakri Mohammed, a media-savvy British-based cleric who claimed to be a spokesman for the political wing of Osama bin Laden's International Islamic Front for Jihad Against Jews and Crusaders, gave an interview to *Computerworld* magazine in which he suggested that al-Qaeda would soon carry out devastating cyberattacks against major stock exchanges.[69] That same year, the United States seized computers belonging to al-Qaeda operatives

in Afghanistan, suggesting that they had gathered information about how to program SCADA systems that run critical infrastructures, information that some al-Qaeda detainees claimed they intended to use for launching cyberattacks.[70] More recently, other jihadists have expressed their familiarity with Stuxnet in online discussion forums and talked about the possibility of carrying out cyberattacks on SCADA systems and industrial controllers.[71]

While some of these incidents served as a wake-up call to government authorities, it is important to subject such claims to dispassionate, critical evaluation, particularly when they are made in open discussion forums or through media interviews. To be effective, terrorists need to communicate their messages to wide audiences, and they often use the media and the Internet to do so. To enhance the propaganda value of their communications, terrorists and their supporters often inflate their ability to carry out devastating attacks, whether using chemical, biological, nuclear, or cyberweapons. Propaganda aside, there is usually a wide gap between terrorists' stated desires and their technological and operational capacity to transform these desires into reality. Individuals like Omar Bakri frequently engage in "jihad of the tongue" to alarm the United States and its allies—in this case by exaggerating al-Qaeda's computer capabilities. As intelligence experts have long observed, Bakri is a "fire-breather" who lacks inside knowledge of al-Qaeda's ability to launch cyberattacks.[72]

Whatever the propaganda value of Bakri's claims, his thinly veiled threats have not materialized. More than a decade after his interview and after American authorities publicized al-Qaeda's interest in SCADA attacks, neither the terrorist network nor hackers act-

ing on its behalf have come close to executing cyberattacks capable of causing the big economic collapse Bakri predicted. While some jihadist websites and discussion forums contain information and software for basic hacking, there is no evidence that militants have attempted cyberattacks against industrial controllers or SCADA systems, or that they even have access to labs with the specialized software and equipment needed to carry out such attacks.[73] Instead of exploiting online resources to conduct Stuxnet-like attacks that are beyond their capabilities, al-Qaeda and other nonstate terrorists continue to use the Internet to gather information, spread propaganda, radicalize their supporters, and coordinate their activities, including carrying out simpler flesh-and-blood attacks using conventional weapons. Even after Stuxnet, as Denning explains, "Al-Qaeda and other terrorist groups still prefer bombs to bytes, and cyber terrorism remains a hypothetical threat even as the overall threat level in cyberspace has increased."[74]

CONCEPT STRETCHING

Some observers have responded to the lack of cyberterrorism by arguing that the concept itself is flawed and needs to be expanded, to include terrorist use of the Internet, cyberattacks, and hacktivism. One prominent analyst suggests that "any application of terrorism on the Internet," including posting videos of attacks online and building websites to spread propaganda, should be considered cyberterrorism.[75] To illustrate his point, he characterizes Younis Tsouli, the young West Londoner who facilitated Abu Musab al-Zarqawi's efforts to disseminate his propaganda online by hacking into computer servers, and the hack-

tivists who carried out the denial-of-service attacks against the Danish media websites in 2006 as cyberterrorists.[76] A pair of computer security researchers take a similar, if more subtle approach, suggesting that cyberterrorism targeting computers is "pure" cyberterrorism, while "regular" cyberterrorism occurs when the terrorist leverages "the other factors and abilities of the virtual world . . . in order to complete his mission, whatever that may be."[77]

In removing the computer-as-target condition of cyberterrorism from their definitions, these authors equate terrorists' use of information technology with cyberterrorism.[78] Terrorists use information technology for all sorts of reasons—some of them directly related to their attacks, some not. Using computers and the Internet as tools to spread propaganda, raise funds, or even facilitate conventional gun-and-bomb assaults is different from engaging in computer-to-computer attacks to spread widespread fear and terror. Only the latter qualifies as cyberterrorism; the former refers to some of the many different ways terrorists use the Internet instrumentally.

In fact, modern-day terrorists use a wide variety of communications technologies to facilitate their attacks, not just the Internet. For example, terrorists routinely use cell phones to communicate with their colleagues, coordinate their activities, and detonate their improvised explosive devices. We do not call this "cell phone terrorism," nor do we make fatuous distinctions between "regular" cell phone terrorism and "pure" cell phone terrorism. Instead, we simply view cell phones, along with other communications technologies like global positioning system devices, satellite phones, and personal digital assistants, as tools terrorists use to carry out their activities.

In the media, where much of the discussion on cyberterrorism takes place, it is common for journalists to equate cyberattacks, hacktivism, and cybercrime with cyberterrorism and thereby inflate the threat we face from the latter.[79] As unfortunate as this may be, it is also understandable, given the tight deadlines many journalists face, that many "experts" on whom they draw fail to distinguish cyberterrorism from hacktivism and cyberattacks. Also understandable is the temptation news editors face to exploit sensational terms like "cyberterrorism" to attract more readers, viewers, and listeners. What is less explicable, and perhaps less excusable, is when scholars—highly educated academics with the time and intellectual freedom to be able to make such distinctions—fail to do so.

While many academic researchers carefully highlight the differences between hacktivism and cyberterrorism, others are not immune from the hyperbole and definitional sloppiness that plague the popular discourse on this topic. Indeed, one of the most notorious examples of such scholarly embellishment was published by the prestigious National Research Council (NRC), one of the nation's premier bodies for disseminating scientific research to enhance the public welfare. In 1991, the NRC's System Security Study Committee, which included faculty members from the University of California at Santa Barbara, the Massachusetts Institute of Technology, and Harvard University, published a report on computer security with an alarming description, which later became a touchstone for journalists and researchers writing about the threat of cyberterrorism. "We are at risk," the report began, going on to describe American dependence on computers and vulnerability to attack before deliver-

ing the chilling punch line: "Tomorrow's terrorist may be able to do more damage with a keyboard than with a bomb."[80]

If 23 years qualifies as enough time for assessing the damage caused by tomorrow's terrorist, the authors' worst fears appear not to have been realized. More to the point, the distinguished scholars who wrote the report failed to distinguish between cyberterrorism, terrorist use of the Internet, hacktivism, and cyberattacks. They are not the only academics to do so. One communications professor defines cyberterrorism as "the intentional use of threatening and disruptive actions against computers, networks, and the Internet."[81] This broad definition would include most cybercrimes and cyberattacks and virtually all hacktivism. Indeed, in discussing his examples of cyberterrorism, he lists acts commonly associated with hacktivism, including:

> penetrating a top-secret federal computer system and stealing data, damaging files . . . disrupting monetary systems, damaging the mass media . . . disseminating false information, sabotaging operations, erasing data, [and] threatening to divulge confidential information or system weaknesses.[82]

Another academic, a professor of international law, offers a necessarily broad definition of cyberterrorism that "includes everything from basic hacking and denial of service attacks to concerted efforts to unleash weapons of mass distraction or mass disruption."[83] Among this professor's list of significant examples of cyberterrorism are: a series of espionage attacks from Chinese hackers against American defense contractors beginning in 2003, the disruptive cyberattacks launched by patriotic Russian hackers against Estonia in 2007, a week-long series of hacking attacks against

U.S. and South Korean government websites in 2009, and thousands of attempts by unknown hackers to remotely access the Pentagon's computer systems.[84] While all of these computer-generated efforts to steal information and disrupt computer systems qualify as cyberattacks and some, depending on the motives of the perpetrators, may qualify as hacktivism, none of the attacks caused the violence and fear necessary to meet the criterion of cyberterrorism.

These examples are not meant to disparage any particular researchers working in this conceptually cluttered field, but to illustrate how easy it is to undermine the analytical precision of cyberterrorism by conceptually stretching its parameters.[85] When concepts that are meant to be precise, like cyberterrorism and hacktivism, are extended to make them indistinguishable from each other and from more general concepts like cyberattacks, we undermine our ability to comprehend the phenomena these concepts are meant to explain. There is a real and compelling difference between a nonviolent denial-of-service attack or website defacement that seeks to publicize a cause, and a computer attack against industrial controllers or SCADA systems intended to terrorize a large audience by causing substantial physical damage to people and property. Both acts are politically motivated, computer-generated attacks on computer systems, but here their similarities end. The first act seeks to communicate through disruption; the second, through terror. The definitions we use to describe these phenomena must be precise enough to allow us to identify such distinctions and to apply them consistently to the phenomena we seek to explain. Broad definitions and applications of cyberterrorism, including those that stretch the concept to include hacktivism and all

manner of cyberattacks, fail to make such distinctions. In doing so, they confuse rather than clarify.

Conceptual precision is not important for just understanding phenomena, but also for gathering and interpreting information about them as well. As Giovanni Sartori observed many years ago, concepts need to be sufficiently precise and discriminating to allow researchers to collect data that correspond to the concepts they are meant to explain. When concepts are not sufficiently precise, because of definitional sloppiness and concept stretching, then mistaken data gathering and misinterpretation are unavoidable.[86] This occurs when data that correspond to a general concept, such as cyberattacks, are mistakenly applied to a more precise concept like cyberterrorism. When data misclassified in this way are used for interpretation, it contributes to a false understanding of both concepts. In the cybersecurity field, examples of cyberattacks are frequently mischaracterized as cyberterrorism, leading to significant over-reporting of the latter. One study that likens cyberattacks to cyberterrorism claims that there have been millions of cyberterrorist incidents.[87] Another claims that "the actual number" of cyberterrorist attacks annually "is so colossal that there could not be accurate reporting on just how frequently those attacks occur."[88] Such mischaracterizations suggest that cyberterrorism is pervasive, with thousands of incidents a day. The reality is that few, if any, of these incidents are cyberterrorism, as opposed to cyberattacks more broadly. These mischaracterizations also obscure what terrorists are actually doing online, that is, using the Internet as a communications and coordination tool to advance their cause rather than to destroy critical infrastructures through complex computer attacks.

CONCLUSION

Cyberterrorism may not have happened yet, but that does not mean it never will. Stuxnet, in particular, has brought us closer to cyberterrorism than any other recent incident. To be sure, the purpose of the Stuxnet attacks was to sabotage Iran's uranium enrichment program, not spread terror. But the demonstration effect of the cyberweapon was enormous, showing the world how cyberterrorism could potentially unfold, by attacking the computer controllers and SCADA systems that regulate industrial machinery. Perhaps, even more troubling, the Stuxnet genie is out of the bottle: the code has spread to computer programmers and hackers around the world. To date, the damage caused by Stuxnet's spread has been minimal, because the worm was carefully calibrated to attack only the industrial controllers and electrical motors used at Natanz and contained a built-in expiration date that has since passed.[89] The danger now, as former White House czar for cybersecurity Richard Clarke points out, is that thousands of programmers and hackers "are playing with it," modifying the code in ways that might allow them to attack other industrial controllers and SCADA systems for their own purposes.[90] Many specialists believe it is only a matter of time before the United States is targeted with a Stuxnet-like cyberweapon.[91]

But perhaps not. Given the history of knee-jerk hyperbole surrounding "digital Pearl Harbors," "cyber-Armageddons," and other overwrought warnings that never panned out, an element of caution remains in order, even when assessing the threat of cyberterrorism today. After Boden caused sewage water to pollute the area surrounding a water-treatment plant

in Queensland in 2000, computer security specialists sounded the alarm with chilling forecasts that terrorists would soon use SCADA attacks to wreak havoc on critical infrastructures in the United States. While numerous incidents since then have confirmed that poorly protected industrial controllers and SCADA systems are vulnerable to remote penetration, none of these attacks produced destructive effects anywhere near the doomsday scenarios predicted by many.[92] One reason was that the same security specialists sounding the alarm were also studying the Boden attack and other incidents to identify—and fix—the vulnerabilities hackers were exploiting. A second reason was that cyberattacks that caused physical damage to industrial machines, including the incident in Queensland, required substantially greater expertise than denial-of-service attacks, website defacements, and other standard hacking techniques. For all the fears that Stuxnet has reignited, the attack has been widely studied by computer security specialists who have developed patches for many of the security flaws the worm exposed. While Stuxnet was not as sophisticated as many media reports suggested, developing and deploying the worm still involved a level of technical expertise that is beyond the capacity of most nonstate terrorists today. State hackers and cybercriminals with the necessary skills and knowledge to exploit Stuxnet's code to malicious effect are more likely to use such weapons to wage cyberwar or to commit an online crime.

If the history of contemporary 4th Wave terrorism is any guide, nonstate terrorists, including al-Qaeda and its Islamist affiliates, are much more likely to carry out flesh-and-blood attacks using simpler, easier-to-acquire conventional weapons—guns, bombs, and

knives—than intricate attacks against SCADA systems and industrial controllers, the fear-inducing capacity of which remains uncertain. While terrorists have increased their use of information technology in recent years, they use these tools instrumentally to facilitate their own real-world activities, rather than to bring the Internet crashing down. The real cyberthreat from nonstate terrorists lies in their ability to exploit the Internet to raise funds, research targets, and recruit and radicalize enthusiasts rather than to execute SCADA attacks. Cyberterrorism may well be in our future, but for now, at least, the virtual dangers we face have a lot more to do with online crime, hacktivism, and even cyberwarfare than they do with cyberterrorism.

ENDNOTES - CHAPTER 6

1. Nicole Perlroth, "Attacks on 6 Banks Frustrate Customers," *The New York Times*, September 30, 2012; Nicole Perlroth and Quentin Hardy, "Bank Hacking Was the Work of Iranians, Officials Say," *The New York Times*, January 8, 2013, available from *www.nytimes.com/2013/01/09/technology/online-banking-attacks-were-work-of-iran-us-officials-say.html;* David E. Sanger, "Obama Order Sped Up Wave of Cyberattacks Against Iran," *The New York Times*, June 1, 2012.

2. John Arquilla and David Ronfeldt, "Cyberwar is Coming!" *Comparative Strategy,* Vol. 12, No. 2, Summer 1993, pp. 141-165.

3. Elisabeth Bumiller and Thom Shanker, "Panetta Warns of Dire Threat of Cyberattack on U.S.," *The New York Times,* October 11, 2012.

4. David Shamah, "Latest viruses could mean 'end of world as we know it,' says man who discovered Flame," *The Times of Israel*, June 6, 2012.

5. James A. Lewis, "Cybersecurity and Critical Infrastructure Protection," Center for Strategic and International Studies (CSIS) Working Paper, Washington, DC: CSIS, January 2006.

6. Gabriel Weimann, "Cyberterrorism: The Sum of All Fears?" *Studies in Conflict and Terrorism*, Vol. 28, No. 2, 2005, p. 131.

7. Joshua Green, "The Myth of Cyberterrorism," *Washington Monthly,* November 2002.

8. National Research Council, Committee on Offensive Information Warfare, *Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities*, Washington, DC: National Academies Press, 2009, pp. 1, 10.

9. David E. Sanger, John Markoff, and Thom Shanker, "U.S. Steps Up Effort on Digital Defenses," *The New York Times*, April 27, 2009.

10. National Research Council, Committee on Offensive Information Warfare, *Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities*, p. 11.

11. Sharon Weinberger, "Top Ten Most-Destructive Computer Viruses," *Smithsonian Magazine,* March 19, 2012, available from *smithsonianmag.com/science-nature/Top-Ten-Most-Destructive-Computer-Viruses.html*, accessed November 12, 2013; Andrew Nicholson, Stuart Webber, Shaun Dyer, Tanuja Patel, and Helge Janicke, "SCADA Security in Cyber-Warfare," *Computers and Security,* Vol. 31, No. 4, June 2012, pp. 418-436.

12. Sarah Gordon and Richard Ford, "On the Definition and Classification of Cybercrime," *Journal in Computer Virology*, Vol. 2, No. 1, August 2006, p. 14.

13. Phil Williams, "Organized Crime and Cybercrime: Synergies, Trends and Responses," *Global Issues* Vol. 6, No. 2, 2001, available from *crime-research.org/library/Cybercrime.htm*, accessed October 16, 2013; Rob McCusker, "Transnational organised cyber crime: distinguishing threat from reality," *Crime, Law, and Social Change,* Vol. 46, Iss. 4, December 2006, pp. 257–273.

14. James P. Farwell and Rafal Rohozinski, "Stuxnet and the Future of Cyber War," *Survival: Global Politics and Strategy*, Vol. 53, No. 1, February-March 2011, pp. 23-40.

15. Gordon and Ford.

16. Andrew Conte, "PSU grad accused of orchestrating $1.2B in illegal drug sales on secret Web network," *Pittsburgh Tribune-Review,* October 4, 2013; Joseph Goldstein. "Arrest in U.S. Shuts Down a Black Market for Narcotics," *The New York Times,* October 2, 2013.

17. "Lulz" is a mean-spirited derivative of the digital portmanteau LOL ("laugh out loud"). With lulz, the laughter is at the expense, and often deep personal embarrassment, of another. Gabriella Coleman, "Our Weirdness Is Free, The Logic of Anonymous—Online Army, Agent of Chaos, and Seeker of Justice," *Triple Canopy,* No. 15, January 13, 2012; Parmy Olson, *We Are Anonymous: Inside the Hacker World of LulzSec, Anonymous, and the Global Cyber Insurgency,* New York: Little, Brown and Company, 2012.

18. Oona A. Hathaway, Rebecca Crootof, Philip Levitz, Haley Nix, Aileen Nowlan, William Perdue, and Julia Spiegel, "The Law of Cyber-Attack," *California Law Review,* Vol. 100, No. 4, August 2012, pp. 817-885; Coleman; Gordon and Ford; Olson.

19. Siobhan Gorman, "Annual U.S. Cybercrime Costs Estimated at $100 Billion; Study Casts Doubt on Previous, Higher Figures," *The Wall Street Journal,* July 22, 2013; Dorothy E. Denning, "Whither Cyber Terror?" *10 Years after September 11: A Social Science Research Council Essay Forum,* 2011, available from *essays.ssrc.org/10yearsafter911/whither-cyber-terror/,* accessed September 20, 2013.

20. Steven A. Hildreth, "Cyberwarfare," *Congressional Research Service Report for Congress,* June 19, 2001; Hathaway *et al*.

21. National Research Council, Committee on Offensive Information Warfare, *Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use* of *Cyberattack Capabilities*, p. 174; John Markoff, "Before the Gunfire, Cyberattacks," *The New York Times*, August 12, 2008.

22. Izz ad-Din al-Qassam Cyber Fighters (2012a), "Operation Ababil, The second week," available from *hilf-ol-fozoul.blogspot*

.com/2012/09/cyber-fighters-groups-statement_25.html, accessed October 1, 2012; Izz ad-Din al-Qassam Cyber Fighters (2012b), "Phase 2 Operation Ababil," available from *pastebin.com /E4f7fmB5*, accessed on October 15, 2013; Izz ad-Din al-Qassam Cyber Fighters, "Operation Ababil, 2nd Phase/4th Week," available from *pastebin.com/dwu47giH*, accessed September 23, 2013.

23. Nicole Perlroth and David E. Sanger, "Cyberattacks Seem Meant to Destroy, Not Just Disrupt," *The New York Times*, March 28, 2013; Nicole Perlroth and Quentin Hardy, "Bank Hacking Was the Work of Iranians, Officials Say," *The New York Times*, January 8, 2013.

24. Joseph J. St. Marie and Shahdad Naghshpour, *Revolutionary Iran and the United States: Low-intensity Conflict in the Persian Gulf*, London, UK: Ashgate, 2011.

25. Farwell and Rohozinski.

26. Ralph Langner, "Stuxnet: Dissecting a Cyberwarfare Weapon," *IEEE Security and Privacy*, May/June 2011, p. 49.

27. *Ibid*.; Sanger.

28. Farwell and Rohozinski.

29. Ron Rosenbaum, "Richard Clarke on Who Was Behind the Stuxnet Attack," *Smithsonian Magazine*, April 2012, available from *smithsonianmag.com/history-archaeology/Richard-Clarke-on-Who-Was-Behind-the-Stuxnet-Attack.html*, accessed November 12, 2013.

30. Sanger.

31. Hildreth; Hathaway *et al*.; National Research Council, Committee on Offensive Information Warfare, *Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use* of *Cyberattack Capabilities*.

32. National Research Council, Committee on Offensive Information Warfare, *Technology, Policy, Law,* p. 278.

33. Evan F. Kohlmann, "The Real Online Terrorist Threat," *Foreign Affairs,* Vol. 85, No. 5, September/October 2006, pp. 115-124; Denning, "Whither Cyber Terror?"

34. National Research Council, Committee on Offensive Information Warfare, *Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities*, p. 278; Isabel Kershner, "2 Israeli Web Sites Crippled as Cyberwar Escalates," *The New York Times*, January 16, 2012.

35. Gabriella Coleman, "Hacker Politics and Publics," *Public Culture,* Vol. 23, No. 3, 2011, p. 516.

36. Coleman, "Hacker Politics and Publics"; Coleman, "Our Weirdness Is Free, The Logic of Anonymous—Online Army, Agent of Chaos, and Seeker of Justice"; Olson, pp. 32-33.

37. National Research Council, Committee on Offensive Information Warfare, *Technology, Policy, Law,* p. 172.

38. Jaak Aaviksoo, "Cyberspace: A New Security Dimension at Our Fingertips," public presentation at the CSIS, Washington, DC, November 28, 2007; National Research Council, Committee on Offensive Information Warfare, *Technology, Policy, Law,* p. 172.

39. Church of Scientology, "Statement about 'Anonymous'," available from *newhavenindependent.org/index.php/archives/entry/masked_protesters_picket_scientologists/*, accessed October 16, 2013.

40. Dorothy E. Denning, "Cyberterrorism," testimony before the Special Oversight Panel on Terrorism, Committee on Armed Services, U.S. House of Representatives, May 23, 2000.

41. National Research Council, Committee on Offensive Information Warfare, *Technology, Policy, Law,* p. 172.

42. Denning, "Cyberterrorism."

43. Similar to industrial controllers, SCADA systems are computers that run industrial machines. They are widely used to manage electricity grids, regulate temperatures in nuclear power plants, and make sure trains run on time. They also have a host of other industrial uses. Nicholson *et al*., 2012, pp. 418-419.

44. Marshall Abrams and Joe Weiss: "Malicious Control System Cyber Security Attack Case Study: Maroochy Water Services, Australia," *National Institute of Standards and Technology Report*, July 23, 2008, available from *csrc.nist.gov/groups/SMA/fisma/ics/documents/Maroochy-Water-Services-Case-Study_report.pdf*, accessed November 13, 2013; Barton Gellman, "Cyber-Attacks by Al Qaeda Feared: Terrorists at Threshold of Using Internet as Tool of Bloodshed, Experts Say," *The Washington Post*, June 27, 2002.

45. Sanger; Gellman.

46. Jessica Stern, *The Ultimate Terrorists*, Cambridge, UK: Harvard University Press, 1999; Bruce Hoffman, *Inside Terrorism*, Rev. and Expanded Ed., New York: Columbia University Press, 2006.

47. Abrams and Weiss; Denning, "Whither Cyber Terror?"; Sanger; Gellman; Green.

48. Denning, "Cyberterrorism."

49. Maura Conway, "What Is Cyberterrorism?" *Current History,* Vol. 101, No. 659, December 2002, pp. 436-442; Weimann.

50. Denning, "Whither Cyber Terror?"

51. John Rollins and Clay Wilson, *Terrorist Capabilities for Cyberattack: Overview and Policy Issues*, Congressional Research Service (CRS) Report for Congress, Washington, DC: CRS, January 22, 2007, p. 3.

52. Wilson, p. 4.

53. Conway, p. 436.

54. Mark M. Pollitt, "Cyberterrorism: Fact or Fancy?" *Proceedings of the 20th National Information Systems Security Conference,* October 1997, pp. 285-289.

55. Kelly A. Gable, "Cyber-Apocalypse Now: Securing the Internet Against Cyberterrorism and Using Universal Jurisdiction as a Deterrent," *Vanderbilt Journal of Transnational Law*, Vol. 43, No. 1, January 2010, p. 63.

56. Hoffman, pp. 16, 25-27.

57. Brian Michael Jenkins, "The Study of Terrorism: Definitional Problems," *RAND Paper Series*, P-6563, Santa Monica, CA: RAND, December 1980.; David Claridge, "State Terrorism: Applying a Definitional Model," *Terrorism and Political Violence,* Vol. 8, No. 3, Autumn 1996, pp. 47-63; Alexander L. George, ed. *Western State Terrorism,* New York: Blackwell Publishers, 1991; Richard Jackson, "The Ghosts of State Terror: Knowledge, Politics and Terrorism Studies," *Critical Studies on Terrorism*, Vol. 1, No. 3, 2008, pp. 377-392.

58. Hoffman; Daniel Byman, *Deadly Connections: States that Sponsor Terrorism,* New York: Cambridge University Press, 2005; Paul R. Pillar, *Terrorism and U.S. Foreign Policy*, Washington, DC: Brookings Institution Press, 2001; Bureau of Counter-Terrorism, Country Reports on Terrorism 2012, Washington, DC: U.S. Department of State, May 2013, available from *www.state.gov/documents/organization/210204.pdf*, accessed October 24, 2013.

59. Jenkins, pp. 2-3.

60. Alex P. Schmid and Albert J. Jongman, *Political Terrorism: A New Guide to Actors, Authors, Concepts, Data Bases, Theories, & Literature,* New Brunswick, NJ: Transaction Publishers, 2005.

61. Adapted from Hathaway *et al*., p. 833.

62. Conway; Dorothy E. Denning, "Activism, Hacktivism, and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy," in John Arquilla and David Ronfeldt, eds., *Networks and Netwars*, Santa Monica, CA: RAND, 2001, pp. 239-288, Dorothy Denning, "Stuxnet: What Has Changed?" *Future Internet*, Vol. 4, 2012; Michael Stohl, "Cyber terrorism: a clear and present danger, the sum of all fears, breaking point, or patriot games?" *Crime, Law and Social Change* Vol. 46, No. 4, 2006, pp. 223-238; Weimann.

63. Denning, "Stuxnet," pp. 672-687; Gellman.

64. Denning, "Stuxnet," p. 678.

65. Green; Denning, "Whither Cyber Terror?"

66. Kohlmann; Denning, "Whither Cyber Terror?"

67. Green.

68. Denning, "Stuxnet," p. 678; Green; Weimann.

69. Dan Verton, "Experts: Don't dismiss cyberattack warning," *Computerworld*, November 18, 2002, available from *computerworld.com/s/article/76000/Experts_Don_t_dismiss_cyberattack_warning*, accessed October 28, 2013.

70. Gellman.

71. Denning, "Whither Cyber Terror?"

72. Verton.

73. Denning, "Whither Cyber Terror?"; Denning, "Stuxnet."

74. Denning, "Whither Cyber Terror?"

75. Quoted in Eben Kaplan, "Q&A: Terrorists and the Internet," *The New York Times*, March 6, 2006.

76. Kohlmann; Kaplan.

77. Sarah Gordon and Richard Ford, "Cyberterrorism?" *Computers and Security,* Vol. 21, No. 7, 2002, p. 637.

78. Conway; Weimann.

79. Amy Embar-Seddon, "Cyberterrorism: Are We Under-Siege?" *American Behavioral Scientist,* Vol. 45, No. 6, February 2002, pp. 1033-1043; Weimann.

80. National Research Council, System Security Study Committee, *Computers at Risk*, Washington, DC: National Academies Press, 1991, p. 7.

81. Jonathan Matusitz, "Cyberterrorism: How Can American Foreign Policy Be Strengthened in the Information Age?" *American Foreign Policy Interests,* Vol. 27, No. 2, 2005, p. 137.

82. *Ibid.*, p. 138.

83. Gable, p. 63.

84. *Ibid.,* pp. 60-62.

85. Giovanni Sartori, "Comparing and Miscomparing," *Journal of Theoretical Politics,* Vol. 3, No. 3, 1991, pp. 243-257.

86. Giovanni Sartori, "Concept Misformation in Comparative Politics," *American Political Science Review*, Vol. 64, No. 4, December 1970, pp. 1033-1053; Giovanni Sartori, "Comparing and Miscomparing."

87. Gable, p. 62.

88. Elizabeth Minei and Jonathan Matusitz, "Cyberterrorist Messages and Their Effects on Targets: A Qualitative Analysis," *Journal of Human Behavior in the Social Environment*, Vol. 21, No. 8, 2011, p. 1002.

89. Farwell and Rohozinski.

90. Rosenbaum.

91. Sanger; Paul K. Kerr, John Rollins, and Catherine A. Theohary, *The Stuxnet Computer Worm: Harbinger of an Emerging Warfare Capability*, CRS Report for Congress, Washington, DC: CRS, December 9, 2010.

92. Nicholson *et al*.

CHAPTER 7

CHINA'S RECONNAISSANCE AND SYSTEM SABOTAGE ACTIVITIES: SUPPORTING INFORMATION DETERRENCE

Timothy L. Thomas

Disclaimer: The views expressed in this report are those of the author and do not necessarily represent the official policy or position of the Department of the Army, Department of Defense, or the U.S. Government.

The Foreign Military Studies Office (FMSO) assesses regional military and security issues through open-source media and direct engagement with foreign military and other security specialists to advise Army leadership on issues of policy and planning critical to the U.S. Army and the wider military community.

INTRODUCTION

For the past decade, numerous nation-states have accused China of conducting extensive reconnaissance activities against their militaries, banks, and industries. Due to the anonymity of the Internet, it is difficult to pin the blame for these reconnaissance activities on any one nation. However, the feeling appears to be widespread among nation-states that Chinese hackers lie behind the majority of these intrusions.

These China-based cyberactivities appear aimed at uncovering nation-state digital vulnerabilities in peacetime. As such, they are part of a larger digital strategy to accomplish two objectives. The first is to gain access to important industrial information that

would increase the military capability of the People's Liberation Army (PLA). The second is to map any potential opponent's digital terrain, uncover vulnerabilities, or plant dormant viruses, thereby establishing a digital strategic advantage so that China can "win victory before the first battle" if such a confrontation ever occurs.

One of the more offensive actions that China is practicing is system sabotage operations. When this capability is perfected, information deterrence can be generated. This chapter discusses Chinese strategic reconnaissance activities, how they lead to the ability to conduct "system sabotage," and how the latter leads to the development of information deterrence concepts. All of the activities are part of a plan to "gain victory before the first battle."

RECONNAISSANCE

In a 2010 article in *Qiushi* (a semiofficial journal of the Communist Party of China's Central Committee), Jiang Yong discussed the issues of cyberspace and information superiority. Cyberspace was defined as:

> A network consisting of the interconnected computers, satellites, cables, and various types of information terminals. It connects political, military, business and trading, financial, and transportation entities in all trades and industries, including governmental and non-governmental organizations, enterprises and individuals, and thus shapes the 'nerve system' on which the contemporary world and all sovereign states rely for normal operation.[1]

Cyberspace contains a massive volume of information that is used to spread a user's influence, which

can be either benevolent or harmful or a combination of both. Information flows have become a strategic resource, in China's opinion. China worries about U.S. hegemony in cyberspace, since the latter controls 10 of the world's 13 root servers and, therefore, information flows. China states that, if alterations are made to information in the servers or deception is used here, it can provide the United States with the power to control the information resources of another nation. China believes the United States also controls the Internet through the Internet Corporation for Assigned Names and Numbers (ICANN), which assigns domain names and digital addresses.[2] Therefore, China is pressing to change the system and is developing cyberconcepts with Russia, the International Telecommunications Union, and others. Information superiority, Jiang concluded, is becoming the key factor in determining future calculations of comprehensive national power.[3]

For that reason, cyber-reconnaissance is becoming more important than ever. Over a decade ago, China developed a theoretical framework dedicated to cyber-reconnaissance activities, which have enabled Chinese experts to examine the cybervulnerabilities of a potential opponent's cyberinfrastructure. The best example of this conceptual framework is the book *Direct Information War*, written by Dai Qingmin, formerly the head of the General Staff Department that handled information warfare activities. Dai discussed a host of network reconnaissance actions. He stated that in computer network warfare, being able to seize intelligence related to operational objectives is of primary importance. Only then can one "Know yourself and know the enemy, and you need not fear the results of a hundred battles." The process of gaining enemy computer network intelligence is termed "computer network reconnaissance." Computer network recon-

naissance, Dai added, is mainly information about the computer network system under reconnaissance, such as the hardware configuration of the topological structure and all network nodes, the communication systems, encryption methods, computer network protocols, the system platforms and system capabilities of software, and the geographical location of the target nodes.[4]

Dai discussed the importance of cyber-reconnaissance:

> Computer network reconnaissance is a prerequisite factor for seizing victory in network warfare. The status and role of computer network reconnaissance in computer network warfare is proving to be decisive. Possessing complete intelligence not only creates the necessary conditions for controlling battlefield initiative, it also lays the foundation for giving full play to strategic victory in military competition, and it can even begin the path for attaining the ideal state of 'breaking the enemy's resistance without fighting.' For this reason, computer network intelligence reconnaissance with the objective of contending for intelligence and with the goal of 'knowing the enemy' is both an effective measure for military competition and also an important strategy for military competition.
>
> Computer network reconnaissance is the basis for computer network warfare, and it runs through the entire course of computer network warfare. It provides accurate intelligence support for computer network attack and it guides offensive computer network operations such as choosing opportune moments, places, and measures for attack, and it collects evidence used to evaluate attack effectiveness.[5]

Dai's focus is on collecting technical parameters and specific properties of all categories of information weapon systems and electronic information products.

He described various reconnaissance techniques that have played important roles in computer network reconnaissance operations. These techniques include information interception, code breaking, conventional reconnaissance, covert reconnaissance, and infiltration reconnaissance. Intelligent reconnaissance techniques, including data mining and fusion processing, can also be used to gain as much sensitive information from inside target networks as possible and to use counter-reconnaissance techniques to safeguard one's own information security.

Network Information Interception.

Network information interception techniques are one of the main methods of computer network reconnaissance, offering important research content for computer network warfare. The data in the information transmitted online can be illicitly intercepted and monitored, thereby acquiring sensitive information from the side under reconnaissance, the only requirement being to impose physical or logical measures on network transmission links.

Code Breaking.

Most information that is intercepted, especially important sensitive information, is encrypted. Therefore, it is necessary first to crack the code of the encrypted text. Only then is it possible to carry out the next steps of analysis and processing. Code breaking techniques can be used to get into military computer networks surreptitiously via the common networks to which they connect.

Conventional Computer Network Reconnaissance.

Conventional computer network reconnaissance refers to scanning and surveying target mainframes or networks on the Internet and acquiring useful information, such as security loopholes that exist in the target computer network system. This provides an important foundation for the next step in carrying out a network attack. Each week, 15-30 loopholes may emerge, and they can affect software and hardware installations at great range, including operating systems themselves and their support software, computer network clients and server software, computer network routers and security firewalls, etc.

Covert Network Reconnaissance.

There are many methods used to conduct covert reconnaissance. For the most part, they can be separated into two categories. The first is making reconnaissance actions secretive to the best of one's ability, e.g., adjusting reconnaissance tactics according to the security defense installations of the target system in order to attain the goal of not being discovered. The second is using some deceptive techniques and gaining the trust of the mainframe of the side under reconnaissance and its operators in order to gain valuable information.

Network Infiltration Reconnaissance.

Conventional computer network reconnaissance techniques have no way of penetrating firewalls to search the information inside the local area networks located behind the firewalls. For this reason,

network infiltration techniques have emerged as the times required. The great majority of firewalls can frequently carry out extremely strict filtering of the links coming from outside the network to inside the network, but they are neglectful of taking precautions against the links sent out from the inside. Infiltration reconnaissance makes use of Trojan horses to serve as probes. They collect large volumes of information and ultimately penetrate the firewall from the inside to send information back outside.

Intelligent Network Reconnaissance.

Intelligent network reconnaissance uses intelligent computer network probing programs that act on their own in roaming computer networks to probe fixed-computer network targets, monitoring and probing targets and sending back collected intelligence information via covert communications methods.

Network Counter-Reconnaissance.

Infiltration detection systems conduct real-time monitoring of computer networks without affecting the performance of the computer networks, collecting and analyzing information from a number of key nodes and seeing whether there are behaviors that violate security strategy or indications of infiltration in the computer network. In addition, computer hackers can also be used to send a flood of false and useless information intentionally to the enemy's information systems, creating a "mighty information torrent" that clogs or crams its information transmission channels. This leaves the enemy with no way to timely and

effectively collect, transmit, and process the information it needs in order to delay enemy information reconnaissance.[6]

The Chinese have developed an extensive cyber-reconnaissance organization within the General Staff. This organization was highlighted in the report, *The Chinese People's Liberation Army Signals Intelligence and Cyber Reconnaissance Infrastructure*.[7] Authors Mark Stokes, Jenny Lin, and L. C. Russell Hsiao, writing for the Project 2049 Institute, discussed both the PLA's Third Department (signals intelligence collection, cryptology, computer security, and analysis agency) and the Fourth Department (radar, electronic support measures, electronic warfare, electronic intelligence, and electronic countermeasures). Since the Third Department is the focus of reconnaissance activities, it is discussed here. It is believed that Major General Meng Xuezheng serves as the director of the Third Department.

The authors note that their Third Department discussion is tentative and theoretical. They analyze two areas: the command structure and subordinate research institutes; and the department's 12 operational bureaus. The command has a headquarters, political department, logistics department, science and technology intelligence bureau, and science and technology equipment bureau. Key subordinates to the Department include the 56th Research Institute (supercomputing), the 57th Research Institute (communications intercepts, signals processing, and satellite communications), and the 58th Research Institute (cryptology and information security technology).[8]

The study lists the operational bureaus of the Third Department:

- 1st Bureau (61786 Unit)—decryption, encryption, information security;

- 2nd Bureau (61398 Unit)—U.S. and Canada focus;
- 3rd Bureau (61785 Unit)—line of sight radio communications, direction finding, and emission control;
- 4th Bureau (61419 Unit)—Japan and Korea focus;
- 5th Bureau (61565 Unit)—Russia focus;
- 6th Bureau (61726 Unit)—no mission given; Wuhan University network attack and defense center is located in this area of operation;
- 7th Bureau (61580 Unit)—some computer network attack and computer network defense, some work on the U.S. network-centric concept, and psychological and technical aspects of reading and interpreting foreign languages;
- 8th Bureau (61046 Unit)—Western and Eastern Europe, Middle East, Africa, Latin America;
- 9th Bureau (unknown Unit)—strategic intelligence analysis/database management, the most opaque bureau;
- 10th Bureau (61886 or 7911 Unit)—Central Asia or Russia, telemetry missile tracking, and nuclear testing;
- 11th Bureau (61672 or 2020 Unit)—Russia;
- 12th Bureau (61486 Unit)—satellites and space-based signals intelligence collection.[9]

These operational bureaus, according to the report, are separate from the technical reconnaissance bureaus (TRB) under the seven military region (MR) headquarters. The TRBs of the MRs include the following responsibilities:

- Beijing MR (66407 Unit)—Russia, along the Inner Mongolian border;

- Chengdu MR (78006 and 78020 Unit)—two TRBs; English, and computer network exploitation operations;
- Guangzhou MR (75770 Unit)—Internet viruses, and voice over Internet protocol;
- Jinan MR (72959 Unit)—oversees 670 technical specialists, microwave relay intercepts, Korean, Japanese, English, and other language specialists;
- Lanzhou MR (68002 and 69010 Units)—monitors border military activities;
- Nanjing MR (73610 and 76630 Units)—Western Pacific and Taiwan;
- Shenyang MR (65016 Unit)—Russian, Korean, and Japanese targets.[10]

Finally, the report listed several organizations associated with the Third Department. The PLA's Information Engineering University is the Third Department's training vehicle. According to the report, other organizations associated with computer network defense include:

- PLA Communications Security Bureau;
- China North Computation Center;
- Third Department Computing Center;
- National Research Center for Information Security Technology (Network Risk Assessment);
- PLA Information Security Evaluation and Certification Center;
- Information Security Research Institute;
- National Information Center (affiliated with science and technology equipment);
- National Information Security Engineering Technology Center.[11]

Today, Chinese authorities recognize that digital reconnaissance lays the groundwork for achieving future results and aids in the development and analysis of war-control issues.[12]

Reconnaissance thus enables the PLA to establish what is known as virtual *shi*, a strategic advantage or posture in the cyberworld. It is akin to taking the high ground in a physical battle. Retired Chinese General Tao Hanzhang noted that, with regard to an attacking force, *shi* is "the strategically advantageous posture before a battle that enables it to have a flexible, mobile, and changeable position during a campaign."[13] The attainment of strategic advantage through the planting of Trojan horses or viruses or spotting vulnerabilities in Western systems via reconnaissance activities helps ensure the ability to "win victory before the first battle." This requires mapping the cyber terrain of potential adversaries. Destructive codes that are planted in this terrain can be activated at a time of China's choosing. Further, knowing a system's weaknesses ahead of time helps attain the initiative in future battles, since system searches are not required—they have already been performed. Reconnaissance efforts can even take the form of a cognitive attack, such as controlling or manipulating the information a source receives, thereby causing a source to divulge important information. It is no secret that the Chinese have conducted extensive reconnaissance activities against numerous nations during the past several years. When confronted with accusations from several nation-states of numerous reconnaissance activities against their banks, militaries, and industries, Chinese authorities have continued to ignore such protests or to state that Chinese authorities have never conducted such activities. Electronic reconnaissance activities offer an opportunity

for the PLA to put into place the initial stages of its war-control planning process. Western analysts must become aware of the purpose behind these Chinese reconnaissance activities if they hope to keep the lead in 21st-century cyber prowess.

Of particular concern to Western societies should be the question of whether "shaping the situation" (as the U.S. terminologically designates digitized preemptive moves) could also involve controlling market societies and manipulating the electronic flows of free societies. Analysts need to be constantly aware of such potential. Can one well-placed and educated computer specialist serve this purpose today and stop the flow of 10,000 (or more) decisions in the marketplace? General Tao notes that there is the saying in China: "With only one man guarding the mountain pass, 10,000 men are not able to pass."[14]

SYSTEM SABOTAGE

The attainment of virtual *shi,* or strategic advantage, is the shaping mechanism that enables the use of preemptive moves and system sabotage activities. The Chinese have noted that a post-emptive move is "not an effective way to seize the initiative on the informatized battlefield."[15] Rather, in order to seize the initiative and control war in the initial state of a conflict, the active offense must be emphasized.

The book, *A Study Guide for Information Operations Theory*, described system sabotage warfare:

> What Is System Sabotage Warfare? The basic characteristics of informatized wars are that they are guided by information and that they consist of two systems fighting each other. This is why system sabotage is so important as it is the decisive mechanism of informa-

> tized operations, and it is the basic path to victory in informatized wars.
>
> The key point to system sabotage is in 'gaining control, using precision strikes for maximum damage, and paralyzing the enemy to subjugate his will.' This primarily entails using asymmetrical operations where the emphasis is on the 'destruction' part of the equation. Methods to attack weaknesses in a system include blocking network connections, breaking down the system architecture, and lowering operational effectiveness.[16]

The authors note that to make system sabotage effective, there needs to be a basic mode of thinking where the Chinese "destroy before conducting war, using destruction to aid in the fight." This is because under-informatized conditions, the core elements, and mechanisms for victory in war have undergone critical changes. There are significant differences in the procedures and centers of gravity for current operations compared to those in past wars. Destroying the material and technical foundation of a systems-integrated operation (the network-based information system) makes it impossible to adjust to problems on the battlefield. Obviously, conducting system sabotage requires an emphasis on destroying the network first before engaging in war.[17] For that reason, reconnaissance is very important because it identifies the nodes to destroy and in what order.

Cyber destruction refers to concentrated and continuous strikes on perception and information transmission systems on the battlefield. Implementing strikes where Chinese forces "kill two birds with one stone" means cutting off the "seamless link between sensors and launchers" to greatly hamper reconnaissance and detection, rapid response, and precision-

strike capabilities in an integrated operational system, thus creating the chance for dividing and ruling. When it comes to combat, this primarily refers to the favorable conditions in war for reducing the effectiveness of an operational system by conducting long-range precision strikes as the primary means of nonlinear, noncombat operations. Continued strikes on weak points break down an enemy's operational actions, shatter his operational intentions, and shake his will to resist. Of course, combat occurs during destruction, and vice versa, so the two are connected, but the focus and aim are different.[18]

Ping Zhiwei, a deputy director of the Campaign and Tactics Department of the Shijiazhuang Army Command Academy, and Majors Zeng Xiaoxiao and Zhang Xuehui, both from the Combined Tactics Teaching and Research Office of the same department and academy, noted that system sabotage is an operational mechanism of the system of systems (SoS) concept, along with domain control, effect control, integrated joint action, and self-organized collaboration.[19] The system sabotage mechanism aims to damage the structure of an adversary's operational system or, at least, disrupt it. The system-to-system confrontation and sabotage concept offer the capability to paralyze an adversarial operational system. Confrontations are aimed at severing an opponent's campaign and tactical systems. Sabotage is aided through maneuver and precision strike capabilities that keep an adversary guessing as to the place and time of a final assault.[20]

The military press in China often is peppered with references to the system sabotage concept. The press stated that this concept is a better method of fighting in the digital age than attrition; that it utilizes both hard and soft strikes; and that it is identified as an

operational pattern of war, whereas SoS is recognized as a characteristic of war.

Both concepts increase in use under informatized operational conditions. Methods are developed for employing system sabotage operations. Further, from exercises conducted in the field, it is clear that, on occasion, system sabotage methods are employed in the PLA's internal red versus blue exercises. The Mission Action-2010 exercises, for example, emphasized the position and role of information as the main element guiding the exercise, "firepower as the main battle in system sabotage," and the inspection and examination of system sabotage tactics, such as forward depth precision strikes and the selection and striking of key targets.[21] It appears that the system sabotage element is becoming a key part of any planning stage in PLA operations.

CHINA'S INFORMATION DETERRENCE CONCEPT: FROM 1999-2011

In 1999, Chinese author Shen Weiguang, the father of information war (IW) in China, wrote that the main IW battlefield will be intangible information space, and this will cause a change in the state of war. The effect of this change will include the softening of strategic objectives, the development of information deterrence as a new means of preventive action, the determination of military actions by the possession of information, the rising status of special forces, and the use of civilians on the battlefield.[22] Also writing in 1999, authors Lu Xiuru and Yu Zhengxue noted that intellectual information deterrence would be part of the intellectual-economic era that had descended on the world. This era will change the form of war and

no longer make violence necessary.[23] A 2000 article by noted Chinese stratagem specialist Li Bingyan stated that "future war will be a high-technology war within the framework of nuclear deterrence and information deterrence."[24] Thus, the Chinese have been discussing information deterrence for some time.

Interestingly, the definitions and discussions of the concept imply that cyber-reconnaissance and system sabotage (even though not listed by name) are key methods for imposing information deterrence against an opponent. A 2002 article in *Jiefangjun Bao* stated that information deterrence would make warfare more transparent.[25] So far, however, cyberactivities have been most often characterized as anonymous. The difficulties associated with uncovering identities are actually roadblocks to transparency. In 2003, editor Cai Cuihong's book, *Information Networks and International Politics*, proposed an information deterrence theory. The work views the information umbrella as more utilitarian than the nuclear umbrella. The information umbrella must be able to control information dominance and enable one side to see the adversary, while not allowing the adversary to see friendly activities. Control over information has become a new deterrent force as a result. Cai's work notes that:

> the side that controls information can manipulate the start and conclusion of wars, can use informatized weapons to paralyze enemy weapons and command systems, and can destroy the enemy's precision guided weapons.[26]

Information control appears to be a key aspect of a deterrent force, according to this explanation. Cai adds that "information network warfare under conditions of nuclear deterrence will be the new form of future international conflict."[27]

Network warfare includes network spy warfare and network attack and defense warfare. It is a form of fighting similar to IW.[28] Network warfare is low cost, full of surprises and anonymity, involves low personnel casualty costs, and is asymmetrical. The latter concept indicates that warfare could be conducted between countries, between countries and organizations, between countries and individuals, between organizations, between organizations and individuals, and even between individuals.[29]

Further, the mission has changed:

> The goal of computer network warfare is no longer annihilating the enemy and preserving oneself; rather, it is controlling the enemy and preserving oneself. What we call control is mainly influencing the thinking and will of the war decision-makers, putting the adversary into a darkroom, depriving him of the means for 'knowing himself and knowing the enemy,' and making it impossible to turn war potential into actual capabilities for engaging in war.[30]

The combat strength of China's armed forces will be balanced on the basis of its computing power, communications capacity and reliability, real-time reconnaissance capabilities, computer simulation capabilities, and other information elements. These elements can deter through misconceptions and psychological pressure. Without a distinction between front and rear, wars will truly become "people's wars," and their shape could be strongly influenced by invisible information space.[31]

If China is able to capture the strategic information resources of a country, then it can "win victory before the first battle." It can check an opponent's

behavior using non-war methods. In the past, China has referred to the United States as a cyber-hegemonic power. To attack this process, China is engaging in an information cultural offensive to takeover the war of words and use them as part of an information deterrence strategy. China must develop into a cyberpower if it is to develop the proper counter-deterrence ideology required to put up a unified fight. If military power is the main deterrent component of comprehensive power, then cyberpower cannot follow far behind. Cyberpower is most likely now considered the main ingredient of comprehensive power computations that the Chinese update regularly. China cannot utilize information deterrence if it is not a cyberpower. As a cyberpower, China can attempt to exploit foreign information resources, like it is apparently trying to do, as it procures terabytes of information from foreign nations' information systems via reconnaissance probes.

Information deterrence is defined in the PLA work, *The Science of Military Strategy* as:

> the deterrence that depends on the powerful performance of information science and information technology, and it is put into effect by the momentum and power of information warfare.[32]

In the world of information, the creation of deterrence from momentum is accomplished via the preparation of cyberpower, showing an enemy force a disposition or capability of cyber strength, and from actual cyberstrikes (perhaps the numerous computer reconnaissance activities of the Chinese).

Information deterrence, according to authors Peng Guangqian and Yao Youzhi, has the following features: first, permeability or the ability to permeate not only the military but also politics, the economy, cul-

ture, and science and technology; second, ambiguity, where the difference between information deterrence and information offense is hard to distinguish; third, diversity, such as unauthorized visits, malicious software, database disruption, etc.; fourth, two-way containment, where victims of an information attack may not be just the enemy but also others, to include oneself, due to the interconnectedness of networks and the global grid; and fifth, the use of people's war as a capability, that is, the potential of people joining in to combat an enemy on the net.[33]

The Science of Military Strategy also notes the following points, which apply more to the transmission of information ("information transmission is the necessary condition for creating the deterrent impact of strength and determination")[34] in order to impact the cognition of an opponent after extensive reconnaissance and the mapping of his systems:

> Deterrence requires turning the strength and the determination of using strength into information transmitted to an opponent, and to impact directly on his mentality in creating a psychological pressure to shock and awe the opponent . . . for this reason, effective strategic deterrence depends not only on strength and determination, but also on the above-mentioned information acquired by the deterred side. If the opponent has not acquired the above information or the information acquired is not accurate, or the deterred side believes that the acquired information is only bluffing and intimidation, then it cannot create creditable and effective strategic deterrence . . . only when the opponent on receiving deterrence information perceives and believes that if he acts rashly, he may suffer a more severe punishment, can the deterrence obtain the expected impact.[35]

Finally, Peng and Yao write that deterrence seeks momentum in several postures: creating momentum through military preparation, demonstrating momentum by showing one's disposition of strength, and augmenting momentum with military strikes.[36] Momentum is a term sometimes used interchangeably with strategic advantage when defining *shi*.

Writing in *China Military Science* in 2001, Zhao Xijun, a deputy commander of the Second Artillery (responsible for nuclear weapons), defined deterrence as:

> military actions in the form of a show of force between countries or political groups, or an indication of their resolve and readiness to use force, intended to make an opponent not dare to take hostile action or to escalate his actions.[37]

In this case, a show of force could simply be the presentation to the other side of the virtual layout of its cyberinfrastructure or digital terrain. If one were to attempt to extrapolate what China's cyberdeterrence theory might look like from its strategic deterrence theory, Zhao's article is an interesting contemporary start point. Zhao implies that deterrence theory is based on a combination of stratagems. These stratagems are using soft power and reconnaissance to win victory without war, and winning victory before the first battle. To Zhao, these specific formulations of the concept of deterrence theory in military thought come from the early works of Sun Tzu.[38]

Zhao notes that key factors in Sun Tzu's writings that influence contemporary deterrence theory include having superior military power, being fully prepared for war, having severe measures of punishment at one's disposal, having superb skill at "attacking strategy" and "attacking diplomacy," and making

one's ideology of deterrence be a lynchpin in a more complete system. The essence of deterrence is to resolve war with non-war measures. Western warfare is, in Zhao's opinion, very different conceptually than Chinese warfare. He feels Western theory is based on using war to achieve political objectives.[39]

A Chinese deterrence warfare strategy protects national interests; ensures that a nation's economy, science, and technology develop quickly; and offers the nation an invincible position in complex environmental and international disputes. Zhao adds that a counter-deterrent capability is the most effective method to stop the aggressive attempts of powerful nations from harming China's national interests. Flexibility and effectiveness are other important principles for the use of deterrence, which reflects the strategists' resolve, the manifestation of military strategy, and the embodiment of power. The key factors of deterrence must be cleverly assembled, flexibly mobilized, and securely developed to enable the ideal strategic outcome.[40] The anonymity of the Internet appears to fit these criteria perfectly.

First, a proper deterrence strategy includes the ability to judge the hour and to size up the situation while cautiously making decisions. Do what suits the time, place, and to coordinate actions. A nation must have a good grasp of the target and the objective of its deterrent posture. Again, this is where digital reconnaissance perfectly fills the bill. The correct timing and judgment must also be used when attacking an alliance. Initially, it is necessary to attack those countries with weak social and political foundations. These actions warn others and create a chain reaction of fear in the alliance.[41] The United States must theorize whether Chinese hacker intrusions are nothing more

than an attempt to size up the target and to map the U.S. infrastructure in order to spot vulnerabilities or if other purposes are present.

Second, Zhao notes that China should use an integrated deterrence approach. A single deterrent force is not sufficient to constitute effective deterrence. Comprehensive power must be employed to retain the strategic initiative. This thought brings to mind the work of Qiao Liang and Wang Xiangsui in their book, *Unrestricted Warfare*. The authors noted 24 different types of warfare and then theorized that a cocktail mixture of the methods would best bring about success. Thus, one might envision cyberpreemption, plus network reconnaissance, plus high-tech deception, plus financial market disruption, plus network deterrence, and so on.

Third, it is necessary to combine truth with falsehood, a direct application of stratagems. This combination can work to awe an enemy force into submission. Friendly forces must look for opportunities to attack an enemy force's power and resolve. They must create a posture of deterrence through a policy of truth and falsehood to deprive an enemy of willpower. When striking, they must do so resolutely, threatening targets with the greatest strategic value first, those the enemy does not want to see hit. Finally, psychological offense and strategy are the best tactics to gain victory. Deterrence is a test of power and resolve and a test of strategy and wisdom. When there is no smoke or gunpowder, strategy acts as a multiplier of power and resolve in deterrence. Strategic thought evolves and develops continuously, along with societal developments, especially as changes occur in the military sphere.[42]

No matter what type of deterrence is used:

> Its ultimate outcome is never merely the result of a comparison of the relative power of the two opponents. More important is the result of an analysis of the benefits which the deterring side and the deterred side might secure, of the price they each might have to pay. Implementing deterrence requires stepped up research of the threat the country faces. It requires scientific analysis and judgments.[43]

The 2004 Chinese book, *New Concepts During Military Transformation*: *Interpreting 200 New Military Terms*, defined several deterrence-related terms, to include the strategy of deterrence, strategic deterrence, nuclear deterrence, space deterrence, forward deterrence, full spectrum deterrence and, most importantly, information deterrence. The latter term, defined as follows, should be considered in conjunction with cyber-reconnaissance and system sabotage activities:

> With the backing of information weapons, intimidating and containing an adversary by threatening to use information weapons or when necessary carrying out an information attack. Information deterrence is essentially warning an adversary in advance about the possibility that information weapons will be used or information attacks will be carried out, as well as the serious consequences these actions may give rise to, causing the adversary to weigh the pros and cons and thereby producing psychological fear, forcing him to submit to the will of the side carrying out deterrence or abandon his original plans and thus allowing the side carrying out deterrence to achieve certain political objectives.[44]

An equally interesting article on strategic deterrence was published in 2004 in *China Military Science*.

Zhou Peng and Wen Enbin, from the Academy of Military Science, wrote that strategic deterrence refers to a:

> country or political bloc's military actions to compel an adversary to not dare take hostile action or escalate actions through a show of force or indicating the resolve of being prepared to use force, thereby achieving specific strategic goals.[45]

The possession of military strength is a prerequisite, along with the resolve to use force and the ability to make the one being deterred aware of one's capabilities. Informatized warfare can increase its deterrent power to be capable of achieving strategic objectives when combined with nuclear deterrence capabilities. Targeted deterrence can be achieved due to the controllability and flexibility of informatized measures.[46]

Former Chinese President Jiang Zemin recommended elevating deterrence to the level of strategy, according to Zhou and Wen. It should be used to contain war, delay its outbreak, or prevent its escalation. The core of new deterrence capabilities should be "assassin's mace" technologies, which would certainly fit cyber-reconnaissance and digital sabotage methodologies. Jiang emphasized mobilization measures as a priority development. Due to the fast nature of high-tech wars, a war's start can have decisive significance. For that reason, China "must establish an emergency mobilization combat force," as well as a strong traditional force capable of imposing deterrence in the strongest manner. In this way, China can confidently unleash the deterrent effect of people's war under high-tech conditions.[47] This emergency mobilization force in the Information Age could be the cybermilitias utilized in China. Policy analysts

Robert Sheldon and Steven Glinert wrote that the eight million strong militia system (defined as an armed organization composed of the masses not released from their regular work) in China is where the cybermilitia component can be found. Sheldon and Glinert have painstakingly uncovered 64 groups of either information militias or network militias. The relationship of the groups to Chinese developmental programs and high-tech development zones, along with their mobilization potential, possible wartime roles, geographic dispersion, and their functions, roles, and missions are discussed.[48]

It is only through comprehensive national strength, in Zhou and Wen's opinion, that a reliable deterrent effect can be generated. This image of strength must be developed now during China's so-called 20-year "window of strategic opportunity." Strength should be built around nuclear forces; the close integration of information resources, space resources, and conventional forces; and the people's war concept under high-tech conditions. A good deterrent force involves the use of nuclear deterrence, conventional deterrence, space deterrence, and information deterrence, again reminding one of cocktail warfare.[49] The authors add that:

> The acme of the art of strategic guidance is fully reflected in the proper selection and constant innovation of deterrence forms; it is the most real, most dynamic part of wielding strategic deterrence.[50]

In 2007, Major General Li Deyi stated that information deterrence would rise to a strategic level close behind nuclear deterrence. New and important modes of deterrence will include information-technology deterrence, information-weaponry deterrence, and

information-resource deterrence. Further, counter-information deterrence will be part of China's new mode of thinking.[51] Also in 2007, Senior Colonel Deng Yifei wrote that information deterrence would be a means, behind nuclear deterrence, to achieve national strategic goals and military strategic goals. Deng believes that information has become the core concept in military thinking. Vying for information supremacy and forming information deterrence capabilities are key areas of current military thought.[52]

In 2009, a few top nuclear generals in China wrote on information resources and the information components of weaponry as they apply to information deterrence. For example, author Zhou Fangyin noted that the concept of information deterrence is defined as forcing an adversary to lay down his weapons through demonstrations or through highlighting friendly force weaponry's advanced precision under informatized conditions.[53] In 2010, Senior Colonel Yao Yunzhu, writing in the U.S. journal *Air & Space Power* stated that China would continue to apply deterrence at the grand strategic level while depending more on "uncertainty" for a better deterrence effect.[54] Even though her comments were with regard to nuclear deterrence, they could easily fit an information deterrence scenario. In the age of computer hacking, uncertainty as to a hacker's actual identity or government connection is a common problem.

Other terms that may develop in Chinese thought would be political, economic, or even cultural information deterrence. The latter term could be interpreted as the cultural or soft power offensive. Economic information deterrence could mean that if a nation controls or manipulates economic information to a significant degree, then it may be capable of imple-

menting a type of economic information deterrence over another country. One nation could deter another simply based on the former's manipulation of and subsequent control over the latter's economic assets, which are generally in information bases.

CONCLUSIONS

China has continued to conduct reconnaissance activities against the United States and many other nations, ignoring repeated calls to cease such actions. Interestingly, Zhao offers a piece of advice in his article that could be used by U.S. policymakers to counter these reconnaissance activities. Zhao writes:

> If the opponent persists in having his own way and refuses to stop his hostile actions, then the other side must select the right time and an appropriate objective and execute high-intensity deterrent actions against the enemy, to include a warning strike. This is to demonstrate full and resolute determination to fight the enemy to the end, and force the enemy to abandon his high-handed scheme.[55]

Thus, if China refuses to stop its reconnaissance activities, the United States could conceivably, based on such a line of reasoning, fire a warning strike. Of course, a warning strike would be in the form of a cyberattack against a key utility or bank or military communication network. It is doubtful that it would include missile strikes, which could lead to further escalation scenarios. It is also doubtful the United States would react in such a way unless analysts were 100 percent certain as to the origin of the harmful activities, and whoever initiated them ignored repeated warnings to stop such activities.

The interesting thing to note about China's evolving concept of information deterrence is that it is based on extended reconnaissance to identify vulnerabilities in an opponent's cyberlandscape and on system sabotage methods as a means of intimidation. These two items offer inside knowledge of an opponent's system and increased uncertainty in the opponent as to what China actually knows; they also offer a realistic cybercombat power model that can be used to carry out planning. Together, both items can deter an opponent from acting. Interestingly, as Major General Li Deyi notes, there are various forms of information deterrence that can be developed: information-technology deterrence, information-weaponry deterrence, information-resource deterrence, and counter information deterrence, among others. China now appears well on its way to developing a mode of thinking that will integrate with modern technological advances. Where this mode of thinking will lead is anyone's guess.

ENDNOTES - CHAPTER 7

1. Jiang Yong, "Cyberspace: an Invisible New Battle Domain," *Qiushi*, No. 13, July 1, 2010.

2. *Ibid*.

3. *Ibid*.

4. Dai Qingmin, *Direct Information War*, Washington, DC: National Defense University Publishing House, 2002, pp. 55-153.

5. *Ibid*.

6. *Ibid*.

7. Mark A. Stokes, Jenny Lin, and L. C. Russell Hsiao, *The Chinese People's Liberation Army Signals Intelligence and Cyber*

Reconnaissance Infrastructure, Arlington, VA: Project 2049 Institute, November 2011.

8. *Ibid*., pp. 4-5.

9. *Ibid*., pp. 7-11.

10. *Ibid*., pp. 12-13.

11. *Ibid*., pp. 5-6.

12. "War Control," *China Military Science*, No. 6, 2005 (in English), p. 140.

13. Tao Hanzhang, *Sun Tzu's Art of War: The Modern Chinese Interpretation*, New York and London, UK: Sterling Innovation, p. 124.

14. *Ibid.,* p. 128.

15. Zhang Yu, Liu Sihai, and Xia Chengxiao, "On the Art of Controlling War Situation in Informatized Warfare," *China Military Science*, No. 2, 2010, pp. 24-31.

16. Xu Genchu and Dai Qingmin, *Study Guide for Information Operations Theory*, Beijing, China: Academy of Military Science Press, November 2005, pp. 395-396.

17. *Ibid.*

18. *Ibid*.

19. Ping Zhiwei, Zeng Xiaoxiao, and Zhang Xuehui, "A Study of the Mechanism of Information-System-Based System of Systems Operations," *China Military Science*, No. 4, 2010, pp. 34-43.

20. *Ibid*.

21. Chen Zhi, Pan Zhiqiang, and Gao Xiaowen, "A Certain Chengdu Military Region Group Army goes to an Ancient Battlefield in the Northwest—Advancing on Helan, Honing Elite Troops," *Jiefangjun Huabao*, November 18, 2010, pp. 44-45.

22. Timothy L. Thomas, "Chapter Two: The Third World War—Total Information War. The Views of Chinese IW Specialist Shen Weiguang," in Timothy L. Thomas, *Dragon bytes: Chinese information-war theory and practice from 1995-2003*, Fort Leavenworth, KS: Foreign Military Studies Office Publication, 2004, p. 35.

23. Lu Xiuru and Yu Zhengxue, "Forecasting the Trend of War in the Era of an Intellectual Economy," Beijing, China: *Jiefangjun Bao*, April 6, 1999, p. 6.

24. Li Bingyan, "Recognizing One's Own Historical Place in the Flood Tide of Reform: Written on the Conclusion of Discussion of the Topic, 'Is Warfare Gradually Softening?'" *Jiefangjun Bao*, December 26, 2000, p. 6.

25. Xu Guanhua, "S&T Development Impacts All Aspects of National Security," *Jiefangjun Bao*, May 22, 2002, p. 9.

26. Cai Cuihong, *Information Networks and International Politics*, Beijing, China: Hok-lam Press, 2003, pp. 163-164.

27. *Ibid*., p. 172.

28. *Ibid*., p. 173.

29. *Ibid*., pp. 176-177.

30. *Ibid*., pp. 177-178.

31. *Ibid*., p. 178.

32. Peng Guangqian and Yao Youzhi, eds., *The Science of Military Strategy*, English Edition, Beijing, China: The Military Science Publishing House, 2001, p. 220. In a glossary at the back of the English language translation of *The Science of Military Strategy*, in a translation provided by the Chinese, the term "cyber" is equated to the term informationization. That is, the same Chinese symbol was translated as "cyber, informationization." For that reason, this author sees little difference in cyberdeterrence and information deterrence. The terms are used interchangeably hereafter.

33. *Ibid*., pp. 220-221.

34. *Ibid*., p. 215.

35. *Ibid*., pp. 214-215.

36. *Ibid*., p. 222.

37. Zhao Xijun, "Victory without War and Modern Deterrence Strategy," *China Military Science*, 2001, pp. 55-60.

38. *Ibid*.

39. *Ibid.*

40. *Ibid.*

41. *Ibid.*

42. *Ibid.*

43. *Ibid.*

44. National Defense University, Scientific Research Department, *New Concepts during Military Transformation: Interpreting 200 New Military Terms,* Beijing: PLA Publishing House, 2004, p. 108.

45. Zhou Peng and Wen Enbin, "Developing a Strategic Deterrence Theory with Chinese Characteristics," *China Military Science*, No. 4, 2004, pp. 19-26.

46. *Ibid*., pp. 20-21.

47. *Ibid*., pp. 22-23.

48. Robert Sheldon and Steven Glinert, "Civil-Military Integration and China's Cyberspace Operations: A Case Study on PLA Cyber Militias," working paper for the "Conference on China and Cybersecurity," April 11-12, 2012. Used with the author's permission.

49. Zhou and Wen, pp. 24-25.

50. *Ibid*., p. 25.

51. Li Deyi, "A Study of the Basic Characteristics of the Modes of Thinking in Informatized Warfare," *China Military Science*, No. 4, 2007, pp. 101-105.

52. Deng Yifei, "A Revolution in Military Thinking in the Information Age," *China Military Science*, No. 6, 2007, pp. 71-78.

53. Zhou Fangyin, "The Effect of the Information Revolution on Military Affairs and Security," Beijing *Xiandai Guoji Guanxi*, August 1, 2001, pp. 28-32.

54. Yao Yunzhu, "China's Perspective on Nuclear Deterrence," *Air & Space Power Journal*, Spring 2011, p. 30.

55. *Ibid.*

CHAPTER 8

INFORMATION WARFARE A LA RUSSE

Stephen J. Blank

This is an expanded, revised, and updated version of an earlier article, "Russian Information Warfare as Domestic Counterinsurgency," published in 2013 in the journal, *American Foreign Policy Interests*, and derived from a paper presented at the Graduate School of Public and International Affairs - Strategic Studies Institute, U.S. Army War College, conference on Information Warfare, University of Pittsburgh, Pittsburgh, PA, November 1-2, 2012. The views expressed here do not represent those of the U.S. Army, the Defense Department, or the U.S. Government.

Information warfare (IW) and information operations (IO) have become ubiquitous and apparently permanent features of today's military-political-economic landscape. Though their consequences may be anything but routine, media discussions of these general phenomena or specific examples of them have become commonplace. This latter trend does owe much to the explosion of information technology and social media. However, a less appreciated but probably still major cause for the ubiquitous discussion of these subjects is the fact that, in the last 30 years, professionals and amateurs alike have come to embrace a new concept of security, both within states and between or among them, that vastly expands the concept of security from previous classical definitions.[1] According to this "new thinking about security," the internal structures of a society are as much an object of security practice and discourse as were the classical manifestations of a

country's defense policy. Thus, the internal infrastructures of a functioning society and/or state have now become objects of policymaking that postulates these structures as integral elements of a state's security. Consequently, a state's domestic structures have become the object of governments' discourse and actions about security and, particularly with regard to IO, a potential target of hostile adversaries. In a word, they have become securitized.[2]

Securitization denotes a process, mainly conceived in terms of political and/or military rhetoric and action, where leading actors in a state make an issue or series of issues a fixture of the state's security agenda and view them mainly, if not exclusively, through that prism. Issues hitherto not thought of as being related to national security are now seen in that context and through that prism. Political actors who first politicize an issue as a threat to security and then securitize it, aim to persuade relevant audiences—in this case, the political and military elite, and then the rest of the population—that the issue in question poses an "existential threat" to the country, either to its territory, the integrity of the state, its group identity, its environment, or its economic interests.[3] Consequently, government leaders who believe their state is inherently unstable or who grasp the illegitimacy of their rule are quick to believe that they are under assault by foreign adversaries using IO or IW to unseat them.

Securitization thus denotes political actors' efforts most often, though not exclusively, through speech or discourse, to take an issue out of normal politics and bring it into the realm of security and thus much closer state scrutiny. This process subordinates the issue to the competence of security organs, removes it from the public realm, substitutes secret bureaucratic

decisions for open politics, and often contravenes human or civil rights:[4]

> The aim of a 'securitizing move' is typically to enable 'emergency measures' that can secure the survival of a referent object. If and when the content of the security 'speech act' is acknowledged as legitimate by a (significant) 'audience' the issue in question has become successfully 'securitized'. It has been moved out of the sphere of 'normal politics' and into the sphere of 'emergency politics'; where it can be dealt with in an urgent manner and with fewer formal and informal restrains.[5]

Actors make "securitizing moves" not just to place an item on the agenda, but also to claim that their agency alone has either the capability to define or resolve the problem or to implement the appropriate solution.

This securitizing trend has immense significance for IW and IO both globally, and especially for Russia. Russian writers assume that IW and IO are legitimately deployable within the framework of combat operations, as a vital part of contemporary weapons systems, and simultaneously within domestic political struggles in societies that are otherwise formally at peace. For example, when writing in 2005 about the Russian Far East (RFE), Chairman of the Federation Council Defense and Security Committee Viktor Ozerov outlined a threat assessment emphasizing that military strengths not be the key determinant of national power in the system of international relations:

> The new geopolitics are based, as a rule, on the idea of "indirect wars" or "indirect influence." Overt military operations are being replaced by mechanisms of total regulation based on the concentration of financial-economic resources and information-psychological influence.[6]

Since then, Russian writers, and not just specialists on IW, have virtually made this idea a canonical aspect of Russian military thinking. Similarly, in 2006, Chief of the General Staff General Yuri Baluyevsky outlined a list of threats that comprised among them "planning and execution of information, psychological operations against the Russian Federation."[7] Thus, Baluyevsky not only expanded the scope of these threats, but he also gave the military the right to comment on and argue for policies against internal threats. He added to the notion that Russia is at all times under comprehensive internal and external threats to which the military must address itself, and which demand a defense policy response.

Ensuing discussions of threats to Russia followed along these lines. For example, in late-2006, the military journal *Voyenny Vestnik Yuga Rossii* (*The Military Herald of South Russia*) published an account of the tasks of the North Caucasus Military District's Personnel for 2007 that was a much more comprehensive threat assessment.[8] Among these threats were:

> Contemporary international military-political relations are characterized by a rigorous informational-psychological warfare that is aimed at undermining Russia's statehood and integrity. In this connection daily attacks are made according to two criteria: the external and internal information environments. Influence is being exerted on our country's population not by means of direct military interventions but by the adept exploitation of the national and religious contradictions within.[9]

Direct military threats thus included:

> the informational-psychological influencing and infiltration of different spheres of the Russian Federation's vital activity, which may entail the disabling of the system and military administration and control.[10]

As part of this debate, Director of the Academy of Military Science Retired General M. A. Gareyev offered a 2006 presentation that strongly rejected the notion that security threats originate within Russia and firmly stated that they all come from outside Russia.[11] So while he polemicized against the notion that IW represents a novelty in warfare, he accepted its newfound importance in contemporary war. Indeed, Gareyev advocated the creation of a:

> Separate, independent directorate, as part of the Presidential Staff of the Russian government that would be entrusted with coordinating information activity on a countrywide level—from intellectual security, the development of a national idea and shaping Russia's favorable image abroad to countering all types of subversive activity, including the ideological support and organization of 'color', 'velvet', and other sorts of revolutions.[12]

It should be noted that much, if not all, of this program has been put into active operation since then. Moreover, we see many of the consequences of this program in the global manifestations of Russian policy in the wake of Moscow's aggression against Ukraine and its ever-increasing domestic repressiveness against internal critics of the regime. It is precisely such organizations as Gareyev advocated that have been established, and that carry out much of the domestic and foreign activities that constitute Russian IW against both dissidents and foreign adversaries.

Finally, President Vladimir Putin himself has publicly and strongly endorsed this view. He has built upon earlier statements by leading officials and analysts by indicating that acts of IW are nonmilitary means that can be used for achieving strategic as well as military-political objectives. In his annual address to the Duma in 2007, Putin warned that:

> To be frank, our policy of stable and gradual development is not to everyone's taste. Some, making use of skillful use of pseudo-democratic rhetoric, would like to return us to the recent past, some in order to once again plunder the nation's resources with impunity and rob the people and the state, and others in order to deprive our country of its economic and political independence. There has been an increasing influx of money from abroad being used to intervene directly in our internal affairs. Looking back at the more distant past, we recall the talk about the civilizing role of colonial powers during the colonial era. Today, 'civilization' has been replaced by democratization, but the aim is the same—to ensure unilateral gains and one's own advantage, and to pursue one's own interests.[13]

Since then, Putin has openly claimed that information weapons and capabilities are an instrument for the leverage of Russian and other states' political systems. In February 2012, he published a manifesto entitled *Rossiya I Menyayushchiyisiya Mir (Russia and the Changing World)* wherein he wrote that:

> The notion of "soft power" is being used increasingly often. This implies a matrix of tools and methods to reach foreign policy goals without the use of arms but by exerting information and other levers of influence. Regrettably, these methods are being used all too frequently to develop and provoke extremist, separatist, and nationalistic attitudes, to manipulate the public,

> and to conduct direct interference in the domestic policy of sovereign countries. There must be a clear division between freedom of speech and normal political activity on the one hand, and illegal instruments of "soft power" on the other. The activities of "pseudo-NGOs" and other agencies that try to destabilize other countries with outside support are unacceptable.[14]

Thus, Putin's subsequent attacks on nongovernmental organizations (NGOs) hardly came as a surprise. Neither is it a surprise that Putin ordered the special services to expand their coordination to prevent extremist and terrorist propaganda (which of course goes undefined) in the global information space.[15] A plethora of laws has steadily constricted the space for domestic opposition and transmission of information while subjecting the country to a relentless nationalist mobilization. Leading think tanks like the Valdai Club endorse this view as well. In their recent paper on Russia's defense reform, members of the Club wrote that:

> Military operations are designed to not only defeat the enemy physically, but also to crush their morale, and not just of the troops but also of the people and the government. Factors such as the depth of support for the war among the general population play an increasingly important role, and accordingly, so does understanding and using culturally specific features of the enemy and his political system, including through exposure via the media. The distinction between "civilian" and "military" segments of society is disappearing. The aim of a military campaign is to impact not only the enemy army, but also its society, understood in terms of its cultural as well as its physical aspects. This trend makes it necessary to conduct joint "civilian-military operations," rather than purely military ones.[16]

Along with this conceptualization of IW, we see a corresponding discussion and effort to define what constitutes an IO. Thus, Russia's defense doctrine of 2010 stated that one of the features of contemporary military conflict is:

> The prior implementation of measures of information warfare in order to achieve political objectives without the utilization of military force and, subsequently in the interest of shaping a favorable response from the world community to the manifestation of military force.[17]

It should be emphasized here that the 2010 doctrine's guidance is that these measures be launched in advance of actual combat operations, thus indicating that IW and IO are peacetime affairs and not just wartime activities. In other words, IO and IW occur all the time, and this is as it should be. If anything, in the wake of Ukraine, this precept stands out all the more clearly. Correspondingly, a prominent Russian theorist of IW, A. A. Strel'tsov, defined an IO as:

> activities coordinated in terms of time, efforts, and objectives performed by agents to implement government information policy over a relatively long period of time that are directed at carrying out mid-term or short-term political tasks.[18]

The aspect of IW and IO that is aimed at military targets, command and control, or at degrading the performance capability of enemy weapons, or to enhance the information component of one's own weapons, or to cause physical infrastructure to malfunction, is called the information-technical aspect of IW. Whereas, the use of IW and IO targeted at media, socio-political structures, and mentalities is the information-psychological aspect.[19]

Russian leaders take both aspects of IW or information confrontation (*Informatsionoye Protivoborstvo*) quite seriously. In early-2012, Chief of the General Staff General Nikolai Makarov observed that, while land and sea have ceased to be the main theaters of war, the focus has shifted to the aerospace and information spheres, including cybersecurity. Moreover, the wise use of "asymmetric action, [during] the initial period of hostilities has begun to exercise a decisive effect on the way a war is waged and on its outcome." Both kinds of IW can be used in that period.[20] In this context, it is hardly remarkable that in 2011, President Dimitri Medvedev tasked the armed forces to develop measures "to destroy the information and control assets of an ABM system" as part of a campaign emphasizing the information-technical aspect of IW.[21]

Russian definitions of the two aspects of IW and IO are notable because they openly discuss a long campaign carried on in peacetime. These campaigns undertake what amounts to—at a minimum—an information/intelligence preparation of the battlefield (IPB) that can long precede (as was the case in Estonia, Georgia, and now Ukraine) the actual manifestation of overt conflict. Here again, the distinction between peace and war has been effaced, indicating that from Moscow's standpoint, "war is peace," in George Orwell's words, and is being waged continually, even now.

Indeed, leadership, doctrinal, and expert statements like Strel'tsov's observations define a two-part strategic role for IW and IO in the future, if not in the Estonian and Georgian operations:

> First, IO can be used to undermine the leadership and decrease the morale of the citizens of a target country.

> The operational ways of such actions would be, as was displayed in 2007 and 2008, attacks on government, media, and financial websites aimed at limiting a government's ability to control its resources and communicate with the population.[22]

Given this long-term, implicitly cumulative, and steadily reinforcing nature of IW and IO, some analysts have likened its effects to the tightening vise of a naval blockade. The destruction or degradation of enemy means of communication and weapons systems represents the information-technical aspect of Russian IW concepts, while the attacks on the enemy country's media and population represent the information-psychological component.[23]

While there are Western writers who see IW and IO in this light, for the most part, this kind of conceptualization is fundamentally alien to U.S. and Western writing on IW and IO, which focuses on the technical and not the psychological aspect.[24] American writing on IW and IO definitely underrates or omits the information-psychological aspect and concentrates almost exclusively on the information-technical aspect of "cyber war"; Russian writers explicitly and fully incorporate the latter aspect into their assessments.[25] Moreover, we have seen Russia employing both aspects of IW and IO in its strategic activities since its war with Chechnya in 1994-96. Thus, IW and IO have featured prominently in Russian operations at home and the wars with Chechnya since 1994, in the domestic consolidation of the Putin regime, against Estonia in 2007, Georgia in 2008, and against other Commonwealth of Independent States (CIS) targets at various times in the last several years. Thus, as we have suggested, the use of IW and IO in Ukraine is hardly an

anomaly, but rather is a continuation and refinement of previous thinking and activity.

This Russian way of thinking and of employing information technologies in warfare denotes an autochthonous approach that is informed by Western practice and writing but nevertheless diverges from it and represents a creative adaptation or updating of these phenomena to Soviet strategic and military-political thinking. As U.S. Colonel Richard Zoller's analysis of Russian thinking about IW concerning the general process that Russians call informatization observed:

> More than any other nation-state, Russia uses the cognitive domain of cyber as much as the technical domain. Where Western definitions of cyberspace focus on technical aspects of information technology, "informatization" takes on a much broader definition. "Informatization" can be broadly defined as applying modern information technologies into all fields of both social and economic development, including intensive exploitation and a broad use of information resources. What this means is that Russia uses cyberspace more to disrupt an adversary's information than to steal or destroy it.[26]

Thus, for Russia, IW and IO are fully legitimated weapons or instruments of internal political as well as foreign military-political contestation. IW and IO are weapons of internal and/or external political struggles within or between political entities (not only states) and can be used for public, government, civic, and private strategies. Accordingly, it goes without saying that in a society in peacetime or at war, the struggle to influence and shape "the information space" is ongoing. Moreover, recent Russian writing about IW notes that conflict over information space has been waged throughout history between states to expand their

political zones, control raw material resources, etc. Meanwhile, today IW is being constantly waged both between and within states for all kinds of purposes, not least the "possibility of manipulating moods and behaviors of large masses of people."[27] Indeed, Vladimir Karyakin argues that the advent of information and network technologies, coupled with advances in psychology regarding the study of human behavior and the control of people's motivations, "make it possible to exert a specified effect on large social groups but [also] to also reshape the consciousness of entire peoples."[28] This kind of thinking about IW establishes a direct link between current Russian writings about IW and IO and the Leninist tradition of using indoctrinated Communist Party cadres as a political surrogate for armies, e.g., "a fifth column."[29]

Therefore, we can argue that, at least in the efforts to influence a society's information space, there is no distinction between war and peace, and some would also argue among war, peace, and the use of social technology for criminal purposes. This is a new phase in a process of "neither war nor peace," and a direct continuation of the Leninist tradition of a constant state of siege within and between states, societies, and blocs. Similarly, there is no hard and fast definition (unlike U.S. thinking) between war and peace. As Russian writers and officials see it, conflict is constant, and one major target, especially in domestic political arenas or among populations at war with each other, is the mentality of the "home front." According to Karyakin:

> The mental sphere, a people's identity, and its national and cultural identity have already become battlegrounds. The first step in this direction is the discredit-

> ing of and then the destruction of a nation's traditional values. And in order for external aggression to be perceived painlessly to the mass consciousness, it must be perceived as movement along the path of progress.[30]

He then outlined a systematic campaign of IW against a nation's mental perspectives.[31] Allegedly, the United States waged such a war against post-war Germany and Japan to destroy these societies' earlier military spirit and to enforce an irreversible outcome unlike that of shooting wars. Information and network attack was duly directed against their mental space and led to a replacement of earlier national values by those of liberalism. "In this case, the mass consciousness does not recognize the fact of implantation of the enemy's mental viruses."[32] Today such warfare assumes the following form:

> The aggressor puts multiple social structures into play in the information and network war. First, and foremost, this includes the mass media and religious organizations, cultural institutions, nongovernmental foundations, and social movements, several of which are funded from abroad. In their totality they wage what is called a 'distributed attack' by inflicting numerous pinpoint destructive actions against a country's social system under the banner of 'development of democracies and civil society' and 'observance of human rights.'[33]

Karyakin also locates such tactics in the alleged Western manipulation of the Arab Spring. He observes that information and network confrontation of states encompass a struggle to establish control over territory. This control is accomplished through; global information and surveillance systems; encouraging separatist and terrorist movements; engaging enemies in low-intensity conflicts and organizing agitation of

the masses, economic warfare, including embargoes and sanctions; and ideological warfare as described here. In addition, control is accomplished through network strikes by organizing hacker attacks and introducing various computer viruses into computers, communication systems, and databases.[34] In this context, it is noteworthy that the Putin regime's attacks on Estonia and Georgia, as well as its targeting of domestic reformers, all follow Karyakin's and others' script in regards to both the targets and methods of waging IW and IO.

Therefore, the following observations apply to Russia with particular force for several reasons. First, the expansion of the theaters of military operations, from purely battlefield phenomena to the totality of states' physical and socio-political networks, can be construed as a direct evolution from the Leninist theory of political struggle. Lenin began by expanding "the state of siege" within Russian Social Democracy into a global one that reached its apogee in the Cold War and comprised struggles within states as well as between blocs on a global scale. Now information technology has vastly expanded the opportunities for almost anyone to conduct such operations in both real time and over the course of time, as well as in depth. Anyone can target anyone or anything else for as long as he or she wants and can do so more often than not with plausible deniability.

Moreover, in this context, information technology and the uses to which it can be put can replace the strategic and political role played by indigenous Communist parties that functioned very much as a surrogate for missing combat power in order to affect the political balance of power in targeted countries. Russian leaders, even before Putin's remarks shown

earlier, openly viewed information technology as a nonmilitary means by which they could achieve military, strategic, or political goals. One need not have a ramified "organizational weapon" like the Communist Party to gain leverage, if not control, over a nation's policies, if information weapons can be used adroitly for those purposes.

Thus, the use of IW at home as well as abroad becomes a conscious securitizing move to enhance the power and stability of the current Russian state and of the security services within it. Actors make "securitizing moves" not just to place an item on the agenda, but also to claim that their agency alone has the capability to define, resolve, or implement the appropriate solution for the problem. This Russian process is consciously intended to regain state control over multiple domestic processes after the much freer and uncontrolled experience of the 1990s. Consequently, IW and IO are legitimate weapons in the domestic and/or international struggle for political power. Since the Russian government believes itself under attack from a linked ensemble of foreign governments and democracy promoters who have joined with domestic reformers, IW and IO in Russia are critical instruments of what might be called a domestic counterinsurgency strategy. At the same time, in foreign contexts, they are weapons as well as strategies that are deployed cumulatively over time, not just to disable an adversary's military machine, but also to demoralize and subvert it from within and isolate it from other networks abroad that could support it.

Thus, while Russian theorists have discussed what they call the information-strike operation against enemy forces, which was evidenced in the 2008 war with Georgia, most actual uses of information weapons

in operations have aimed at the domestic "nerves of government" or of society, not combat forces or military command and control. Indeed, the "information-psychological" aspect that covers the use of the press and the media broadly conceived against a target's information space is a key category among many in the Russian definition of IO and IW.[35]

Russia has been constantly at war against either Chechnya or Islamic insurgents in the North Caucasus since 1994, with only a brief and very tenuous respite in 1996-99. Since Russia remains a society at war in the most literal sense, its recourse to IW and IO emerges out of the strategic imperatives and initial conditions of military operations in 1994-96, and then again since 1999. Even today, its regime fully understands its illegitimacy in the face of a rising tide of popular opposition. Consequently, Russia has frequently waged its own form of IW and IO against its own people at home in order to secure or sustain the existing political regime.

Russia's leaders fully believe as well that not only does Russia conduct IO or IW at home and abroad, but also that Russia is the constant target of foreign governments and intelligence services who operate together with all the domestic forces who are demanding reforms—domestic reformers, NGOs, or foreign critics of the regime—to undermine the Russian government.[36] The expulsion of the U.S. Agency for International Development in September 2012 and accompanying draconian legislation against all manner of opposition to the regime suggests an intensifying governmental fear of this dissent. It also reveals a governmental obsession, wholly consonant with Russian tradition about subversion from within, supported from abroad, and aided by the systematic use

of information technology. These fears have extended the life of the Leninist threat paradigm of internal enemies of the political order who are linked with foreign governments, a paradigm that continues to this day. In this context or according to this logic, the measures taken by the government to wage IW and conduct IO against the Russian people—and by its logic implicitly against the West—are eminently rational.

But at the same time, the growing signs of mass political disaffection in Moscow and beyond have only made the regime more adamant in its perception of this threat assessment. Thus, Russia's own experience plus its contemplation and assessment of that experience, even as it occurs, confirms to its leadership, if not also to external observers, that the highly protean concepts of IW and IO apply both at home and abroad and can also be deployed simultaneously to target both domestic and foreign audiences. For these reasons, this chapter, while not neglecting the information-technical element as seen in the 2008 war with Georgia, concentrates on the information-psychological element, which is more often deployed either at home in service to a domestic governmental counterinsurgency strategy or to the attainment of strategic foreign policy goals.

ASSESSMENTS OF IW

Russian military and political leaders have been aware of the importance of the information factor in warfare since 1991, when Operation DESERT STORM first revealed that significance to the world at large. This understanding has grown, expanded, and developed along with Moscow's capabilities for employing IO and IW at home and abroad. Indeed, Russia

has taken IW and IO so seriously that it even crafted a draft treaty for submission to the United Nations that would restrict other governments' abilities to use these weapons against Russia. This signifies Russia's anxiety about the use of these weapons against it at home in both peace and war. However, throughout the period of 1991-2012, its leaders and analysts have assiduously sought to understand and define IW and IO in ways that would let them be incorporated into doctrine and operational guidelines for the government and military.[37] Since Tim Thomas and Leigh Armistead, among others, have cogently explored this literature, there is no need to recapitulate it here.[38] Instead, we can examine what at least some Russian military-political leaders and commentators have said about the role of IW and IO in contemporary warfare, particularly as these phenomena apply to the domestic front in what Moscow calls "information confrontation." From there, we can examine how Russia has actually employed IW and IO.

Writing in 2006-07, Deputy Premier and former Defense Minister Sergei Ivanov indicated Moscow's full awareness of IW, and that it was a surrogate for a more classical military kind of operation. Indeed, Ivanov openly admitted that IW and IO allowed Moscow to find a new weapon to use in what might be called purely political, i.e., nonviolent, warfare. It also allowed them to update the Leninist inheritance of using Communist parties, fifth columns, and intelligence penetration of targeted societies as weapons in what became the Cold War to obtain political and strategic advantages. Ivanov observed that:

> The development of information technology has resulted in information itself turning into a certain kind

> of weapon. It is a weapon that allows us to carry out would-be military actions in practically any theater of war and most importantly, without using military power. That is why we have to take all the necessary steps to develop, improve, and, if necessary—and it already seems to be necessary—develop new multi-purpose automatic control systems, so that in the future we do not find ourselves left with nothing.[39]

Furthermore, leading Russian military figures like Baluyevsky and Gareyev openly discussed threats to Russia in which the country might suffer even a crushing defeat without a shot being fired.[40] Gareyev stated that:

> The breakup of the Soviet Union and Yugoslavia, the parade of "color revolutions" in Georgia, Ukraine, Kyrgyzstan, and so on show how principal threats exist objectively, assuming not so much military forms as direct or indirect forms of political, diplomatic, economic, and informational pressure, subversive activities, and interference in internal affairs. . . . The RF's security interests require not only that such threats be assessed, but also that effective measures of countering them be identified.[41]

Clearly, what happened to Russia could be turned around and made to happen to others. But these statements indicate that Russian statesmen and leading military thinkers like Gareyev clearly grasped that IW and IO were and remain a double-edged sword. Indeed, leading Russian analysts, not just Gareyev, have openly argued (even before Putin did so in 2012) that the United States is waging "a network war" against Russia. Aleksandr' Dugin, a prominent Russian geostrategic thinker, openly made this claim in 2007. In network war, according to his assessment, informa-

tion is converted into a political instrument for use by socio-political organizations and institutions in a general and flexible way. He not only saw evidence of this employment of the network concept in the "color revolutions" of Serbia, Georgia, and Ukraine after 2000, but also al-Qaeda employing its own version of network war.[42] He was not alone in his concern for Russia's internal stability under such conditions.

Dugin and other similarly inclined writers have repeatedly argued that Russia itself has been subjected to information attacks by outside forces. They also occasionally claim that Western critiques of Russian policies and form of government represent information attacks. This line of reasoning also applies to the other non-Russian authoritarian regimes in the CIS who regard U.S. and/or NGO efforts to promote democracy as forms of IW. Thus Belarusian Television 1, the government's official channel, openly stated that "a war of a new type, based on networks of organizations, is being waged on the post-Soviet space."[43] Typically, this "network war" is being directed by the State Department and U.S. intelligence services that mobilize thousands of smaller organizations; which was first tried out in Ukraine's 2004 election campaign.[44] Subsequently in late-2011, Putin, as Prime Minister, claimed that Secretary of State Hillary Clinton gave a signal to opponents of the Russian regime to demonstrate against the patently false elections that had just occurred.[45] But particularly interesting is that the description the tactics of this operation closely resemble the Estonia crisis of 2007. In other words, Moscow employed what it professed to believe were its enemies' tactics against Estonia in its own cause. According to this Belarusian report:

> Political technologies and manipulating information form the basis of "the network war." Networks consist of numerous modes, and each of them, civil organizations, movements, foundations, human rights activists, and the mass media, are playing their particular role: staging protests and pickets, conducting seminars and publishing articles and reports, in other words, displaying any instance of public activity seeking to deliberately destabilize the situation in the country. . . . [in Ukraine in 2004] the number and intensity of democratization programs have been stepped up, the target audience and the net of pro-Western forces are being expanded. Youth, women, and religious organizations, independent trade unions and regional opposition unions and the mass media are seeking to implement a civil eruption scenario with numerous sources of fire.[46]

According to this line of reasoning, all opposition political activity is essentially an act of war against the government, and more likely than not, is supported, funded, or directed from abroad in a deliberate act of war against the targeted state. Ultimately, this leads governments like Russia to equate all dissent with treason.[47] Therefore, if IW "is essentially the implanting of one's own *Weltanschauung* (world view) in a targeted population," then the Russian response must be a state-directed campaign of patriotic indoctrination and suppression of foreign and, therefore, noxious communications.[48]

Nikolai Patrushev as head of Russia's Federal Security Service (FSB) in 2007 called upon CIS states to expand cooperation between secret services, security agencies, and law enforcement agencies to fight the use of the Internet for terrorist purposes. Of course, the hidden agenda is also to stifle dissent in all these states, but nonetheless, the threat to which we and he are referring is real enough.[49] Similarly, Chief of the CIS Anti-Terrorist Center Police Colonel-General Andrei Novikov told a meeting of this organization that

the expansion of terrorist activity from the Balkans to Afghanistan places every member of the CIS within the orbit of terrorist information warfare:

> Terrorism not only exchanges information with the help of the Internet and recruits new members, but also carries out active propagandist work. This circumstance dictates the need for developing adequate and effective strategic methods of information counteraction on the part of CIS states.[50]

Novikov and Patrushev have very good reason for their anxiety about IW conducted by terrorists. Russia, according to the author's conversations with Russian analysts, has also been victimized in this regard as part of the Chechen war (indeed, this aspect of that war has received hardly any coverage). Reportedly, in late summer 2007, the Russian armed forces went offline because so many hackers and penetrations of the system were recorded from pro-Chechen sources that their network could not cope with these threats.[51] Certainly, the Russian government understands both the opportunities and threats, as President Putin had advanced a plan in 2007 calling upon Russia to become a global leader in information technology (IT); but also warned at the same time that Russia must guard against the threat of cyberterrorism, develop innovative companies, and replace foreign components by domestic products.[52] Similarly, the report by a leading Russian think tank, *Soviet Vneshnei i Oboronitel'noi Politiki-SVOP* (The Council on Foreign and Defense Policy), "The World Around Russia: 2017," warned that:

> The emerging global system, which involves economic globalization and the spread of information technology, opens up unprecedented opportunities for

> development, but at the same time makes the entire system increasingly exposed to terrorism, WMD, and IT weapons.[53]

As noted above, Russian officials grasped the power of IT from the "color revolutions" after 2000. Dmitry Frolov, an official from the FSB's Information Security Center, cited Georgia and Ukraine to Duma legislators and observed that the Internet was, "becoming a serious player on the information field capable of shaping public opinion [and it had the capability] to mobilize political forces against the authorities in their state."[54] Therefore, he concluded that the jurisdiction of Russia's *Siloviki* (power structures) to monitor electronic communications "should be substantially expanded."[55] Other CIS states have followed suit. In the wake of the Arab spring of 2011, Uzbekistan, an already draconian state in many ways, launched a further crackdown on mobile Internet media along with denials by government agencies throughout the area that revolution is possible. Indeed, Uzbekistan took control over cellular companies there, instructing companies to report on any suspicious actions by customers and on any massive distributions of text messages through their cellular lines.[56] Azerbaijan also attacked Facebook and Skype.[57] Uzbekistan and Turkmenistan have instituted news blackouts.[58] In addition, the Uzbek government has intensified its controls over Internet access by blocking "hostile" websites, and promoting instead official websites that present a roseate view of current conditions there.[59] Moreover, such attacks upon Internet use have continued right up to the start of 2013.[60] These are examples of the way in which Central Asian states emulate Russian laws and practices designed to preserve the status quo.[61]

Of no less importance is the fact that current wars have brought home to the Russian military that, "It is difficult to overestimate the importance of the information factor in local wars and armed conflicts of the early 21st century."[62] Equally importantly, the Russian power structures fully understand the capabilities of information weapons and the need for Russia to compete in their production and use. Ivanov's earlier statement strongly suggests that Russia sees its cybercapabilities as giving it asymmetric or alternative ways to counter perceived Western challenges and threats by what are clearly militarily superior adversaries.[63]

Russian military writings were, if anything, even more systematic and detailed about the inherent potential of IO and IW. A 2003 article by naval Captain of the First Rank (Reserve) R. Bikkenin observed that IW not only occurs in the struggle between opposing military forces and technologies, but also comprises "disorganization of all means of a society's life support, including the enemy military infrastructure."[64] As part of his analysis, Bikkenin included in his categorization of IO, the use of the media, leaflets, religious propaganda—specifically intended for use in the then occurring Chechen campaign—and showing the extension of IW to this domain as part of the general process of securitization.[65]

By 2008, authoritative military writers were publishing detailed analyses of netcentric warfare (NCW) and effects based operations (EBO) as they understood it.[66] There is also good reason to argue that the current defense reform, launched in the wake of the disappointing performance in the Russo-Georgian war of 2008, aims to create an army capable of conducting NCW and EBO in future wars.[67] Other writers focused on the advent of IW in all its operational and politi-

cal forms, e.g., creating the basis for public information and political support as well as protecting critical civilian and defense infrastructures, again accusing Washington of waging IW against Russia, in this case, on behalf of Georgia in 2008.[68] Since the Georgian war, these themes have been amplified in literature and political statements.

For example, according to Colonel S. G. Chekinov, electronic warfare will become an independent operation in its own right in future wars, not just a support operation. Likewise, we can expect further technological breakthroughs in next-age generation weapons that will combine physical, informational, psychological, and even biological weapons in combat over vast areas, including outer space, i.e., multidimensional warfare.[69] Remote operations will occur as much as direct force-on-force missions; the battlefield will be transformed into a combat environment concept, including virtual targets and the enemy's entire range of psychological orientations and capabilities.[70] In this environment, the computer will become a strategic weapon in and of itself. Furthermore:

> It may be assumed that the informational and engineering components of the so-called information weapons will be able to paralyze the enemy's poorly defended computerized troops and weapons control systems and deprive the enemy of an opportunity to transmit information.[71]

Thus:

> In terms of content, therefore, the main specific aspect of armed struggle in wars and armed conflicts of the 21st century is that the new forms of military operations can be multidimensional and fought in all areas

> of armed struggle (land, sea, and air/space), where electronic, economic, psychological, informational warfare, and armed force will be used with growing intensity over time and terrain to achieve decisive results in the shortest time period and to deprive the enemy of initiative and freedom of maneuver.[72]

Chekinov and Lieutenant General S. A. Bogdanov (Ret.) subsequently have argued that information weapons already can actually tackle strategic tasks, such as disorganizing enemy military control, state control, and the aerospace defense system (which Russian writers expect will be the first target in a conventional offensive), deceiving the enemy, creating the desired public opinion, organizing protests against the enemy government, and launching other operations while aiming at reducing the enemy's will to resist.[73] Indeed, they argued that today the focus of both interstate and intrastate confrontation is turning toward nonmilitary means, including informational means, not least because of the danger of mutual annihilation in a nuclear conflict.[74] But this also means that new technologies can generate what they call climactic weapons, and that new methodologies can induce dozens of different pathways for psychologically manipulating and controlling an enemy to follow a prescribed course of ultimately self-destructive actions—this sounds very much like the old Soviet concept of reflexive control. The supposed next generation of weapons that could combine psychological, informational, and even biological attributes, will be based, in the famous words of Marshal Ogarkov, upon "new physical principles" and exemplifies this trend. Along with a plethora of Russian officials, that from Putin down, they charge the United States with developing and deploying these methodologies in the

color revolutions in Georgia, Ukraine, Central Asia, and elsewhere.[75]

In this context, the authors charge that after 1945, the United States developed what they call "the organizational weapons" (the irony here is that the Communist Party type of organization developed by Joseph Lenin was originally and rightly called the organizational weapon), whose purpose is "to eliminate a certain society, organization, company, or family" (the mission does not have to be on a global scale.).[76] Like Gareyev, they argue, therefore, that states that cannot defend their information security put their economic and political independence at risk. American and allied military conduct in the last few decades produced an object lesson in showing how active information operations can impact the mass consciousness of societies and governments, and ultimately their military control allowed the United States and its allies to secure their military-strategic goals.[77] Finally, the United States may go beyond IW to new climactic weapons. They cite the U.S. High Frequency Active Auroral Research Program (HAARP) in particular, as possessing the capability to manipulate the weather and cause natural disasters, earthquakes, tsunamis, floods, tornadoes, droughts, etc. They quote Russian "defense expert" Yuri Boylov who claimed that everything that occurred in the Indian Ocean tsunami of December 2004 was the direct result of U.S. local tests of radio-physical and geographical super-weapons under the HAARP program.[78]

We may dismiss this kind of analysis as being both unoriginal and literally fantastic, if not paranoid. However, despite Moscow's systematic self-disinformation and paranoia, the vistas presented here merit our close attention because they are so utterly

pervasive throughout the military-political leadership. Chekinov and Bogdanov seem to have open access to the General Staff's military journal *Voyennaya Mysl* (the English version is *Military Thought*) as these and other articles suggest.[79] The views presented here show a strong consistency with leadership statements in asserting that the Russian state is at risk at home and abroad from U.S. and allied IW and IO, specifically aiming to undermine the Russian government and manipulate the domestic political playing field. Russian interests are also constantly at risk from these forces, suggesting a continuation of the Leninist state of siege mentality as well as the Leninist threat paradigm into the post-Cold War world. Warfare, i.e., IW, goes on even in peacetime, and the Russian state is the target of a growing campaign. These views are fully in sync with the overblown, even hysterical, threat perceptions embodied in Russia's 2009 *National Security Strategy* and 2010 defense doctrine, which insisted that the threat of force being used against Russia was growing. These views also embody the outlook of a militarized police state (and criminal enterprise) that has little confidence in its own legitimacy and security and insists on viewing the world through this combative, even paranoid lens.[80] Moscow's IO and acts of IW at home and abroad comport with these estimates of the centrality of information weapons and threats and highlight the strategic significance of IW and IO for both domestic and external strategic operations.

In other words, we already are long since in the midst of what Russian leaders and thinkers would call an IW being waged in Russia proper; and Russian leaders fully believe they are under attack from within as well as from the outside the country. As we have seen, they fully endorse the idea of IW as a

weapon of war not only against weapons systems and C2 neworks, but also against entire social structures and mass cognitive processes, and they believe they are being so attacked and must respond in kind. This aspect of IW and IO has received much less attention in the West, thereby signifying our own myopic ethnocentrism and inattention to strategic issues and other peoples' thinking about contemporary warfare. We may believe that we are at peace with Russia, but Russian leaders do not share this view. As long as this inherited Leninist threat paradigm prevails, updated with the new methods of information technology, from Moscow's standpoint insofar as the United States and the West are concerned, if Russia is not actually at war with them, then at best it is in a state of neither war nor peace, or at best, peaceful coexistence. As long as this mentality, which now governs Russia, prevails, we need to understand what it means for our own benefit and to grasp the full significance of the ongoing domestic struggle inside Russia for the future of international security.

ESTONIA

Bearing the foregoing analysis in mind, the 2007 Russian cyberattack on Estonia stands in a clearer light than before. Although this attack cannot be definitively traced to Moscow, the available evidence that it was a predesigned Russian attack is overwhelming. Indeed, Duma Deputy and a frequent spokesperson for the Russian Administration Sergei Markov boasted in 2009 that his assistant and office were behind the attacks, and that more of such events would happen.[81] Whether or not Markov's boasting is truthful, there is much more evidence that Russia planned this attack, and it clearly conforms to the elements of Russian

thinking about IW and IO described earlier. Worse yet, now that Putin has admitted that the war in 2008 with Georgia was planned by Moscow from 2006, it is possible that Estonia served in some ways as a dress rehearsal for that war and as a probe of its defenses and the North Atlantic Treaty Organization's (NATO) response.[82]

For example, the attacks on Estonian socio-economic and political institutions were allegedly the reaction to Estonian authorities' transferal of the site of a monument—the Bronze Soldier—to Soviet liberators of Estonia from the Nazis in Tallinn to another site. However, in fact, Estonia's authorities' investigation of the April-May 2007 incidents revealed that Russian planning for the demonstrations in Tallinn began a year earlier, i.e., well before any sign that the monument would be removed.[83] Further evidence confirms this assertion:

> They were planned in advance and at least somewhat coordinated, as Russian-language forums were full of the preparations and planning in the days leading up to the attacks. The Estonian government even planned to release news of the strike three days before it began, but was dissuaded by the European Union (EU) because of an upcoming meeting between then-EU president and German chancellor Angela Merkel and Russian president Vladimir Putin.[84]

Further, evidence all but states that the Russian strike was an act of high policy. The attacks included denial of service, botnets, hacking, etc.[85] This "war" lasted from April 26, 2007, until mid-May 2007, a period of several weeks. Although some have argued that the sources of these attacks cannot be conclusively traced to Russia, the Estonian government has

insisted from the start that Moscow was behind it. Indeed, it originally claimed to trace the source of some of these attacks to Russian governmental addresses.[86] It is impossible to charge Russia conclusively with orchestrating the attack because of the use of botnets, short for robot networks. According to James Hughes, botnets are the newest fad in cybercrime. In a botnet attack, a cybercriminal or attacker takes control of a foreign computer by surreptitiously loading software on it without the consumer's awareness that the computer has been compromised.[87] Criminals typically use bots to infect large numbers of computers. These computers form a network or a botnet that is then used to send out spam email messages, spread viruses, attack computers and servers, and commit other kinds of crime and fraud. If your computer becomes part of a botnet, your computer might slow down and you might inadvertently be helping criminals.[88]

Moreover, some botnets are huge, embracing tens of thousands of computers across the world so that attacks can seem, as in this case, to be coming from everywhere. As Hughes points out, this does not prove Moscow's innocence, since its agents could have used chat rooms and email to incite patriotic Russian hackers, of which there are plenty, as well as cybercriminals to attack Estonian targets.[89] Nevertheless, the nature of the attacks described next and the fact that Moscow continued to maintain sanctions on Estonia afterwards to demand revision of Estonian laws concerning its Russian minorities, and to call it a Fascist or pro-Fascist regime, suggest its hand was behind this attack.[90] Also of interest is the fact that, in a 2006 article, Russian scientists forecast the exact nature of the use of botnets to achieve denial of service in targeted computers.[91] In addition, of course, Estonian officials staunchly believe it as well.

Besides these computer and cyberattacks, Moscow organized violent demonstrations in Tallinn among the Russian diaspora there, and among its homegrown youth organization, *Nashi* (Ours) in Moscow, against the Estonian embassy. *Nashi*, the main Russian youth organization, is, like the other such youth groups in Russia, a creation of the Putin regime. These groups all espouse a strongly nationalistic pro-Russian and pro-Putin attitude, almost to the point of xenophobia. Their attitudes, behavior, and governmental support make them a kind of legatee of the tactics of the Komsomol; Mao's youth gangs during the Cultural Revolution of 1966-69; the Hitler Jugend; and Fascist Squadristi. Moscow has also employed *Nashi* and other groups against other foreign embassies and domestic dissidents.[92] Moscow also has intermittently imposed various ongoing forms of economic warfare, such as interference with trade and transport, energy cutoffs, etc., upon Estonia (and on other Baltic states which have defied its requests) since the 1990s.

Thus, this information war, the first in European history, has been combined with attempts to incite domestic violence in Estonia, attack its embassy in Moscow through violent demonstrations there orchestrated by *Nashi*, an ongoing public diplomacy campaign targeting both domestic Russian and Western audiences to label Estonia's regime as Fascistic, and ongoing economic warfare.[93] Accordingly, it seems clear that the computer attacks or the IO and other steps taken by Moscow against Estonia were acts of high policy that reflected a coordinated strategy devised in advance of the removal of the Bronze Soldier from its original pedestal.[94] More to the point, the elements that went to make up this strategy represent aspects of a new but already long-standing Russian strategy of

asymmetric war, which need not be confined only to the Baltic, Eastern Europe, or Russian use:

- Cyberwar;
- Economic sanctions;
- Domestic and international public information campaigns against Estonia;
- Manipulation of youth organizations;
- Manipulation of gangs;
- Russian efforts to penetrate key sectors of the Estonian economy;
- Russian efforts to subvert politicians through intelligence penetration and the use of connections with the energy industry;
- Russian links with organized crime and Baltic elites in general.[95]

This strategy often involves the collaboration of Russia's energy firms (which are largely state-owned), intelligence agencies, organized crime, and embassies. These entities work together in an effort to spend money buying up key businesses in targeted states, donate money to political movements and politicians thereby compromising them, and in general exercise a covert influence on local politics there. Manifestations of this strategy pervade Russian policy from the Baltic to the Black Sea.[96] For example, in 2004, Roman Giertych, Deputy Chairman of the commission that investigated the notorious Orlen scandal in Poland, concluded in his report:

> The commission has evidence that a certain kind of conspiracy functioned "within the background of the State Treasury Ministry, the Prime Ministerial Chancellery, the Presidential Chancellery, and big business," which was supposed to bring about the sale of the Polish energy sector into the hands of Russian firms.[97]

Subsequently, Lithuanian businessman Rimandas Stonys, President of Dujotekana, Lithuania's Gazprom intermediary who had close ties to Russian and Lithuanian officials and extensive investments in Lithuania's energy and transit sectors, was investigated by Lithuania's Parliament. These investigative reports charged that he used his ties to Russian intelligence and other Lithuanian political connections to advance personal and Russian interests in Lithuania's energy sector. Dujotekana reputedly was a front for Russian intelligence services, which were already entwined with Gazprom. A counterintelligence probe into a foreign citizen's efforts to recruit senior Lithuanian Intelligence (VSD) officers led to the firm, which also recruited government officials. Key executives of Dujotekana are apparently also KGB alumni. Similar charges are raised in regard to Stonys' and his firm's influence in Lithuania's transit sector, his large contributions to politicians and media, and his influence over political appointments.[98] In previous years, attempts were made to compromise Lithuanian politics by using such figures as Viktor Uspaskich, founder of the Labor party who tried to make a comeback, and the disgraced ex-President Rolandas Paskas.[99] Likewise, in Estonia, the 2006 annual report of the Security Police noted that the Constitution Party is financed partly from Moscow.[100]

Therefore, the strategy involved here goes beyond Russia's tense relations with its neighbors, whether they are Baltic or other neighbors, to encompass global potentials for waging such war against hostile governments or as part of an insurgency within a state or as a takeover from within. Cyberattacks may play a role as needed in implementing such a strategy, or they may be a self-standing operation in its own right that can be repeated endlessly and turned on or off.

Indeed, the cyberattacks occurred within this context of Russia's unyielding pressure to exploit energy dependencies in all three Baltic states and used the combination of energy monies, bought and subverted politicians, intelligence penetration—often through firms influenced or owned by Russian or pro-Russian personages with shadowy connections to Moscow—and organized criminal syndicates as a constant means of pressure upon the Baltic and East European states.[101] Such criminal and political penetration or subversion are long-standing tactics that have also been reported in Poland, if not throughout all of Eastern Europe. In addition, these often involve attempts by linked Russian intelligence, energy, and criminal elements operating in tandem to takeover key energy firms and gain key positions in political parties or economic influence over political organizations in these countries.[102]

For these reasons and due to the evidence discussed later, it is safe to argue that these cyberattacks appear to have been strategic in their choice of targets and political objectives, part of a larger long-term strategy, and therefore long-planned. They aimed at accomplishing certain goals, disrupting and possibly unhinging the Estonian government and society, and demonstrating NATO's incapacity for protecting Estonia against this novel form of attack. Undoubtedly as well, this operation aimed to compel Estonia to take Russian interests into account in its policies. In other words, it had a classically Clausewitzian character of compelling the enemy, i.e., Estonia, to do Russia's will even though it was a bloodless and nonviolent attack. In this case, as perhaps in Georgia's case, this attack may have reflected not so much, or not only, an effort to correct Estonia's behavior or influence its orientation, but also a desire to punish it and deter others

from following suit by holding it up as an example of the risks to anyone who crosses Russia.[103]

Certainly, people outraged at the removal of the Bronze Soldier did not generate the demonstrations spontaneously, and chances are that the same principle applies to the cyberattacks. First, Estonian authorities have reported that their investigations and courts found that planning for the demonstrations in Tallinn were begun a year in advance of their actual occurrence. Second, they recorded the presence of Russian Special Forces (it is not clear which of the many different kinds of the Russian Special Forces they meant) at the demonstrations in civilian clothes.[104] This tactic also turned up in the Russian-organized demonstrations in the Crimea against NATO in 2005.[105] In this respect, the demonstrations in Tallinn resembled earlier tactics and efforts by Soviet and Russian Federation authorities to destabilize or even unseat governments deemed insufficiently friendly or obedient, e.g., the Czechoslovak government in Prague in 1948 and in Bulgaria as well.[106] These examples were cited by those authorities. Though essentially bloodless, these attacks nonetheless represent war as defined by Clausewitz, i.e., a clash of wills where one side attempts to compel the other side to do its will, although it is not fully clear what Moscow concretely wants other than to assert its hegemonic status in the Baltic.

The Estonian investigators also believe that the plan devised in Moscow for these violent demonstrations among and by Estonia's Russian diaspora was aimed at inciting so large a series of demonstrations that they would provoke violence. They similarly contend that the ensuing violence could then have been used as a pretext for an intervention by Moscow or for the launching of a kind of insurgency directed against Estonia, which could have justified either direct Rus-

sian support for the insurgents or some form of direct or even military intervention from Russia. Though Western audiences might consider such threat assessments and scenarios to be far-fetched, the Estonians do not. Indeed, they emphasize that this operation represented something quite close to state-sponsored terrorism.[107]

While labeling these attacks as state-sponsored terrorism may be stretching the definition of terrorism, there is little doubt that one purpose of these attacks was to "derange" the Estonian social order and create a sense of mass panic within that society. Though this may not be terrorism, there is a similarity as to some of the intended goals of terrorist attacks. As Estonian Defense Minister Jaak Aaviksoo said:

> It is true to say that the aim of these attackers was to destabilize Estonian society, creating anxiety among people that nothing is functioning, the services are not operable, this was clearly psychological terror in a way.[108]

He also observed that the attacks in April-May 2007 represented a botnet strike that for the first time simultaneously targeted an entire country on every digital front. The attacks, he observed, targeted Estonia's essential electronic infrastructure, banks, telecommunications, media outlet, and name servers, thereby threatening the entire nation's security.[109] Thus, they came close to describing this operation as an act of terrorism, underlining, even if only implicitly, the well-established link between terrorism and IW, and linking it to state-sponsored terrorism as enacted by Russia. In these crucial respects, the attacks certainly conformed to Russian thinking about IW and IO depicted earlier.

Estonian officials also maintained that these provocations and the cyberwar were directed against Estonia's society and government, and targeted those institutions like banks and the media whose destabilization would induce mass social panic in Estonia and undermine confidence in both the stability of the government and of the country's leading institutions. Last, they are also quite convinced that these attacks represented probes to find out to what degree European security institutions like the EU, NATO, and the Council of Europe would stand by Estonia. In this regard, they say, Russia was surprised to find the strong, if somewhat belated, response by the EU and Council of Europe and was also disappointed by the lack of support for this program of action by Estonia's Russians.[110] However, NATO's response was late in coming, something that might signify a real weakness in NATO.

The combination of IW or IOs, criminal penetration, incitement through diasporas or other similar organizations, and intelligence subversion of politicians and political institutions, represents a potentially lethal form of warfare aiming to destabilize a state and could serve as a paradigm or as elements of a paradigm for asymmetric war.[111] Thus, we should realize that this kind of situation has not been confined to Estonia, although other instances of such operations may differ in some important particulars from the Estonian situation. For example, another noteworthy aspect of the Estonian incidents is the subsequent scandal in Latvia. During the fall of 2007, a major scandal broke out in Latvia after attempts were made to blow up the Director of the Customs Service criminal department, and a secret service officer was found in the Daugava River. During the subsequent investigations, it was discovered that Russian-funded political organizations were

buying Latvian politicians, and Prime Minister Aigars Kalvitis then observed that there exists a criminal gang consisting of former employees of the KGB and employees of the Latvian security services of Parliament and the presidential office. When President Valdis Zatlers refused to accept the anti-corruption minister's report concerning this network of corruption, the minister resigned. This resignation then triggered a large defection from the cabinet where Kalvitis and ultimately the entire government also resigned, underscoring the threat to these new states from the threat of Russian-inspired corruption.[112] These almost concurrent events or crises underscore the consistency of the Russian strategy for "political warfare" in the Baltic and Eastern Europe, as noted earlier.

But beyond these facts, the melding of tried and true Leninist tactics of subversion and intimidation with the new forms of IW or of large-scale influence-buying reflects as well, the continuing development of the Soviet and Leninist belief that Russia (previously the Union of Soviet Socialist Republics [USSR]) is permanently under threat and that its national security policy begins from the standpoint of what the German philosopher Carl Schmitt called the presupposition of enemies.[113] In other words, the tactics and strategies developed and employed by the Soviet Union have served as a foundation for the development of new strategies that incorporate at least some of this Leninist repertoire and new trends like IW for the conduct of continuous political warfare against hostile targets. The continuity in tactics employed in Estonia with those utilized in earlier Communist takeovers underscores this point. For example, in attempting to demonstrate to Estonia that its allies would not or could not defend it, Moscow, as in 1968 when it sought successfully to isolate the Dubcek regime in Czecho-

slovakia, operated on the belief expressed by Ivo Ducachek that:

> For a successful revolution, the Communists must have, among other things, a clearly favorable balance of potential outside aid. The democratic majority must feel isolated *internationally*; while the Communist minority is sure of direct or indirect support from Soviet Russia or other Communist states.[114] (Italics in original).

Furthermore, the use of aggrieved ethnic or class minorities, especially when backed by a neighboring great power, as a pretext for subverting an established order is a hallmark of Leninist tactics that have since been globalized. Indeed, the use of tactics of terrorism or that resemble terrorism in order to undermine a state's adhesion to NATO was also a Soviet tactic. Thus Spanish officials reported in 1980 that Soviet Foreign Minister Andrei Gromyko told them that Moscow would help with their terrorist problem if they refrained from joining NATO. On the other hand, he implied that entry into NATO would leave Spain more vulnerable to terrorism.[115] Similarly, we can understand the Soviet attempt to organize large-scale political organizations in targeted countries along with smaller-scale guerrilla movements, intelligence networks, and to use either or both for purposes of political subversion in those states as a conscious strategy. Devised at a time of military weakness, such methods were used to expand the repertoire of instruments available to Moscow for waging political warfare against its enemies to destabilize them and their societies through what were then novel means, among them colonial insurgencies. Such tactics in their day, like IW today, were surrogates for large-scale military capabilities that were unavailable or simply not usable.[116]

Not only was this the first case of IW between states, it also is clearly a major weapon in Russia's unremitting efforts to subordinate the former Soviet Republics to its exclusive sphere of influence, and to undermine the processes of European integration and democratization. Thus, there are indicators of IOs being directed against political figures and forces inimical to Russian interests in CIS countries. In Ukraine's 2006 elections:

> the Ukrainian Central Election Commission's servers and network were repeatedly attacked, totaling nearly 29,000 attacks. Most failed, so the servers continued to operate. Defense [officials] attribute responsibility to Russian actors or even the Russian government.[117]

In early-2009 in Kyrgyzstan, Moscow launched an IO to shut down its Internet networks to pressure the government to remove the U.S. military base at Manas. These were the same kind of attacks as in Estonia and Georgia, namely denial of service attacks to disrupt communications links within Kyrgyzstan and to Manas, and they were also apparently orchestrated by a mobilization of hackers as occurred against Georgia in 2008 and Estonia in 2007.[118]

Second, such attacks involving hackers, Russian Internet forums, and officials continue, again in keeping with Russian ideas that IW and IO are constant long-term operations:

> On June 25, 2008, the Estonian television channel ETV24 reported the prevalence of appeals for cyber attacks by Russian hackers against Estonia, Latvia, Lithuania, and Ukraine on Russian Internet forums. The following weekend, a cyber attack against Lithuania began, and government, commercial, and private Web sites were defaced with vicious slogans and Communist symbols (earlier that summer, Lithuania passed

> a law against the display of Communist symbols, angering Russia). The attack was short, and the Web sites were fixed by early July. However, Lithuania was hit again on July 20, when the state tax Web site was taken down for the weekend with DDOS attacks. Both attacks can be traced back to Russia. That same day, the Georgian president's Web site was taken down for more than twenty-four hours by DDOS attacks that were traced back to Russia and operatives connected to RBN (the Russian Business Network, a notorious cybercrime operation).[119]

Third, in Estonia and in subsequent manifestations of IW and IO, we see the Russian government fully cooperating with organized crime structures like the RBN to launch these attacks. Thus, beginning with Estonia, these attacks represent a clear fusion of government with organized crime for the purposes of subversion and destabilization of neighboring governments and have since become an integral component of Russian foreign policy operations in Eurasia. RBN has been described in the following ways:

> RBN is a cyber crime organization that ran an Internet service provider (ISP) until 2007 and continues to be heavily involved in cyber crime such as phishing, malware distribution, malicious code, botnet command and control, DDOS attacks, and child pornography. Though the most recent structure of RBN began in 2005, there are rumors that date RBN (as an unofficial group of cyber criminals) back to 1996. In 2002, the group became more structured and more active. It was accused of attacking the United States Department of Defense and the Russian Department of the Treasury in 2003, though none of this can be proven officially. While it is not certain that RBN is directly connected to the Russian mafia, it is highly likely. RBN is heavily involved in child pornography, which is traditionally controlled by the Russian mafia, and its official leader,

who goes by the alias "Flyman," is suspected of running those operations (and of possibly being a pedophile himself). It is also known that Flyman has family connections to the government: his father or uncle was involved in politics in St. Petersburg before taking an important position at a ministry in Moscow. Another RBN member, Aleksandr Boykov, is a former lieutenant colonel in the *Federalnaya Sluzhba Bezopasnosti* (FSB, the successor agency to the KGB). While it is currently not possible to prove that RBN has worked in tandem with the FSB or other security services (collectively, the *Siloviki*), it is likely that they are at least connected. When RBN officially hosted Internet services between early 2006 and November 2007, it was linked to 60 percent of all cyber crime. Due to increased pressure (including blocking and blacklisting of RBN IP addresses and domains) from the cyber security industry and increased attention in published reports and news articles, RBN attempted to restructure itself in October 2007, concealing its affiliations with a variety of IPs. When this failed, it deleted a number of its domains and shut down, moving to Chinese and Taiwanese networks on November 6, 2007. This failed to divert attention, however, and two days later, it ceased routing traffic and its networks. However, it would be incorrect to say that RBN no longer exists or even that it has disbanded. While it no longer runs an ISP, the group appears to be active still and harder to track on a much more dispersed level across a variety of mostly legit ISPs. In general, Russian cyber crime certainly has not decreased with the end of RBN's ISP. Instead, it continues to grow, spread across a variety of ISPs and domains, and in February 2008, Russia surpassed China as the largest generator of malware, with 27.9 percent compared to China's 26.5 percent (the United States is a distant third at 9.98 percent). Cyber security experts continue to use the term "RBN" to refer to the loosely organized group of cyber criminals based in Russia, and cyber activity and crime by this group continue to remain high. [120]

RBN is also used for other covert operations involving information technology, and not only in Russia. For example:

> RBN has a history of involvement in major cyber operations not only against hostile/unfriendly foreign targets such as Estonia and Georgia, but also in support of friendlier foreign entities such as Iran. Recent RBN deployment into Iran to assist that regime in monitoring dissidents implies at least tacit consent from Russian leadership given the importance of Russian-Iranian relations. While it may indeed be a coincidence that RBN operations have on several occasions coincided with official Russian Federation views and/or actions, it is also likely that the Russian leadership is well aware of the capabilities RBN offers and utilizes them to assist in achieving international Russian strategic objectives.[121]

GEORGIA

In Georgia, we see for the first time an attempt to combine both elements of IW and IO, namely attacks against forces' C2 and weapons systems on the one hand, and the information-psychological attacks against media, communications, and perceptions on the other. Moreover, this was the first time Russia did this in coordination with a plan of attack that, as we now know, dated back at least to 2006. Although the results were mixed, there is no doubt that Moscow has deeply studied this campaign and is constantly seeking to refine the tactics used in both aspects of its IW campaign against Georgia for future use. Thus, Richard Weitz observes that:

> The techniques used by the Russian attackers suggest they had developed a detailed campaign plan against the Georgian sites well before the conflict. The attack-

> ers did not conduct any preliminary surveying or mapping of sites (which might have prematurely alerted Georgian forces), but instead immediately employed specially designed software to attack them. The graphic art used to deface one Georgia web site was created in March 2006 but saved for use until the August 2008 campaign. The attackers also rapidly registered new domain names and established new Internet sites, further indicating they had already analyzed the target, written attack scripts, and perhaps even rehearsed the information warfare campaign in advance.[122]

Weitz also concluded that Russian proficiency at IW had not only improved substantially from the Estonian operation of 2007 to the Georgia war of 2008, but also that Russia had employed, in both cases, botnets directing computers from locations all around the world to attack both Estonia and Georgian sites.[123] Other studies underscore the sophistication of these IOs directed against Georgia. Civilians actually carried out most attacks with little or no direct (or certainly traceable) involvement by the Russian government or military. But these organizers of cyberattacks also probably had advance notice of Russian military intentions and were tipped off about the timing of Russian military operations while they were taking place. As Weitz noted, they did not involve reconnaissance or mapping of sites but jumped directly to attack them, signifying a prior deep intelligence penetration by the Russians of the Georgian networks. In addition, these cyberattackers were being recruited through the Internet and social technology, and as in Estonia, aided by Russian organized crime even to the point of hosting software ready for use in other cybercrime activities. The number of attackers against Georgia was much greater than those attacking Estonia, even though fewer computers were involved.[124] Similarly, Jeff Carr, an investigator for Project Grey

Goose, an organization of 100 U.S. volunteer security experts from the private and government sector, concluded that "the level of advance preparation and reconnaissance strongly suggests that Russian hackers were primed for the assault by officials within the Russian government."[125]

The first wave of cyberattacks on August 6-7, 2008, 24 to 48 hours before the actual war, were carried out by botnets and C2 systems that were prepared before the invasion and associated with Russian organized crime. After this, the second wave resorted mainly, though not exclusively, to postings on websites, again a carryover from Estonia. These postings contained both the cyberattack tools and lists of suggested targets for attack. Cyberattacks were limited to denial of service and website defacements, relatively unsophisticated types of attacks, but carried out in a very sophisticated manner.[126] Once Russian troops had established positions in Georgia, the attack list expanded to include many more government websites, financial institutions, business groups, educational institutions, news media websites, as well as a Georgian hacking forum to preclude any effective or organized response to the Russian presence and induce uncertainty as to what Moscow's forces might do. These attacks significantly degraded the Georgian government's ability to deal with the invasion by disrupting communications between it and Georgian society, stopping many financial transactions and causing widespread confusion. It is possible that spyware or malware was inserted into the Georgian systems for future use, criminal or military-strategic.[127] The clear objective of the cyberstrikes was to support and further the goals of the military operations, and they were timed to begin on a large scale within hours of the first Russian military operations and ended just after those operations ended.

Indeed, subsequent reporting found that online attackers began attacking Georgian websites and discussing upcoming military operations weeks before the actual onset of hostilities, even to the point of conducting what appeared to be another "dress rehearsal" of the upcoming cyberattacks, providing further evidence of the unprecedented synchronization of cyber with all other military combat actions.[128] Likewise, the comparative restraint in not attacking key infrastructural targets, but demonstrating the ability to do so and strike at key energy installations and structures whose importance went far beyond Georgia must be disconcerting.[129]

The Georgian IW campaign points to the returns that Moscow harvested on its substantial investment in the resources needed to conduct IOs and an IW after 2000. As Jane's observed:

> Russia has in recent years stepped up its information warfare preparations, especially since 2003 when the Federal Agency of Government Communications and Information (Federal'noe Agentstvo Pravitelstvennoi Svyazi I Informatsii: FAPSI) was largely incorporated into the Federal Security Service (Federal'naya Sluzhba Bezopastnosti: FSB). As the FSB's special communications and information service, this has moved increasingly into 'active measures,' ranging from coordinated Internet propaganda and disinformation campaigns to the use of cyber attacks to silence, dismay, and disorganize unfriendly states.[130]

Another assessment of the Russian cyberwar in Georgia argued that its objectives were to silence and isolate Georgia from the international community and to impose a psychological disorientation upon the population leading to a substantial demoralization in the wake of Georgia's defeat. Beyond this, the

cybercampaign was part of a larger information battle between Russian media and the Georgian and Western media for control of the narrative. Here, Russian bloggers were able to flood a CNN Gallup poll stating that Russia's cause was justified and to attempt to prevent Georgian media from telling Tbilisi's story.[131] In the early stages, Russian hacktivists shut down the websites of Georgia's President, Ministry of Defense, Ministry of Foreign Affairs, Parliament, National Bank, and the English language online news dailies, *The Messenger*, *www.civil.ge*, and the online Rustavi-2 television channel, while also defacing the Ministry of Foreign Affairs and National Bank's websites.[132]

CONCLUSIONS

Many conclusions flow from the Russian attacks and subsequent "post-mortems" of them. First, we have observed how IOs can facilitate or even become a means of an IPB. It is clear that Moscow was able to orchestrate its hacktivists to rehearse operations and blind or deafen Georgia and its allies to what was happening. Estonia, too, surprised outside observers, although possibly not so much as in Georgia. In Estonia, the government was able to get some advance notice, though the international community was surprised.[133] Such IOs that are preparatory to overt or covert military hostilities are therefore likely to become precedents for future attacks by Russia or other countries upon strategic adversaries.[134] In addition to these factors, we see the government's deliberate employment of Russian crime syndicates as part of the war effort in both the Estonian and Georgian cases. Not only does this raise the possibility that Russian cybercrime is not just a manifestation of criminal behavior, but also and simultaneously a fully employed instru-

ment of the Russian state's grand strategy. It already is well-known that the Russian state is a criminalized or Mafia state. This aspect provides a telling example of the larger phenomenon, whereby a state utilizes its own organized crime figures that it clearly can control for the accomplishment of vital strategic aims through a program of covert actions and cyberwar.

Equally disquieting is the second lesson that Moscow learned in Georgia:

> From the cyber campaign against Estonia in April and May of 2007, Russians had already learned that a cyber campaign mounted by civilians could cause serious economic and psychological disruptions in a country without provoking any serious international response. This lesson was reinforced by their experiences with the cyber campaigns against Lithuania at the end of June 2008 and against Kazakhstan in January 2009, where major local disruptions produced remarkably little international press coverage. The campaign against Georgia took place under different conditions, because Russia was engaged in overt military action against the country, but the cyber component was still carried out by civilians, and there were no international reprisals. Given this history, it would be very surprising if most future disputes and conflicts involving Russia and its former possessions or satellites weren't accompanied by cyber campaigns.[135]

Third, Moscow repeatedly has shown that it can mobilize and synchronize civilian hackers and organized crime to coordinate with its government and armed forces in either pure cyberoperations, as in Estonia, or in major combat operations targeting not just military forces but also other potential centers of gravity including media, government, and socio-economic institutions. Moreover, it has done so, not only twice but repeatedly in Kyrgyzstan, Lithuania, and Ukraine with impunity.[136]

Fourth, the Russian experiences in Estonia and in Georgia, as well as other probes against Eurasian governments from Ukraine to Kyrgyzstan, indicate that Moscow is thinking about what U.S. analysts have called strategic information war. This is a war whose intention is to achieve victory by paralyzing a target country's social infrastructure networks, i.e., what might be called its central nervous system. Although U.S. analysts have occasionally warned that, the further we go into the era of information weapons, the more likely it is that such a war might be waged against us or against other states; in fact U.S. writings minimize and downplay such approaches.[137]

As Chris Demchak has recently written, we focus on what many think is the unlikely event of interstate war and neglect society-wide effects of non-wartime cyberstrikes directed against critical socio-technical-economic systems. We leave many critical sectors of the private sector relatively unguarded, excessively downplay the role played by the cybercrime community, and view national security problems in cyberspace as primarily technological ones while ignoring how human cognitive functions "can cause surprise to leap to technical system failure or erratic behaviors and back again."[138] Thus, we have failed to take into sufficient account the possibility of a strategic information offensive or war used against our interests, allies, and our own society.

Fifth, the target nation's patriotic hackers will, along with vital socio-political institutional structures, probably become early and primary targets of future IOs and IW attacks to deprive states of their ability to retaliate, especially as cyberstrikes are notoriously difficult to attribute to anyone. Furthermore, those attacks are ever more likely to be preemptive strikes or, as we have seen in Russia, long-running, long-

standing attacks mounted either overtly or covertly in peacetime, further effacing any distinction between war and peace. Russia is unlikely to be the only offender in this regard.[139] Finally, the means of communication and information in a society are likely to become an increasingly critical center of gravity and therefore a target for these ever more likely preemptive strikes.[140]

Sixth, Russia has updated and modified, but preserved, the Leninist inheritance of a world torn by conflict, and of a Russia that is besieged by linked internal and external enemies who are constantly waging a war, in this case an information war, against the Russian government. Moreover, they have attempted to identify social strata in targeted countries that can be swayed by information campaigns. In distinction to most U.S. writing which sees IW and IOs largely in terms of incapacitating enemy C2 and physical infrastructures, Russian thinking goes beyond this to embrace the notion of IW and IOs as a weapon that is being used and that it should use in an effort to sway mass as well as elite psychology. Moreover, Russian writers long have accepted the idea that the advent of information weapons could and probably would lead to a new generation of weapons that could directly affect mass psychology. Thus, several years ago, Russian writers on the topic of IW argued that they discerned seven types of information weapons. These means include:

- Precision location of equipment that emits rays in the electromagnetic spectrum and for developing that equipment by conventional fire;
- Affecting the components of electronic equipment;
- Affecting the programming resource of control modules;

- Affecting the information transfer process;
- Propaganda, disinformation, and psychotropic weapons, i.e., weapons that literally affect and even afflict the psyche of enemy personnel.[141]

The operational and strategic concepts involved in the ongoing Russian discussion of IW are most interesting and merit serious consideration here. However, for our purposes we need to focus on the possibility of new technologies, specifically the seventh type of weapon. Psychotropic weapons come very close, at least conceptually, and probably even more so in practice, to creating an overlap between biological warfare (BW) and IW. If one can deploy informatized systems not only to mislead or warp enemy judgment and perception, but also to affect the enemy physiologically by directly targeting the brain's physical structure and content, the systems that do so will cross the boundary from IW into BW. This way of thinking could eventually generate a formulation bringing informational and biological weapons, as well as chemical and/or biological warfare (CBW), and IW closer together in theory and/or in practice. Should Russia or another country be able to deploy such weapons on a mass basis, the results could be catastrophic given the ease with which information weapons and attacks may be disseminated.

Although we cannot know if such weapons are feasible or can be developed, the fact that they have been postulated as a possibility suggests that ongoing research is taking place in Russia—and perhaps with other partners like China—to develop such weapons or find ways of using known systems to accomplish this goal. If such a technological breakthrough were to be consummated, it would have devastating implications and must be kept in mind constantly as a

real possibility for the middle range and longer-term future.

Seventh, Russian writers have now come up with the concept of an information-strike operation *(IUO-Informatsionnaya-udarnaya operatsiya)*.[142] This operation could be targeted against enemies' strike platforms, troops, its society, or some combination thereof and has come to assume an important place in new Russian thinking about operational art.[143] Once again, we see efforts being made, with interesting and even successful results as in the domestic and Georgian cases, to update not only the Leninist threat paradigm, but also the inheritance of Soviet military art. This is not to say we have a mere derivation of the latter for contemporary purposes. Rather, Russian writers and officials dealing with these issues have evolved and are further refining concepts that they find strategically useful from the inheritance bequeathed to them by their Soviet forebears. This process has thus led them to view IW and IO in much grander and arguably much more realistic strategic fashion than has most U.S. and Western writing on the subject. Russian thinking goes far beyond the use of IW to disable weapons systems; command, control, communications and intelligence; or physical infrastructure to embrace a vision of conflict against a society's overall mental patterns.

Thus, Russia is currently waging an IW and a systematic IO against its own people, as we have suggested, as an instrument of domestic counterinsurgency. It tried this out in Chechnya, viewing domestic public opinion and succeeding handsomely in doing so. Since then the Russian population as a whole has been the target of an unremitting special operation, and an IO as well, to ensure that the government alone dominates Russia's information space and the range of plausible political thinking. This relatively success-

ful experiment clearly inspires Russian thinking about IWs and IOs in general and demonstrates to Moscow the practical utility of such operations against an entire society. We therefore can be reasonably certain that this operation will not stop at home or at Russia's borders, and that we will continue to see such efforts taking place beyond Russia's borders in an effort to reshape international opinion concerning Russia. It also goes without saying that elements of all of these foregoing points, as well as some new innovations, are all discernible in Russia's aggression against Ukraine and Russia's threats and IW directed against the West.

We ignore such thinking at our own peril. Given the besetting ethnocentric vice of U.S. writing on defense, strategy, and war, it may be no surprise that we have not done nearly as well in exploiting the opportunities presented by the advances in information technology as we should have, mainly because of incapacity to think strategically about it. While Russian efforts have been hobbled by serious organizational and technical shortcomings; that is no excuse for us to ignore Russian thinking.[144] Indeed, it was the combination of Russian thinking aligned to the early stages of the "revolution in military affairs" and new operational concepts that gave us our last clear victory in Operation DESERT STORM. We could do worse than to relearn this lesson.

ENDNOTES - CHAPTER 8

1. Barry Buzan, Ole Wæver, Jaap de Wilde, *Security: A New Framework For Analysis*, Boulder, CO: Lynne Rienner Publishers, 1998; Giampiero Giacomello and R. Craig Nation, eds., *Security in the West: Evolution of a Concept Milan*, Milan, Italy: Vita et Pensiero, 2009; Stephen Blank, "Security: An Unending Debate," in Giampiero Giacomello and R. Craig Nation, eds., *Security in the West: Evolution of a Concept Milan*, Milan, Italy: Vita et Pensiero, 2009, pp. 59-82.

2. Buzan, Wæver, De Wilde.

3. Elizabeth Wishnick, "The Securitization of Chinese Migration to the Russian Far East: Rhetoric and Reality," in Melissa G. Curley and Wong Siu-lun, eds., *Security and Migration in Asia: The Dynamics of Securitisation*, New York: Routledge, 2008; Kristian Åtland and Kristin Van Bruusgaard, "When Security Speech Acts Misfire: Russia and the Elektron Incident," *Security Dialogue*, Vol. XL, No. 3, 2009, pp. 335-336.

4. Edwin Bacon and Bettina Renz with Julian Cooper, *Securitising Russia: The Domestic Politics of Russia*, Manchester, UK: Manchester University Press, 2006, pp. 10-11.

5. Kristian Åtland and Torbjørn Pedersen, "The Svalbard Archipelago in Russian Security Policy: Overcoming the Legacy of Fear—Or Reproducing It?" *European Security*, Vol. 17, Nos. 2-3, June-September 2008, pp. 230-231.

6. Alexander Rzheshevsky, "Far East Military Threats: Old and New," Moscow, *Parlametnyskaya Gazeta*, in Russian, May 24, 2005; Open Source Committee, *Foreign Broadcast Information Service Central Eurasia,* (Henceforth FBIS SOV), May 24, 2005.

7. *Ibid.*

8. Rostov na Donu, "*Voyenny Vestnik Yuga Rossii*," in Russian, November 20, 2006, FBIS SOV, November 20, 2006.

9. *Ibid.*

10. *Ibid.*

11. FBIS SOV, March 31, 2006.

12. *Ibid.*

13. Vladimir Putin, "Annual Address to the Federal Assembly," Moscow, Russia, April 26, 2007, available from *en.kremlin.ru/events/president/transcripts/24203*.

14. Vladimir Putin, "Rossiya i Menyaushchiysiya Mir," *Moskovskiye Novosti*, February 27, 2012, pp. 6, 14.

15. Moscow, *Interfax*, in English, October 3, 2012; FBIS SOV, October 3, 2012.

16. Valdai Discussion Club Analytical Report, *Military Reform: Toward the New Look of the Russian Army*, 2012, p. 8, available from *valdaiclub.com*.

17. "Military Doctrine of the Russian Federation," February 5, 2010, available from *kremlin.ru*; also available in FBIS SOV, February 9, 2010.

18. Cited in Colonel Timothy L. Thomas (USA Ret.), *Recasting the Red Star: Russia Forges Tradition and Technology Through Toughness,* Ft. Leavenworth, KS: Foreign Military Studies Office, 2011, p. 143.

19. Thomas, *Recasting the Red Star*, p. 247.

20. Moscow, *Interfax-AVN Online*, in English, January 30, 2012, FBIS SOV, January 30, 2012.

21. "International: Open Source Center OSC Summary," in English, December 2, 2011, FBIS SOV, December 2, 2011.

22. John E. Bolen, Jr., *Operational Art Goes Digital: Information Warfare and the Future of Russian Operational Theory*, Summer Student Paper, Carlisle Barracks, PA: U.S. Army War College, August 2012, p. 16.

23. *Ibid.*

24. William M. Darley, "Clausewitz's Theory of War and Information Operations," *Joint Forces Quarterly*, No. 40, 2006, pp. 73-79.

25. Franklin Kramer, Stuart H. Starr, and Larry Wentz, eds., *Cyberpower and National Security*, Washington, DC: Potomac Books, 2009.

26. Colonel Richard G. Zoller, "Russian Cyberspace Strategy and a Proposed United States Response," in Jeffrey L. Caton, John H. Greenmyer, Jeffrey L. Groh, and William O. Waddell, eds., *Information as Power: An Anthology of Selected United States Army War*

College Papers, Vol. 5, Carlisle Barracks, PA: Strategic Studies Institute, U.S. Army War College, 2011, p. 118.

27. Vladimir Vasilyevich Karyakin, "The Era of a New Generation of Warriors—Information and Strategic Warriors—Has Arrived," Moscow, Russia, *Nezavisimaya Gazeta Online*, in Russian, April 22, 2011, FBIS SOV, September 11, 2012.

28. *Ibid*.

29. Stephen Blank, "Class War on the Global Scale: The Culture of Leninist Political Conflict," Stephen J. Blank *et al*., *Conflict, Culture, and History: Regional Dimensions*, Maxwell AFB, AL: Air University Press, 1993, pp. 1-55.

30. FBIS SOV, September 11, 2012.

31. *Ibid.*

32. *Ibid.*

33. *Ibid.*

34. *Ibid.*

35. Thomas, *Recasting the Red Star*, p. 247.

36. *Radio Free Europe Radio Liberty Newsline*, November 9, 2006; Vladimir Isachenkov, "Spy Chief: West Wants to Split Russia," Associated Press, October 10, 2007.

37. E. Leigh Armistead, ed.*, Information Warfare: Separating Hype from Reality,* Washington, DC: Potomac Books, 2007.

38. *Ibid.*

39. Moscow, *NTV*, in Russian, August 15, 2007, FBIS SOV, August 15, 2007.

40. M. A. Gareyev, "Russia's New Military Doctrine: Structure: Substance," *Military Thought*, No. 2, 2007, pp. 1-14; Yu N. Baluyevsky, "Theoretical and Methodological Foundations of the Military Doctrine of the Russian Federation (Points for a Report)," *Military Thought*, No. 1, 2007, pp. 15-23, exemplify this point.

41. Gareyev, p. 4.

42. Aleksandr Dugin, "Russia on the Threshold of a Network War," *Izvestia,* October 18, 2007, cited in *Johnson's Russia List,* October 18, 2007.

43. Minsk, Russia, *Belarusian Television 1*, in Russian, August 12, 2007, FBIS SOV, August 12, 2007.

44. *Ibid.*

45. Miriam Elder, "Vladimir Putin Accuses Hillary Clinton of Encouraging Russian Protests," *The Guardian*, December 8, 2011, available from *guardian.co.uk/world/2011/dec/08/vladimir-putin-hillary-clinton-russia.*

46. FBIS SOV, August 12, 2007.

47. Ellen Barry, "Russia Moves to Broaden Definition of High Treason," *The New York Times*, September 21, 2012, available from *nytimes.com/2012/09/22/world/europe/russia-moves-to-broaden-definition-of-high-treason.html?_r=0*.

48. El Murid, "Informatsonnye Voiny," *Krasnaya Zvezda*, August 3-9, 2011.

49. "FSB Chief Calls for Wider Cooperation Against Internet Use by Terrorists," *ITAR-TASS*, September 6, 2007.

50. Moscow, *ITAR-TASS*, in English, July 27, 2007, FBIS SOV July 27, 2007.

51. Conversations with U.S. and Russian specialists, August 2007.

52. Moscow, *Kommersant.com*, in English, July 26, 2007, Open Source Committee, FBIS SOV, July 26, 2007; Moscow, *Interfax*, in English, July 25, 2007, FBIS SOV, July 26, 2007.

53. State University-Higher School of Economics RIO Center, *The World Around Russia: 2017, An Outlook for the Midterm Future*, Moscow, Russia: The Council on Foreign and Defense Policy, 2007, p. 25.

54. D. J. Peterson, *Russia and the Information Revolution*, Santa Monica, CA: RAND Corporation, 2005, p. 101.

55. *Ibid*.

56. Murat Sadykov, "Uzbekistan Tightens Control Over Mobile Internet," *Eurasia Insight*, March 15, 2011, available from *eurasianet.org/node/63076*; Fyodor Lukyanov, "Learning From Libya and Singapore,' *Russia in Global Affairs*, February 25, 2011, available from *eng.globalaffairs.ru/redcol/Learning-from-Libya-and-Singapore-15124*; Abulfazal, "Anti-Revolution Agenda: Seize the Control Over Cellular Companies," March 15, 2011, available from *neweurasia.net/cross-regional-and-blogosphere/anti-revolution-agenda-seize-the-control-over-cellular-companies/*.

57. "Azerbaijan Puts Skype in Its Sights," *Eurasia Insight*, May 4, 2011, available from *eurasianet.org/node/63415.*

58. Muhammad Tahir, "Governments Move To Thwart 'Arab Spring' In Central Asia," Human Rights Society In Uzbekistan, Blog Archive, April 28, 2011, available from *en.hrsu.org/archives/1072;* also in *Eurasia Insight*, April 28, 2011, available from *eurasianet.org/node/63386*; Catherine A. Fitzpatrick, "Will the Revolutions in the Middle East Have an Impact on Uzbekistan?" *Eurasia Insight*, February 4, 2011, available from *eurasianet.org/node/62826.*

59. Ruby Russell, "Uzbeks Bristle Under Regime's Web Scrutiny," *The Washington Times*, October 1, 2012, available from *washingtontimes.com/news/2012/oct/1/uzbeks-bristle-under-regimes-web-scrutiny/?page=all*.

60. Konstantin Parshin, "Tajikistan: Dushanbe Web Regulator Creating 'Preposterous Impediments,'" *Eurasia Insight*, January 2, 2013, available from *eurasianet.org/node/66349*.

61. Mariya Y. Omelicheva, *Counterterrorism Policies in Central Asia*, London, UK, and New York: Routledge, 2011.

62. Gennadiy Chernykh and Colonel Valery Sumenkov, "Based on Data, Not Rumors: The Radiological, Chemical, and Biological Situation as a Factor of Information Conflict," Moscow, Russia, *Armeyskiy Sbornik*, in Russian, March 21, 2007, FBIS SOV, March 21, 2007.

63. FBIS SOV, August 15, 2007.

64. R. Bikkenin, "Information Conflict in the Military Sphere: Basic Elements and Concepts," Moscow, Russia, *Morskoy Sbornik,* No. 10, 2003, pp. 38-40, FBIS SOV, February 6, 2004.

65. *Ibid.*

66. Colonel-General Boris Cheltsov, "Approaches to the Creation of the National Aerospace Defense System and the Future Network-Centric Wars," *Military Thought*, No. 4, 2008, pp. 1-11.

67. Roger McDermott, "Russia's Conventional Armed Forces, Reform and Nuclear Posture to 2020," paper presented at the National Defense University conference, "Strategy and Doctrine in Russian Security Policy," Ft. Lesley J. McNair, Washington, DC, June 28, 2010.

68. Lieutenant General Nikolai A. Molchanov, "Information Resources of Foreign States as a Threat to Russia's Military Security," *Military Thought*, No. 4, 2008, pp. 22-31.

69. Colonel S. G. Chekinov, "Predicting Trends in Military Art in the Initial Period of the 21st Century," *Military Thought*, No. 3, 2010, pp. 52-53.

70. *Ibid.,* pp. 44-55.

71. *Ibid.*, p. 56.

72. *Ibid.,* p. 57.

73. Colonel S. G. Chekinov and Lieutenant General S. A. Bogdanov (Ret.), "Strategy of Indirect Approach: Its Impact on Modern Warfare," *Military Thought*, No. 3, 2011, p. 5.

74. *Ibid.*, p. 6.

75. *Ibid.*, p. 9.

76. *Ibid.*

77. *Ibid.*, p. 8.

78. *Ibid.,* p. 10.

79. See also, apart from the articles cited above, Colonel S. G. Chekinov and Lieutenant General S. A. Bogdanov (Ret.), "Asymmetrical Actions to Maintain Russia's Military Security," *Military Thought*, No. 1, 2010, pp. 1-11.

80. "Military Doctrine of the Russian Federation," February 5, 2010, available from *kremlin.ru*, also available in FBIS SOV, February 9, 2010; *Natsional'naya Strategiya Bezopasnosti Rossii, do 2020 Goda*, (*National Security Strategy of the Russian Federation to 2020*), Moscow, Russia Security Council of the Russian Federation, May 12, 2009. It is available from the FBIS SOV, May 15, 2009, in a translation from the Security Council website (henceforth NSS).

81. William J. Dobson, *The Dictator's Learning Curve: Inside the Global Battle for Democracy*, New York: Random House, 2012, p. 31.

82. "Putin made scandalous statement: Putin Admits Moscow Planned Military Actions in Georgia in Advance," Rusavi2, August 9, 2012, available from *news.az/articles/georgia/66174.*

83. Conversations with Estonian authorities in Tallinn, October, 2007.

84. Gadi Evron, "Battling Botnets and Online Mobs," *Georgetown Journal of International Affairs*, Vol. 9, No. 1, Winter/Spring 2008, pp. 122-123.

85. A concise description of the attacks may be found in Rebecca Grant, *Victory in Cyberspace*, Washington, DC: U.S. Air Force Association, pp. 3-9.

86. *Ibid.*, pp. 7-8.

87. James A. Hughes, "Cyber Attacks Explained," Commentary, Washington, DC: Center for Strategic and International Studies, June 15, 2007.

88. Igor Kotenko and Alexander Ulanov, "Agent-Based Modeling and Simulation of Network Softbots' Competition," Enn Tyugu and Takahira Yamaguchi, eds., *Knowledge Based Software Engineering: Proceedings of the Seventh Joint Conference on Knowl-*

edge-Based Software Engineering, Amsterdam, The Netherlands: IOS Press, 2006; Frontiers in Artificial Intelligence and Applications, Vol. 140, pp. 243-253.

89. Stephen Blank, "Towards the Police State: Increasing Authoritarianism in Putin's Russia," *Acque et Terre*, No. 4, 2007.

90. Moscow, *Interfax*, in English, October 10, 2007, FBIS SOV, October 10, 2007; Moscow, *NTV Mir* in Russian, October 10, 2007, FBIS SOV, October 10, 2007; Moscow, ITAR-TASS, in English, October 1, 2007, FBIS SOV, October 1, 2007.

91. Kotenko and Ulanov, pp. 243-253; Conversations with Estonian authorities in Tallinn, Estonia, October, 2007.

92. Blank, "Towards the Police State."

93. Moscow, *Interfax*, in English, October 10, 2007, FBIS SOV, October 10, 2007; Moscow, *NTV Mir* in Russian, October 10, 2007, FBIS SOV, October 10, 2007; Moscow, *ITAR-TASS*, in English, October 1, 2007, FBIS SOV, October 1, 2007.

94. Conversations with Estonian authorities in Tallinn, October, 2007.

95. Tor Bukkvoll, "Putin's Strategic Partnership With the West, the Domestic Politics of Russian Foreign Policy," *Comparative Strategy*, Vol. 22, No. 3, 2003, pp. 231-233; "The EU, May Day and Moscow," Jane's Intelligence Digest, May 7, 2004; Stefan Pavlov, "Bulgaria in a Vise," *The Bulletin of the Atomic Scientists*, January-February, 1998, p. 30; Robert D. Kaplan, "Hoods Against Democrats," *Atlantic Monthly*, December, 1998, pp. 32-36. As Foreign Minister Igor Ivanov said "Fuel and energy industries in the Balkans are totally dependent on Russia. They have no alternative." "Ivanov on Foreign Policy's Evolution, Goals," CDPP, L, No. 43, November 25, 1998, p. 13; U.S.-Slovakia Action Commission: Security and Foreign Policy Working Group: CSIS, and Slovak Foreign Policy Association, *Slovakia's Security and Foreign Policy Strategy,* 2001; Czech Security Information Service*, Annual Report 2000,* available from *bis.cz/eng/vz2000/vz2000_10.html*; "Interview with Russian General Aslambek Aslanbekov," *Trud*, (Bulgaria), April 8, 2004, FBIS SOV*,* October 2, 2002; Conversations with American diplomats and analysts, and East European

analysts in Vilnius and Washington in May 2000, and September, 2001; Max G. Manwaring, *Latin America's New Security Reality: Irregular Asymmetric Conflict and Hugo Chavez*, Carlisle, PA: Strategic Studies Institute, U.S. Army War College, 2007.

96. *Ibid*.; Janusz Bugajski, *Cold Peace: Russia's New Imperialism,* Washington, DC: CSIS, Praeger, 2004; Richard Krickus, *Iron Troikas*, Carlisle, PA: Strategic Studies Institute, U.S. Army War College, 2006; Keith C. Smith, *Russian Energy Politics in the Baltics, Poland, and the Ukraine: A New Stealth Imperialism?* Washington, DC: CSIS, 2004. Magdalena Rubaj and Tomasz Pompowski, "What Is the KGB Interested In?" Warsaw, Poland: Fakt, in Polish, October 19, 2004, Open Source Center, FBIS SOV, October 19, 2004; Jan Pinski and Krzysztof Trebski, "The Oil Mafia Fights for Power," Warsaw, Poland: Wprost, in Polish, October 24, 2004, FBIS SOV, October 24, 2004; Warsaw, Polish Radio 3 in Polish, October 15, 2004, FBIS SOV, October 15, 2004; Warsaw, Poland: PAP, in Polish, December 13, 2004, FBIS SOV, December 13, 2004; Open Source Center Analysis, "Lithuania: Businessman Stonys Wields Power with Russian Backing," FBIS SOV, October 1, 2007.

97. FBIS SOV, December 13, 2004.

98. FBIS SOV, October 1, 2007.

99. Richard J. Krickus, "The Presidential Crisis in Lithuania: Its Roots and the Russian Factor," *Occasional Papers of the East European Studies Institute,* No. 73; Washington, DC: Wilson Center, 2004; Vilnius, *BNS Internet Version* in English, September 21, 2007, FBIS SOV, September 21, 2007; Kaunas, *Kauno Diena Internet Version*, in Lithuanian, September 20, 2007, FBIS SOV, September 21, 2007.

100. Tallinn, *Eesti Ekspress Internet Version*, in Estonian, October 1, 2007, FBIS SOV, October 1, 2007.

101. Bugajski, *Cold Peace*; Krickus, *Iron Troikas*; Keith C. Smith, *Russian Energy Politics in the Baltics, Poland, and the Ukraine: A New Stealth Imperialism?* Washington, DC: CSIS, 2004.

102. Rubaj and Pompowski; Pinski and Trebski; Warsaw, *Polish Radio 3 in Polish*, October 15, 2004, FBIS SOV, October 15, 2004; Bukevoll; Pavlov; Kaplan; Ivanov; U.S.-Slovakia Action Commis-

sion: Security and Foreign Policy Working Group, Washington, DC: CSIS, 2001; Slovak Foreign Policy Association, *Slovakia's Security and Foreign Policy Strategy,* 2001; Czech Security Information Service, *Annual Report 2000*; "Interview with Russian General Aslambek Aslanbekov," *Trud*, (Bulgaria), April 8, 2004, FBIS SOV, October 2, 2002; Conversations with American diplomats and analysts, and East European analysts in Vilnius and Washington in May 2000, and September, 2001; Manwaring.

103. Cory Welt, "Russia and Its Post-Soviet Neighbors," in Andrew C. Kuchins, *Alternative Futures for Russia to 2017: A Report of the Russia and Eurasia Program Center for Strategic and International Studies*, Washington, DC: CSIS, 2007, p. 54.

104. Conversations with Estonian authorities in Tallinn, October, 2007.

105. Jakob Hedenskog and Robert L. Larsson, *Russian Leverage on the CIS and the Baltic States*, Stockholm, Sweden: Swedish Defense Research Agency, 2007, pp. 37-38, available from *foi.se.*

106. Conversations with Estonian authorities in Tallinn, October, 2007

107. *Ibid.*

108. "Looking West—Estonian Minister of Defense Jaak Aaviksoo," *Jane's Intelligence Review,* October, 2007, available from *https://janes.ihs.com/Janes/Display/1193492.*

109. "Looking West"; Joshua Davis, "Web War One," Wired, September, 2007, p. 163; Conversations with Estonian authorities in Tallinn, October, 2007.

110. Conversations with Estonian authorities in Tallinn, October, 2007.

111. *Ibid.*

112. Vadim Radionov, "KGB Servicemen Motif Used in Public Relations Campaign," Riga, Latvia, *Chas Internet Version*, in Russian, October 2, 2007, FBIS SOV, October 2, 2007; "Latvian Government Resigns," December 5, 2007, available from *stratfor.com*.

113. M.A. Gareev, "Russia' New Military Doctrine: Structure: Substance," *Military Thought*, No. 2, 2007, pp. 1-14; Yu N. Baluyevsky, "Theoretical and Methodological Foundations of the Military Doctrine of the Russian Federation (Points for a Report)," *Military Thought*, No. 1, 2007, pp. 15-23 exemplify this point.

114. Ivo Ducacek as cited in Jan T. Gross, "Social Consequences of War: Preliminaries to the Study of Imposition of Communist Regimes in East Central Europe," *Eastern European Politics and Societies*, Vol. III, No. 2, Spring 1989, p. 287.

115. James M. Markham, "Spain's Terror, Onus on the Soviets," *The New York Times*, May 11, 1980.

116. Christopher Andrew and Vasili Mitrokhin, *The World Was Going Our Way: The KGB and the Battle for the Third World*, New York: Basic Books, 2005.

117. Eli Jellenc and Kimberly Zenz, *Global Threat Research Report: Russia*, Defense Security Report, January 2007, cited in Kara Flook, "Russia and the Cyber Threat," May 13, 2009, available from *criticalthreats.org/russia/russia-and-cyber-threat*.

118. Gregg Keizer, "Russian 'Cybermilitia' Knocks Kyrgyzstan Offline," January 28, 2009, available from *computerworld.com/s/article/9126947/Russian_cybermilitia_knocks_Kyrgyzstan_offline?taxonomyName=security*.

119. James McQuaid, "The RBN Operatives: Part II," Secure Home Network, September 8, 2008, available from *securehomenetwork.blogspot.com/2008/09/rbn-operatives-part-ii.html*. Cited in Flook.

120. Flook.

121. Dighton Fiddner, *National Cyber Security Strategy Against Malevolent Use of the Global Cyberspace*, paper presented at the conference World International Studies Committee (WISC) 3rd Global International Studies, University of Porto, Porto, Portugal, August 17-20, 2011, p. 26.

122. Richard Weitz, "Global Insights: Russia Refines Cyber Warfare Strategies," *World Politics Review,* August 25, 2009, available from *worldpoliticsreview.com/articles/print/4218*.

123. *Ibid.*

124. "Overview by the US-CCU (Cyber-Consequences Unit) of the Cyber Campaign Against Georgia in August of 2008," U.S. Cyber Consequences Unit, 2009.

125. Brian Krebs, "Report: Russian Hacker Forums Fueled Georgia Cyber attacks," *The Washington Post*, October 16, 2008, available from *washingtonpost.com*.

126. "Overview by the US-CCU of the Cyber Campaign Against Georgia in August of 2008."

127. *Ibid.*

128. Alexander Melikishvili, "The Cyber Dimension of Russia's Attack on Georgia," *Eurasia Daily Monitor*, September 12, 2008; David Hollis, "Cyberwar Case Study: Georgia 2008," *Small Wars Journal,* 2011, available from *smallwarsjournal.com.*

129. *Ibid.*; "Overview by the US-CCU of the Cyber Campaign Against Georgia in August of 2008."

130. "Russia's Intelligence Paves Way to War," *Jane's Intelligence Digest*, August 21, 2008.

131. Captain Paulo Shakarian (USA), "The 2008 Russian Cyber Campaign Against Georgia," *Military Review*, November-December, 2011, p. 65.

132. Melikishvili.

133. "Overview by the US-CCU of the Cyber Campaign Against Georgia in August of 2008."

134. *Ibid.*

135. *Ibid.*

136. *Ibid.*

137. See the following Essays in the collection, Zalmay M. Khalilzad and John P. White, eds., *The Changing Role of Information in Warfare*, Santa Monica, CA: Rand Corporation, 1999; Andrew W. Marshall, Foreword; Jeremy Shapiro, "Information and War: Is It a Revolution?" p. 133; John Arquilla, David Ronfeldt, and Michele Zanini, "Networks, Netwar, and Information-Age Terrorism," p. 81; Roger Molander, Peter A. Wilson, and Robert H. Anderson, "U.S. Strategic Vulnerabilities: Threats Against Society," pp. 253-280.

138. Chris C. Demchak, "Hacking the Next War," *The American Interest*, Vol. VIII, No. 1, September-October, 2012, p. 72.

139. "Overview by the US-CCU of the Cyber Campaign Against Georgia in August of 2008."

140. *Ibid.*

141. Timothy L. Thomas, "Recent Developments in Russia's Information War Theory," paper presented at the SSI workshop (Europe module) of the Future Landpower Environment Project (FLEP), Washington, DC, July 10-11, 2001; see Vladimir Rubanov's Remarks at the Press Conference Regarding Russia-West partnership in the Sphere of Security, Arbat Hotel, Moscow, Russia, October 17, 2000, in *CDI Russia Weekly*, No. 120, October 20, 2000; Timothy Thomas, "The Russian view of Information War," Colonel Michael H. Crutcher (USA Ret.) ed., *The Russian Armed Forces At the End of the Millennium*, Carlisle, PA: Center for Strategic Leadership, U.S. Army War College, 2001, pp. 335-360; Timothy L. Thomas, *Information Technology: US/Russian Perspectives and Potential for Military-Political Cooperation*, Fort Leavenworth, KS: Foreign Military Studies Office, 1999, available from *call.army.mil/call/fmso/fmsopubs/issues/infotech.htm;* Lester W. Grau and Timothy L. Thomas, "A Russian View of Future War: Theory and Direction," *Journal of Slavic Military Studies*, Vol. IX, No. 3, September, 1996, pp. 501-518; Timothy L. Thomas, "Deterring Information Warfare: A New Strategic Challenge," *Parameters*, Vol. XXV, No. 4, Winter, 1996-97, pp. 81-91; Timothy L. Thomas, "Russian Views on Information-Based Warfare," *Airpower Journal*, Special Issue, 1996, pp. 25-35; Timothy L. Thomas, "Dialectical Versus Empirical Thinking: Ten Key Elements of the Russian Understanding of Information Operations," paper presented to the U.S. Army War

College, Annual Strategy Conference, Carlisle, PA, April 22-24, 1997; Edward Waitz, "The US Transition to Information Warfare," *Journal of Electronic Defense*, December, 1998, p. 36; Sergei Modestov, "The Possibilities for Mutual Deterrence: a Russian View," *Parameters*, Vol. XXVI, No. 4, Winter, 1996-1997, pp. 92-98.

142. Bolen; Thomas, *Recasting the Red Star*, pp. 351-354.

143. *Ibid*.

144. Thomas, *Recasting the Red Star*, pp. 295-345; Ariel Cohen and Colonel Robert Hamilton, *The Russian Military and the Georgian War: Lessons and Implications*, Carlisle, PA: Strategic Studies Institute, U.S. Army War College, 2011; Stephen Blank, *The Soviet Military Views Operation Desert Storm: A Preliminary Analysis*, Carlisle, PA: Strategic Studies Institute, U.S. Army War College, 1991.

CHAPTER 9

THE ADAPTIVE NATURE OF CRIME: CO-OPTING THE INTERNET

Shawn C. Hoard
Jeffrey L. Carasiti
Edward J. Masten

INTRODUCTION

Organized crime started in classical antiquity, with the Illyrian pirates who plundered ships in the Adriatic Sea. Long since conquered by the Romans and all but forgotten by history, the Illyrian pirates stand as one of the earliest known examples of a group (albeit sanctioned by the queen) working together to participate in illegal activities for profit.[1] Organized crime, in the manner we know it, has been around since the 1800s, in one form or another. Irish immigrants to the United States, in need of protection and income, formed groups like the Forty Thieves to address those needs. In the 1920s, organized crime groups saw Prohibition as a way to vastly increase their profits and influence, and began illegally producing and distributing alcohol.[2] While the typical nature of organized crime groups has changed dramatically since then, the common goals shared by members of such groups remain the same as they have always been: protect your business, protect each other, and make money. In the same way that organized crime groups adapted to meet the opportunity Prohibition provided, today's criminals are exploiting the opportunities technology brings.

No longer do criminals need to risk their physical well-being to make money. In the 21st century they

have been increasingly shifting toward digital crimes and money laundering, to both increase reward and reduce risk. As McKenzie O'Brien noted:

> Criminal organizations, true to their adaptive and adroit nature, have merely co-opted the Internet to more easily, more safely, and more successfully provide services, expand their clientele base, and ultimately derive more profit.[3]

This was evident in October 2004, when the New Jersey State Commission of Investigation reported that while traditional mob moneymakers, like narcotics trafficking, gambling, prostitution, and loan-sharking remained prevalent, those techniques were supplemented by identity theft rackets, money-laundering schemes, multi-million-dollar financial frauds, and other sophisticated activities that utilized the most recent technological advancements to subvert legitimate commerce.[4]

Organized crime groups have not only found ways to improve classic forms of lucrative crime; they have also forged entirely new moneymaking and money laundering ventures with the aid of the Internet and its wide user base. Advancements in this technology and its proliferation have, in turn, allowed more actors to perform illegal cyberactivities across the world. For example, technology like the TOR Browser, which was created by the U.S. Naval Research Laboratory, has allowed Internet users to access any website while remaining anonymous by bouncing their Internet Protocol (IP) address from one node to another around the world. It also has created the "Deep Web," which consists of websites that can only be accessed while using the TOR Browser. Virtual currencies, particularly crypto-currencies such as Bitcoin, have enabled these

same users to transfer money globally within a matter of minutes and with a high degree of anonymity.

Accordingly, this chapter examines some of these technologies and their use in order to highlight various ways that criminals have "co-opted the Internet." This chapter begins with a section on the technology that cyberspace provides criminals to carry out new methods of illicit profit creation. This is followed by an examination on how the Internet and cybertechnology not only facilitate, but also enhance traditional criminal practices. Next is an examination of how money laundering has expanded into the cyberworld. This chapter concludes with several case studies that highlight how organized crime and money laundering operate in cyberspace.

CYBERCRIME TECHNIQUES AND TOOLS

In recent years, organized criminals have been taking full advantage of all the efficiencies, synergies, and multiplier benefits that computers and the Internet bring to their trade. The advent of these tools has generated new opportunities for criminals to steal and monetize information. Whether it is using cyberspace to access and appropriate secret information, reach a broader audience with targeted sales techniques, or directly steal from victims' bank accounts, skilled cybercriminals are proving themselves to be formidable and malevolent actors in cyberspace.

The Norton Cybercrime Report in 2012 announced that the global cost of cybercrime was approximately $388 billion; while the global cost of drug trafficking marijuana, cocaine, and heroin was $288 billion.[5] Although there is certainly a significant difference between the numeric totals of the compared amounts, the numbers listed indicate the costs of cybercrime

and drug trafficking, not the profit gained by criminal groups participating in either of the two fields. Nevertheless, it is clear that criminal organizations would be remiss if they did not take advantage of the virtual opportunities to expand their portfolios of illicit activities.

In order to increase profits, criminal organizations have been adopting techniques that arrived with the widespread adoption of personal computers and the Internet, such as the use of malware to hack into and sometimes control other computers, and phishing—the unlawful acquisition and use of someone else's personal financial information. They have also exploited cyber currencies and "dark" markets. The following sections will discuss ways in which criminal organizations have upped their cyber arsenal in order to boost their capabilities.

Malware.

Since the advent of the computer, hackers have been exploiting software to gain unauthorized access to systems. Malware is integral to the modern-day bank robberies conducted by organized crime. Indeed, criminals have used malware to conduct previously high-risk crimes, like bank robbery, by gaining access to computers protected by information security teams, armed guards, firewalls, or literal walls—and incurred little risk in doing so. A good example is Carbanak, a successful group of cybercriminals who used malware to siphon money from over 100 different financial institutions.[6] This case is discussed more fully below.

Cybercriminals often use malware to steal access codes to bank accounts, advertise products on a com-

promised computer, or illegally access and utilize an infected computer's resources. Common uses of infected computers include the use of botnets to run spam campaigns, conduct blackmailing operations, or participate in large-scale Distributed Denial of Service (DDoS) attacks as a form of extortion.[7] Decades ago, criminals would have to break physically into facilities or bribe someone in order to gain access to secret information. Now, they can hack into servers with malware and steal valuable financial information without even leaving the house. Indeed, in several highly publicized hacks, criminals have installed malware onto Point of Sale systems in order to steal the credit card information from every card that swipes through the devices. This is a creative approach that blends hacking, malware, and carding to exploit modern day vulnerabilities in cyberspace.

Spam and Phishing.

Nearly everyone with an email address has received spam or junk emails in his or her inbox. Cybercriminals will sometimes send out massive amounts of these spam emails in an attempt to solicit business or information from victims or the victims' computers. Spamming is not an inherently new venture. Criminals have been running similar scams for decades, with an early form of advance-fee fraud, which became prevalent in the 19th century, known as the Spanish Prisoner confidence trick.[8] In this particular scam, the criminal employed persuasive writing to con the victim into sending an advance of money to help the Spanish prisoner get out of jail. If the victim fell for it, the criminal would conveniently require more funds, due to increased hardships or changing

developments. Schemes such as these have only been enhanced by the convenience of cyberspace.

In appropriating these kinds of scams for their own use, Nigerians have altered the advance-fee fraud technique and added more modern mechanisms, using email instead of postal mail. These schemes have become so prolific that they have been termed 419 scams, after the section of the Nigerian Criminal Code that deals with fraud.[9] In 419 email scams, the criminal often attempts to implore sympathy from the victim to entice a payment. These emails are sent in massive spam campaigns, in which criminals figuratively throw an enormous net into cyberspace and see who is gullible enough to be caught in it. Even if the majority of Internet users recognize the emails as fake, and only 0.1% of the emails sent are actually opened, the ease with which criminals can send these emails means that they have used very modest resources to eke out more income from unsuspecting victims.

Phishing typically involves sending out emails that entice the victim to click on a link included in the email. Often the emails will advertise deals that are too good to pass up, the promise of sexual partners, or cheap access to legal or illegal drugs. Once these types of emails became more commonplace, criminals began changing them to be more believable. If they do not want drugs, prospective victims will not click on a link that promises cheap pharmaceuticals. However, if people see seemingly legitimate emails, informing them that they have new private messages on a social media site, or that they have important emails that have ended up in the junk section of their inbox, they might be more likely to click the links. As soon as people respond by clicking the links they unknowingly download malware to their computers, which, as noted above, can cause a host of different problems.

Often, phishing is used to obtain passwords, credit card numbers, bank accounts, or other information that can be monetized in some shape or form.[10]

Carding.

After cybercriminals have stolen credit card data, whether through malware, hacking, phishing, or a combination of different methods, they are faced with a choice. Either they can attempt to sell the information as "dumps" on an underground forum, or they can monetize the information themselves, through a process called carding. Dubbed the "daily bread of cybercrime," carding is the practice of dealing in hacked or stolen credit card information.[11]

Criminals can conduct carding with the use of specific machinery designed to imprint financial data onto any sort of credit card. Often, criminals use prepaid gift cards, as they are readily available at any grocery store. After using the carding machinery to imprint stolen credit card information onto prepaid cards, those cards can be used to purchase goods, or even directly withdraw funds from automated-teller machines (ATMs) assuming that the criminal has obtained the corresponding Personal Identification Number (PIN) for the card.

A huge boon to the carding practice came with the invention of the skimming device. Skimmers are devices that are designed to fit on top of a Point-of-Sale (POS) system, an ATM card slot, or the entire front side of an ATM (though those devices are obviously both more expensive and more difficult to employ) to collect both card numbers and PINs.[12] The invention of the skimmer is just another example of criminals adapting to exploit the opportunities of the 21st century.

Zero-Day Vulnerabilities.

Zero-day vulnerabilities (i.e. vulnerabilities in software that have not been patched or fixed yet by the developer) are among the most powerful and lucrative tools in the hacking world. After a zero-day vulnerability is discovered, the code information is usually sold to hackers who then use it to direct users of the software to download malware, which, in turn, can steal and transmit targeted data.[13] For example, a zero-day exploit found in Microsoft's Internet Explorer would allow a hacker to install code on certain websites, directing users to servers hosting the exploit, then prompting download of a malware-containing file or add-on. Thus, personnel in key sectors of interest (defense, technology, financial, etc.) can be targeted after identifying the typical websites they visit, and then exploiting the vulnerabilities in the programs hosting or hosted by the websites to infect their computers (sometimes called watering hole attacks).[14]

A powerful market exists for the discovery of zero-day vulnerabilities. Software developers hold "bug buyouts" and contests for individuals to discover such exploits in their products. Companies such as Facebook, Google, and PayPal will pay anywhere from hundreds to tens of thousands of dollars, while a few, such as Microsoft, will pay six figures for certain discovered vulnerabilities in their products.[15] Six-figure minimums appear to be the norm for black market purchasing of zero-day exploits, with price tags reaching this high for government purchases too.[16] As a result, companies have arisen specifically to discover zero-day exploits or broker sales of the information. Kevin Mitnick, a former black hat hacker,

established one such company.[17] Other entities, such as the Chinese-based "Elderwood Project" (as called by cybersecurity research company Symantec), can target U.S. or other governments' critical infrastructure and technology sectors by discovering, distributing, or using the information of zero-day exploits. Tech giants such as Google have been hacked by the Elderwood Project. Internet Explorer, Adobe products, and other commonly used programs have had their vulnerabilities exploited by this group, which indicates that software with wide user bases is targeted.[18]

With these high price tags, there are strong incentives for new entities to enter into the markets. Companies sell zero-day exploit information currently with little oversight, often only screening customers themselves.[19] As such, zero-day vulnerabilities are one of the most lucrative, and potentially dangerous, tools of cybercrime and cyberwarfare available on the net.

CYBERCRIME AS OLD CRIMES IN NEW BOTTLES

Criminals are evolving and adapting to an increasingly connected world, and in doing so, they are utilizing cyberspace to avoid the risks of some traditional crimes. Moreover, both organized criminals and individual actors are, in some respects, reinventing the wheel to extract illicit profits by using creative approaches to old techniques.

Extortion via DDoS Attack and Intellectual Property Theft.

DDoS attacks are a relatively recent development in the world of online criminal activities. After targeting an organization's website, the attackers utilize two or more computers to send bogus Internet traffic to a website to overload it, essentially parking semi-trucks in grocery store aisles; the fake traffic prevents legitimate customers from accessing the website. Often, attackers utilize a "zombie network" or "botnet," a network of malware-infected computers that the criminal has taken control of, to further enhance the damage caused by the attack.[20]

A capable cybercriminal with a botnet at his or her disposal can attempt to extort money from a business that relies on providing online services.[21] In a typical DDoS attack, an attacker utilizes a botnet of infected computers to send copious amounts of traffic toward a desired target, depleting its resources and knocking it offline. This controlled, "zombie" computer network can be used for many different things, limited only by the botnet master's imagination. For example, in 2008, a Church of Scientology (CoS) video starring Tom Cruise leaked onto the Internet and became massively popular. Upset at the video being "pirated and edited," the CoS threatened YouTube with litigation if it did not remove the video. YouTube acquiesced, and Project Chanology was born.[22] The Internet hacktivist group Anonymous began DDoS attacks against the CoS because the CoS had messed with Anonymous' "lulz," a term stemming from the acronym LOL for laugh out loud. Anonymous was able to completely shutdown the CoS website intermittently for a week in January 2008.[23] The group claimed that utilizing

DDoS attacks was equivalent to conducting a virtual sit-in, in that they both interrupt traffic of some sort. Anonymous' strong belief in what it considered First Amendment rights led it to file a petition to the White House to decriminalize DDoS attacks, thereby allowing Anonymous and others to utilize them as a form of protest.[24] Unsurprisingly, the White House has not decriminalized DDoS attacks.

While Anonymous' use of DDoS falls in somewhat of a legal gray area (or, at least, it did at the time), there are criminal actors who utilize DDoS or other cyberattacks explicitly to extort money from victims, or steal industrial secrets, marketing plans, or intellectual property from business rivals.[25] For example, China has come under fire for sponsoring cybercriminals, specifically the People's Liberation Army Unit 61398. As far back as early 2012, President Obama was concerned about China's overzealous intellectual property theft.[26] Charged with hacking into the networks of Westinghouse Electric, the United States Steel Corporation, and numerous other companies, five members of Unit 61398 were indicted on charges of cybercrime. The indictment named Wang Dong, Huang Zhenyu, Sun Kailiang, Gu Chunhui, and Wen Xinyu as criminals participating in intellectual property theft against the U.S. businesses.[27] As of April 2015, however, the only action observed as a result of PLA Unit 61398's intellectual property theft was China's reaction to the threats. Unsurprisingly, it denied hacking into U.S. organizations and dismissed the evidence discovered by the U.S. Attorney's Office for the Western District of Pennsylvania's evidence as "fabricated facts."[28] In response to the allegations, Chinese officials not only deflected the inquisition, but also accused the United States in return.

Bank Robbery via Hacking and Malware.

From 2003 to 2013, the number of bank robberies in Britain dropped 90 percent. In the United States, there were 3,870 bank robberies in 2012, the lowest figure in decades.[29] The most recent figures show that number is decreasing still, with only 3,430 commercial bank robberies in 2014.[30] One of the main reasons that bank robberies are on the decline is the ever-growing shift away from physical robbery and its inherent risks. While individual actors still steal from banks, organized crime groups rarely take part in bank robberies. Instead, they perform highly lucrative bank heists from comfortable chairs, utilizing either hacking methods or malware to steal information from computers behind firewalls. With the advent of the Internet, online banking became a modern convenience as early as 1995.[31] Now that is has become ubiquitous, criminals have a wealth of methods through which to steal financial information and unlawfully access victims' bank accounts. Utilizing cybercrime to steal from financial institutions allows criminals to both reduce risk and greatly increase their potential reward.

In February 2015, a gang of cybercriminals named Carbanak by security researcher Kaspersky, stole up to $1 billion from over 100 financial institutions. They utilized a technique known as "spear-phishing," in which criminals target pre-selected employees of a bank, and send emails to them that are designed to look legitimate enough to trick them. Then, after the bank employee clicks a seemingly innocuous link, malware is covertly installed onto that computer, allowing Carbanak access to the financial institution's server. After accessing video surveillance systems, the hackers learn the patterns of certain bank clerks, and exploit that knowledge to conduct business like that

specific employee. The hackers, utilizing their newfound knowledge, mimic the activities of certain employees to make withdrawals and transfers without arousing suspicion.[32]

The amount of money surreptitiously stolen from banks in this manner is cause for alarm, and highlights glaring weaknesses in the security standards of financial institutions. Sanjay Virmani, director of Interpol Digital Crime Center, described to Kaspersky the challenges banks face:

> These attacks undermine the fact that criminals will exploit any vulnerability in any system. It also highlights the fact that no sector can consider itself immune to attack and must constantly address their security procedures.[33]

Unless this is done more effectively, cybercommerce could increasingly be seen as a high-risk activity.

Underground Black Markets.

In March 2014, the RAND Corporation released a report on criminal activities in cyberspace, analyzing black markets that trade in all manner of illegal goods and services. The report detailed fundamental characteristics of these black markets and how their existence poses a great threat to the information security environment:[34]

> The hacker market – once a varied landscape of discrete, ad hoc networks of individuals initially motivated by little more than ego and notoriety – has emerged as a playground of financially driven, highly organized, and sophisticated groups . . . [it] has now become a burgeoning powerhouse of highly organized groups, often connected with traditional crime

groups (e.g., drug cartels, mafias, terrorist cells) and nation-states.[35]

Below, a diagram from RAND proportionally depicts the different participants and levels in the underground market. It also gives examples of various roles and shows the typical skill level and sophistication of those roles.[36]

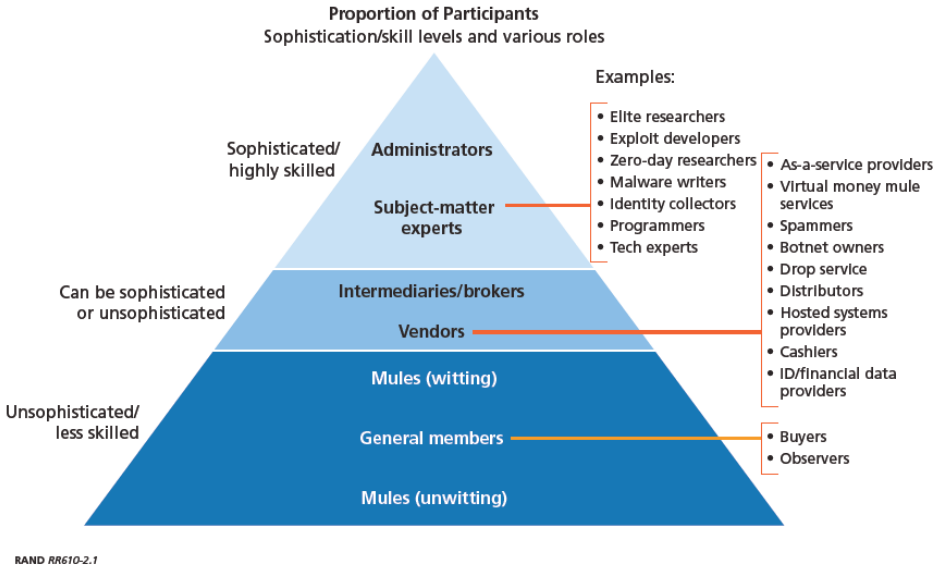


Figure 9-1. Different Levels of Participants in the Underground Market.[37]

Given the findings of the RAND research, it should come as no surprise that organized crime groups have taken to using the Internet as another tool to deal drugs. However, the drug trade moving toward the Internet poses a threat to traditional drug dealers and criminal organizations. Up-and-coming dealers can rely solely on the Internet to conduct business and can

do so at lower risk and lower cost than their counterparts using traditional mechanisms for drug dealing. Moreover, the deals can be conducted using Bitcoin, a crypto-currency that is discussed more fully below.

Cybersex Trafficking.

Human trafficking, slavery, and forced sexual exploitation have been pervasive throughout human history. Following the theme of this chapter, however, these crimes provide even more examples of how criminals have adapted to the cyber age to continue their corrupt endeavors under new packaging. In the Philippines, like everywhere else, organized crime groups have used human and sex trafficking as a primary source of income for decades. Given that there could be up to 100,000 Philippine children involved in the sex trade, it is clear that Philippine organized crime groups see trafficking as a lucrative endeavor, and it should come as no surprise that they have adapted to the advent of computers and the Internet.[38] Nowadays, standard laptop computers come equipped with a camera, and criminals have been using this convenience to force underage children of all ages to engage in sexual exploitation with mostly foreign customers via webcam.[39] In effect, the use of cyberspace for sexual exploitation becomes an adjunct to or a substitute for trafficking, not least because it involves minimal start-up costs, an absence of logistical problems, and very limited risk.

Moreover, the risk that does exist can often be neutralized through corruption. Indeed, corruption is one of the biggest enablers and protectors of the cybersex trade. According to the United States Department of State's Trafficking in Persons Report 2013, there is

corruption at all levels of the government, allowing human traffickers to prosper unimpeded. Tellingly, the study states that officials in government units and agencies assigned to enforce laws against human trafficking reportedly permitted trafficking offenders to conduct illegal activities, allowed traffickers to escape during raids, extorted bribes, facilitated illegal departures for overseas workers, and accepted payments or sexual services from establishments known to traffic women and children.[40] It is almost axiomatic that the same kind of support and protection applies to the sexual exploitation of children in cyberspace.

Fortunately, there are non-profit organizations that are working to combat child exploitation, both physically and in cyberspace. Jo Alforgue, Advocacy Officer with End Child Prostitution, Child Pornography and Trafficking of Children for Sexual Purposes (ECPAT Philippines), explained that one of the problems ECPAT Philippines faces is the issue of locating cybersex dens. Since they can be established inside any sort of building with an Internet connection, they can be extremely difficult to identify.[41]

Identity Theft.

With the ever increasing digitizing of personal records and data over the past decades, identity theft is another example of a criminal venture that has morphed into the cyberworld. For decades, criminals have been finding ways to steal enough information to create fake identities, and while would-be identity thieves could use older techniques such as dumpster diving or searching public records, the Internet has now provided enormous new opportunities and a variety of tools with which to steal from potential

victims. In addition to hacking and using malware, identity thieves can use social engineering to trick victims into giving away information; use credit card skimmers to steal credit card information directly as it enters and exits an ATM slot, exploit spear-phishing, and a number of other techniques.

An excellent example of identity theft involved Sang-Hyun Park, a high-level member of the notorious Park Criminal Enterprise (PCE) that dealt in manufacturing new identities for illegal aliens. In addition to fraudulently creating or obtaining driver's licenses, the PCE also stole identities from people and added those identities as authorized users to credit card accounts of various conspirators. This technique enabled them to raise the credit scores of these fake identities, and then open bank accounts and obtain credit cards. Once these accounts and cards were established, the criminal gang would use them to commit fraud. Park also utilized wire transfers to launder money obtained with the aforementioned methods. In this case, however, Park was sentenced to 12 years in prison and five years of supervised release. To make amends, he has also been ordered to pay restitution to the tune of $4.7 million, which is $700,000 more than he admitted to making via his criminal schemes.[42]

MONEY LAUNDERING WITH IMPROVED CLASSIC METHODS

Similar to many of the organized crime methods discussed above, money laundering has also found its place in the cyberworld. While organized crime groups typically prefer classic methods of money laundering, due to their need to move large amounts of money as quickly as possible, many of the more

computer-savvy criminals have expanded their laundering operations into the recent technologies offered to them by Bitcoin and other crypto-currencies. While crime groups are unlikely to switch completely to digital methods of money laundering, they would be remiss not to explore the avenues presented to them with recent technological developments. This portion of the paper details ways in which criminals have co-opted the Internet to increase the efficiency of traditional money laundering methods.

Wire Transfers & Money Mules.

Traditional wire transfers required customers to enter a physical location and fill out paperwork. This practice always exposed the launderer to the staff of the financial institution. In addition to achieving unwanted exposure, the launderer would have to wait a certain amount of time for the wire transfer to complete. Nowadays, with financial transfers being done through mobile banking and Internet payments such as PayPal, launderers are able to bounce funds around to elude law enforcement, without ever needing to show their faces at the financial institutions.

Many criminal organizations utilize money mules to launder their finances. By dividing up the ill-gotten proceeds and having numerous employees send the transfers online, it becomes a more convenient transaction for everyone involved. The faster wire transfer system enables criminal organizations to send funds through multiple mules quickly, further stymying law enforcement. In addition to utilizing faster transfers, many criminal organizations utilize underground forums as a primary means of communication.[43]

Faster Shell Company Creation.

Additionally, thanks to the Internet, people can create shell companies from the comfort of their own home. Utilizing fake business accounts and offshore banking, criminals are able to easily conceal the history of illicit money by creating a bogus entity. The creators can then hide funds under a corporate name without anyone knowing whose money it is. This makes it more difficult for law enforcement to trace particular funds that are deposited or withdrawn from shell companies.[44] Many offshore and bank secrecy jurisdictions advertise such companies online.

In 2014, *The Intercept* reporter Ken Silverstein created his own shell company for investigative reporting. Silverstein found the procedure relatively painless and was able to create the entity easily and quickly:

> The whole process can be done in 15 minutes online or – as I did, on October 28 [2014] – over the phone. It cost $292 . . . I had a friend in Washington serve as my front. The following day she received incorporation papers for my firm – MCSE, an acronym for Medellín Cartel Successor Entity–which was already up and running.[45]

Silverstein also set up another shell firm that operated under a chosen company specializing in setting up these businesses for people, managed by his original shell firm, MCSE. Silverstein was able to do all of this in less than a week and for under $1,000.[46] Clearly, if it is this simple to shield oneself from taxes or law enforcement, action needs to be taken to diminish the ease with which shell companies and their subsidiaries can be established. If not, they are sure to remain a major tool in the money launderer's tool belt, now far more readily accessible through cyberspace.

Use of Prepaid Cards Online.

Lastly, prepaid credit cards are another one of money launderers' best resources. The convenience with which they can be acquired (via purchase or theft at a grocery store), coupled with the capability to be imprinted with stolen credit card information, make these cards a staple of any efficient money launderer. After using machinery to imprint stolen or hacked credit card information, carders can use them to make withdrawals from an ATM.[47] Often, money launderers will buy high-value products, such as Apple computers, Roomba vacuum cleaners, or other items that hold a high retail value, and ship them as a gift to another country; sending the items as a gift ensures that, unless otherwise flagged, the package should pass through customs unmolested. Once the items arrive, the money launderer's partner can sell the item on a black market website, often for more than the original purchase price.

Arguably, the most useful aspect of the prepaid credit card is as a model template for receiving stolen credit card data. Being able to use an untraceable card to purchase other currencies, additional prepaid credit cards, or digital currencies like Webmoney or Bitcoin (discussed in the next section) greatly increases a money launderer's ability to wash large volumes of money faster than law enforcement can trace it.[48]

CASE STUDIES IN CYBERCRIME AND MONEY LAUNDERING

As discussed above, in addition to using cyberspace to enhance traditional criminal activities, criminal organizations and networks have also embraced

newer crime and money laundering methods that rely completely on technology. This section provides detailed case studies demonstrating the technological advances provided to criminals, in the form of anonymity and convenience, to conduct crime and money laundering in the cyberworld.

Liberty Reserve.

Arthur Budovsky incorporated a business called Liberty Reserve in Costa Rica in 2006. He built the business along the same lines as a previous currency exchange owned by himself and an associate, Vladimir Kats. Dubbed the "financial hub of the cybercrime world" in a 2013 indictment, Liberty Reserve enabled customers to create accounts with little to no verification regarding the account holder.[49] If a customer wanted to protect anonymity, he or she could make an account with the email address "no@yahoo.com," a mailing address of 123 Fake Main Street, and a birth date of 01/01/01 without being challenged by Liberty Reserve's registration system.[50] Whether or not the owners of the site were complicit, the site allowed criminals to launder proceeds from a credit card or an investment fraud, identity theft, drug trafficking, and almost any other crime from the convenience of their homes.[51] At any given time, convenient laundering was just a couple of mouse clicks away.

Eventually, Liberty Reserve had an extremely successful digital currency site, known worldwide for allowing criminals to launder ill-gotten income easily. The founders of Liberty Reserve, however, became overconfident. After brazenly discussing in an online chat how everyone in the U.S. knew that Liberty Reserve was a "money laundering operation that hack-

ers use," Budovsky would soon find his and Katz's entire organization shut down.[52] Liberty Reserve had become popular with criminals, but the creators were too lax in their efforts to maintain a law-abiding front, causing the website to be shut down by United States federal prosecutors on May 24, 2013. On May 28, the site was back online, displaying a notice of domain seizure by the United States Treasury Department, the United States Secret Service, and the Department of Homeland Security.[53]

Liberty Reserve was too overt or explicit about its primary use as a money-laundering channel for criminals, and as a result, was eventually seized and shut down. Future virtual currency enthusiasts will likely take note of this mistake, and be sure to champion a more lawful reason for conducting private digital transactions. Perhaps if a digital currency mechanism cited the right to privacy as an avenue for new virtual currency development, it could continue unrestricted by law enforcement.

Bitcoin and Silk Road.

One of the new technologies enabling criminal activity is Bitcoin. Known as the first crypto-currency, and introduced in 2009 by an individual using the pseudonym Satoshi Nakamoto, Bitcoin is a decentralized, purely peer-to-peer, mathematically generated version of electronic cash. It essentially allows direct and digital wire transfers without the need for a financial institution.[54] It provides criminals the ability to buy and sell goods in online black markets with high levels of anonymity. More convenient and private than typical wire transfers, Bitcoin transfers facilitate illicit transactions and money laundering. Yet, because Bit-

coin technology was designed to be a legitimate tool in the fight for privacy, it maintains a more positive image than Liberty Reserve. On the other hand, in the underground/online market Silk Road, Bitcoin was used exclusively as the currency for trading in illegal goods.

Among the attractions of Bitcoin are low transaction costs and confirmation times. The average Bitcoin transaction fee is about 40 cents.[55] In addition, the average transaction confirmation time is very quick, taking around 7.5 minutes in April 2015.[56] As a software-based online payment system, Bitcoin records transactions on a decentralized network called the block chain, which is the underlying technology of all crypto-currencies. The block chain is a public ledger of all transactions since the inception of crypto-currency, but unlike a bank ledger, is not stored in a centralized location. It can be found on any user's computer who has downloaded the software needed to use a crypto-currency. The decentralized nature of crypto-currencies makes it difficult for governmental organizations to regulate these transactions, or shut down the currency.

The value of a crypto-currency like Bitcoin is not determined by the value of a commodity like e-Gold or pegged to a currency like Webmoney and Liberty Reserve, but instead is determined by the supply and the demand of that virtual currency. For example, every ten minutes, 25 Bitcoins are injected into the market through a process called mining. This increases the supply of Bitcoins at regular intervals. Consequently, the demand is what affects the value of Bitcoins most. In November 2013, the value of a single Bitcoin was around one thousand dollars, a 78-fold increase from January 2013.[57] Within a year, the price of a Bitcoin

had dropped to three hundred dollars. Although it spiked back up in 2014, in mid-2015 the exchange rate was below two hundred and fifty dollars due to low demand. The fluctuations highlight the high risk in owning Bitcoins.

On the other hand, the risk has not deterred criminals, as it is one of the most anonymous ways of transferring money. Even though the ledger that contains all transactions is public, very little identifying information can be obtained regarding each transaction. What does appear in the block chain is simply the user's "public address" a string of 26-35 alphanumeric characters, for example, 1BwGkaVotRx8bXXXXtqsab1jHMDoQfWJc. Each time a user performs a transaction, a new public address will appear in association with that transaction, making it very difficult to identify spending patterns. To make Bitcoin transactions even more anonymous, software programmers have developed applications called mixers and tumblers. Essentially, these services are money-laundering programs intended to mask the source of the transaction. A user of a mixer will put his or her Bitcoins into a shared Bitcoin wallet with other users. When the user wants to perform a transaction, many small transactions are performed simultaneously from that single Bitcoin wallet. Using this method, it is nearly impossible for law enforcement to determine which user of a Bitcoin mixing service is the source of the transaction. One of these services is Dark Wallet. Dark Wallet encrypts and mixes users' payments, making the flow of online money untraceable.[58]

The use of Bitcoins is slowly becoming more widespread. Users can obtain Bitcoins through legitimate means, such as by the sale of goods online, Bitcoin mining,[59] and by purchasing Bitcoins from online

exchange services. Despite this, crime still impacts every aspect of Bitcoin. Criminal actors have created mining botnets that harness the computing power of "zombie" computers. They have also created malware that ransoms a compromised computer's files in exchange for Bitcoins. They use stolen credit cards and compromised bank accounts to purchase Bitcoins from less than reputable online Bitcoin exchange services, and of course, criminals sell goods and services in exchange for Bitcoins on underground forums and markets. One of the most famous black market websites that incorporated Bitcoins to purchase drugs, weapons, malware, and stolen personal identifying information was Silk Road, an online market run by Ross Ulbricht, under the infamous moniker "Dread Pirate Roberts," until his arrest in October 2013.

If the average Internet user, who happens to be searching for drugs, performs a search for Silkroad.com, the human resources management and recruiting company's website that comes up will disappoint the user. A more tech savvy user will head directly to the dark web that users can only access using The Onion Router, more commonly referred to as TOR, an IP address obfuscation tool. Once a user accesses Silk Road through TOR all the categories of goods and services are available. Silk Road became most well known for the sale of illicit narcotics. In order to purchase these drugs the user needs to purchase Bitcoins from an online exchange service or a peer-to-peer exchange and load a balance of Bitcoins to the Silk Road website.[60] In effect, Silk Road operated as an escrow service where the administrators acted as middlemen between sellers and buyers. With a balance of Bitcoins uploaded to Silk Road, the user can start purchasing narcotics, including stimulants, psychedelics, pre-

scription, precursors, opioids, ecstasy, cannabis, and steroids.[61] Once these products were purchased, they were shipped in ordinary envelopes through the UPS, FedEx, and even the United States Postal Service.

Since TOR anonymized the IP addresses of its users, the locations of the Silk Road servers were hidden in the dark web, and all the transactions were anonymized by Bitcoin, so Silk Road seemed untouchable. Consequently, the Federal Bureau of Investigation (FBI) in order to disrupt the online black market, had to resort to hacking and undercover operations.

In 2012, an FBI agent posed as a drug dealer desiring to sell cocaine on the website. He emailed the Dread Pirate Roberts, Ulbricht, and asked for instructions. Ulbricht instructed an "employee" of his to help the undercover seller. The employee purchased the cocaine from the undercover agent and had it shipped to his home. When the drugs arrived at the employee's home, the FBI arrested him. Simultaneously, the FBI had hacked into Silk Road and found the locations of the servers hosting the website in Iceland, Latvia, and Romania.[62] The United States has a Mutual Legal Assistance Treaty with these countries, and the FBI was allowed to copy all transactions and emails that occurred on these servers.[63] This began a process that, with some additional luck, led to the identification and subsequent arrest of Ulbricht, who had failed to take precautionary security measures.[64] On February 4, 2015, Ulbricht was found guilty of all charges and was sentenced in May 2015 to life in prison without parole.[65]

In a sad footnote to the case, two Federal agents, one from the Drug Enforcement Administration and one from the Secret service, were indicted for stealing Bitcoins.[66]

Moreover, the sale of drugs in the dark market did not stop with the arrest of Ulbricht and the takedown of the Silk Road website. Within months, a Silk Road 2.0 was launched with the promise of improved security and the ability to be recreated in the case of another FBI takedown of the site.[67] Silk Road 2.0 was also taken down by the FBI a year after its inception, but another version of Silk Road appeared days after the second iteration was shut down.

The FBI has clearly had some success, mostly from hard work, but partially from luck, in arresting and taking down some of these dark web/black market websites. Yet this is offset by criminal adaptability. As soon as one market shuts down, a new version or an alternative underground marketplace takes its place. The punishment of life without parole given to Ross Ulbricht might be the deterrent required to prevent the creation of new black markets on the dark web, but it is not clear that even this will be effective.

The Target Breach.

On November 27, 2013, just as Americans prepared for the annual Black Friday shopping event, hackers, likely from the former Soviet bloc, prepared for an event of their own. These hackers were setting up the groundwork for the exfiltration of one hundred and ten million customer credentials from the Target Corporation's network.[68] This attack lasted until December 15th when Target confirmed that a group of criminals had installed a variant of a POS malware[69] on their POS systems.[70] Although this type of attack was nothing new, the magnitude of damage it caused was worthy of national headlines for months; the attack cost Target roughly $162 million.[71]

Following the Target breach at the end of 2013, cybercriminals using POS malware continued to attack large retail stores like Home Depot, Neiman Marcus, Michaels, Kmart, and Staples. These cybercriminals subsequently expanded their victims to health insurance providers such as Anthem, restaurants such as PF Chang's and Dairy Queen, entertainment companies such as Sony.

Malware can enter a system in many different ways, but one of the most common ways for malware to infect a network is through a phishing campaign. In the case of the Target data breach, it was not Target employees who were the victims of a phishing campaign but a third party vendor based out of Sharpsburg, Pennsylvania, Fazio Mechanical Services, which provided Target with refrigeration, heating, ventilation, and air conditioning (HVAC).[72]

Some of these contracted third party vendors have poor security standards and do not regularly change their access passwords to retailers' systems, allowing criminals who may have hacked these vendors easy, continuing, and repeated access to retailers' networks. Third party vendors also use their personal devices to access a retailer's network, which makes it easier for malware to transfer from one network to another.[73] This was precisely the case in Target's data breach, as The United States Senate Committee on Commerce, Science, and Transportation report indicates that Fazio Mechanical Services "did not appear to follow broadly accepted information security practices. The vendor's weak security allowed the attackers to gain a foothold in Target's network."[74] This could have been made possible because Target did not isolate and segment the POS system from other, unrelated systems like the HVAC.[75]

It appears Target knew its systems were compromised prior to the Department of Justice informing the retailer about the breach in the middle of December.[76] Target might have known as early as November 30, since FireEye, a computer security firm, had installed a malware detection and removal tool six months prior to the attack specifically designed to detect this type of infection. On November 30, FireEye informed Target's security specialists of the problem and on December 2, alerted Target that the criminals had installed a second variant of the malware.[77] Target failed to respond to both alerts.[78] It was not until two days after the Department of Justice alert that Target hired a third-party network forensics team to investigate and remove the malware, thereby ending the attackers' ability to collect consumer data.[79]

The breach was not made public until independent researchers, particularly Brian Krebs, scouring the underground carding forums for new breaches, saw large batches of credit cards appear on credit card dump shops.[80] Krebs, who has connections at financial institutions, checked with the banks to see if there was something in common regarding these cards, and it was noted that these cards were all used at Target stores from the end of November to the middle of December.[81]

While Target did not detect its own data breach, the retail giant does not stand alone in this. A study done by Verizon Enterprise Solutions found that only thirty-one percent of companies that are breached discover the breach on their own by monitoring their network. It is even worse when you look solely at retail companies: only five percent of retailers self-discovered a data breach.[82]

Extortion through DDoS: Russian Hackers vs. Barret Lyon and Online Gambling Site BetCris.com

As mentioned above, DDoS attacks are a preferred method of extortion for cybercriminals. In the early 2000s, hackers would threaten, or carry out, an attack using botnets of computers to send large volumes of fake traffic to certain websites, bringing the sites down. In return, the criminals asked for tens of thousands of dollars to be wired to countries in Eastern Europe to prevent or cease their attack, often promising protection from other attacks for a period of time.[83] This "wave" of cyberextortion began mostly with attacking online gambling sites, with the phenomena being described as a "training ground for extortionists."[84] These cyberextortionists have subsequently broadened the target list to online payment services, foreign currency exchanges, and financial services companies. Indeed, "anyone who could lose money by being offline is a potential online extortion target."[85] As early as 2005, it was estimated that one out of ten companies had been threatened by online extortion, with experts also suggesting that three out of four cases were never reported.[86]

One of the earliest cases of this "wave" of cyberextortion involved an online gambling site based in Costa Rica called BetCris.com.[87] In 2001, Mickey Richardson, the head of the bookmaking and gambling site BetCris.com, paid $500 in eGold as a protection fee to hackers who had just brought down his website with a DDoS attack.[88] For some time after this, extortionists attacked other international bookmakers. The firms would pay these protection fees ranging from $3,000 to $35,000, wiring the money to locations in Russia and Latvia.[89] Fearing another threat, Richardson pur-

chased a $20,000 server "box" that Sacramento, California-based cybersecurity consultant Barret Lyon recommended to filter out attacks.[90] Unfortunately, two years later, on Saturday, November 22, 2003, Richardson received an email stating:

> Your site is under attack. . . . You can send us $40K by Western Union [and] your site will be protected not just this weekend but for the next 12 months. . . . If you choose not to pay . . . you will be under attack each weekend for the next 20 weeks, or until you close your doors.[91]

Richardson, his information technology (IT) department, and his Internet service provider (ISP) were not concerned; they assumed they had protected themselves.[92] This assumption, however, lasted only until the attack began, with BetCris.com crashing later that day; the defensive equipment held for 10 minutes. "BetCris's ISP crashed, and then the ISP for BetCris's ISP crashed."[93] This was followed by another email raising the fee to $50,000 for the next day if a deal was not made in the next hour. The attackers crashed BetCris.com once again as Richardson and his network administrator, Glenn Lebumfacil, tried to stall. During this time, Richardson estimated that the company would lose $1.16 a second, or around $100,000 a day, as long as the site remained down.[94] BetCris.com's ISP decided to "null-route" the site's traffic itself, which meant the ISP was driving all the traffic "into the ground" to free up its pipes.[95] Lyon was called again, and he agreed to help BetCris.com.[96]

Lyon contacted an ISP company called PureGig, located in Phoenix, Arizona, with 10-Gigabits per second pipe, a bandwidth large enough to handle the defensive system he was developing without disturb-

ing PureGig's regular business. PureGig debated the idea but ultimately decided to allow Lyon to build his system with them, hoping that they could learn a better solution to DDoS attacks besides "null-routing" the traffic and essentially shutting down their customers.[97] Three days of no sleep later, Lyon had a system of original code and commercial products put together, describing it as "a highly fortified data center with proxy and security software and some monitoring, and more bandwidth than the bad guys."[98]

By then Richardson had received another email from the extortionists who were upset that a deal had not yet been made. They threatened to take down the site "forever" if no response was forthcoming.[99] Richardson had also reported the attack to the National Hi-Tech Crime Unit (NHTCU) in Scotland Yard. The NHTCU told Richardson to wire two payments of a few thousand dollars each to separate Western Unions in Eastern Europe, so the crime unit could see who picked them up. No one did, and two weeks later Richardson pulled the money back.[100]

Lyon's system intercepted the traffic designated for BetCris.com's servers, filtered out the attack traffic, and allowed legitimate traffic to go to the proper site. The system also monitored, capacity planned, logged, and analyzed.[101] At this point, it was a chess match; the CEO of BetCris.com's Internet service provider said, "every time Lyon would change something, these guys would change something else."[102] The attackers would change attack vectors, and Lyon would need to adjust things to respond.[103] Initially, the extortionists managed to overload the system, and other gambling sites hosted on the same ISP were also taken down.[104]

The extortionists again raised the price, this time to $75,000, but also threatened to "destroy" Richardson's business as punishment for trying to resist.[105] Lyon and PureGig managed to bring the servers back online, and the next two days Lyon continued to adjust his system to handle the attacks. Then the attacks went up to levels unheard of by Lyon, with the extortionists using more than 20,000 hijacked computers.[106] PureGig's servers suffered, and the ISP took Lyon offline to allow a fix. After Lyon again managed to tweak his system to handle much larger attacks, the system was put back on, segregated from PureGig's other traffic now, and BetCris.com and Lyon monitored and adjusted to the attacks for two more weeks. After three weeks the hackers stopped.[107]

Richardson received an email that was interpreted as an admission of defeat, but also mocked the fact that Richardson had lost many times more money in revenue than the protection fee would have been. In the end though, Richardson never paid the extortionists a thing. The attack was treated by Lyon as a "wake-up call on how good the bad guys had gotten," and thus he set out to create and provide an adequate defense to handle the scale of such DDoS attacks and to track down those who attacked BetCris.com.[108]

Lyon started a company called DigiDefense, later renamed Prolexic, with investment from Richardson and another investor. Lyon also recruited Lebumfacil from BetCris.com's IT department. DigiDefense offered subscriptions for Lyon's anti-DDoS system, and BetCris.com was the first customer.[109] Lyon's business in DDoS defense grew, and with more customers, and also more attacks coming in, Lyon renewed focus to track the hackers down. Dayton Turner, an engineer from another extorted gaming site, was recruited, and the two went undercover to find the extortionists.[110]

Lyon and Turner went into online chat rooms to befriend the extortionists and eventually identified a Russian hacker called Ivan.[111] In February 2004, Lyon and Turner submitted a 36-page report profiling Ivan and their correspondence with him and the other hackers to the FBI and the NHTCU.[112] Under the company name DigiDefense International, Lyon and Turner kept communicating with Ivan, who eventually logged into the chat room without masking his IP address.[113] From this, Turner subsequently found the real name of Ivan Maksakov, an address in Saratov, Russia, and a phone number and sent the information to the NHTCU.[114] Following law enforcement undercover and sting operations, in which the NHTCU's, Andy Crocker worked with Colonel Igor Yakovlev from the Russian Ministry of the Interior, Maksakov was arrested and began cooperating with the authorities.[115]

On October 4, 2006, Ivan Maksakov, along with the one who hired him, Alexander Petrov, and another hacker, Denis Stepanov, were sentenced to eight years imprisonment for "extortion, causing material damage, and establishing and applying hostile software."[116] The sentencing attributed the accused with attacks on nine British and Irish bookmakers and casinos between fall 2003 and spring 2004, with direct damage of 2 million pounds and another 40 million pounds expenditure for the protective equipment the companies needed to purchase.[117]

The BetCris.com case is often regarded a major influence on DDoS defense, as well as how such cases were investigated and handled by authorities.[118] It became apparent, however, that six separate online groups conducting DDoS attacks were "deeper and more organized" than initially suspected.[119] And even

though, in this case, some of the major perpetrators were arrested and imprisoned, DDoS attacks remain a significant problem. Moreover, Botnets are readily available for sale or rent, suggesting that the instruments of cybercrime can also be used for cyberwar.

CONCLUSION

Organized crime groups have had centuries to perfect methods of crime and money laundering. While these groups might never transition entirely to crime in cyberspace or virtual money laundering methods, they are systematically exploiting new and existing cybertechnologies to improve their classic methods of crime. Organized crime groups have embraced cyberspace with new types of criminal methods, and they have repackaged or enhanced older methods. They have also taken money laundering into the cyberworld. Specific examples of more and more commonly practiced cryptocurrency money laundering, successful big-data hacking breaches, "professional" hacking and exploitation, and cyberextortion, highlight just how deep and pervasive criminal activities in cyberspace have become. The cases examined above are just a small selection of those available. Nevertheless, they demonstrate that organized crime groups will explore the new opportunities and avenues presented by a set of technologies that continues to evolve. The criminals themselves are flexible and adaptable. Unless law enforcement can be equally innovative, this form of malevolence in cyberspace will continue. Moreover, while it is less serious than threats of cyberwar, even nation-states, tacitly if not explicitly, are able to use the instruments of cybercrime for their own geopolitical and cyberpolitical purposes.

ENDNOTES - CHAPTER 9

1. Dan Diffendale, "The Roman Navy: The First and Second Illyrian Wars, and Incidental Operations (241-219 BCE)," available from *sas.upenn.edu/~dpd/roman_navy/illyrian.html*, accessed on April 18, 2015.

2. National Museum of Crime & Punishment, "Origins of Organized Crime," available from *crimemuseum.org/crime-library/origins-of-organized-crime*, accessed on April 18, 2015.

3. McKenzie O'Brien, "Organized Crime and Cyberspace," Unpublished Paper, The Ridgway Center for International Security Studies, University of Pittsburgh, 2012.

4. State of New Jersey Commission of Investigation, "The Changing Face of Organized Crime In New Jersey: A Status Report," May 2004.

5. Symantec Corporation, "Norton Cybercrime Report 2012," available from *uk.norton.com/cybercrimereport/promo*, accessed on April 19, 2015.

6. Joseph Menn, Lisa VonAhn, and Gunna Dickson, "Cybercrime Ring Steals up to $1 Billion from Banks: Kaspersky," February 14, 2015, available from *reuters.com/article/2015/02/15/us-cybersecurity-banks-idUSKBN0LJ02E20150215*, accessed on April 19, 2015.

7. Kaspersky Lab, "What is Cybercrime," available from *usa.kaspersky.com/Internet-security-center/threats/cybercrime*, accessed on April 19, 2015.

8. "AN OLD SWINDLE REVIVED. - The 'Spanish Prisoner' and Buried Treasure Bait Again Being Offered to Unwary Americans," *The New York Times,* March 20, 1898.

9. Suyog Sainkar, "419 – The Oldest Trick in the Book and Yet Another Scam," April 27, 2010, estimate from *symantec.com/connect/blogs/419-oldest-trick-book-and-yet-another-scam*, accessed on April 19, 2015.

10. Kaspersky Lab, "What is Spam and a Phishing Scam - Definition," available from *https://usa.kaspersky.com/internet-security-center/threats/spam-phishing#.V2vYjKpf3IU,* accessed on April 19, 2015.

11. Misha Glenny, *Darkmarket: How Hackers Became the New Mafia,* New York: Vintage Books, 2012, p. 8.

12. Glenny; Brian Krebs, "The Biggest Skimmers of All: Fake ATMS," December 2013, available from *krebsonsecurity.com /2013/12/the-biggest-skimmers-of-all-fake-atms/*, accessed on June 25, 2015.

13. Pierluigi Paganini, "Elderwood project, who is behind Op. Aurora and ongoing attacks?" Security Affairs Newsletter, September 9, 2012, available from *securityaffairs.co/wordpress/8528/hacking/elderwood-project-who-is-behind-op-aurora-and-ongoing-attacks.html*, accessed on June 25, 2015.

14. *Ibid*.

15. Andy Greenberg, "Kevin Mitnick, Once The World's Most Wanted Hacker, Is Now Selling Zero-Day Exploits," Wired, September 24, 2014, available from *wired.com/2014/09/kevin-mitnick-selling-zero-day-exploits/,* accessed on June 25, 2015; and Andy Greenberg, "Microsoft Finally Offers To Pay Hackers For Security Bugs With $100,000 Bounty," *Forbes*, June 19, 2013, available from *forbes.com/sites/andygreenberg/2013/06/19/microsoft-finally-offers-to-pay-hackers-for-security-bugs-with-100000-bounty/,* accessed on June 25, 2015.

16. Mark Clayton, "Stealing US business secrets: Experts ID two huge cyber 'gangs' in China," *The Christian Science Monitor,* September 14, 2012, available from *csmonitor.com/USA/2012/0914/Stealing-US-business-secrets-Experts-ID-two-huge-cyber-gangs-in-China*, accessed on June 25, 2015; Andy Greenberg, "Shopping For Zero-Days: A Price List for Hackers' Secret Software Exploits," *Forbes,* March 23, 2012, available from *forbes.com/sites/andygreenberg/2012/03/23/shopping-for-zero-days-an-price-list-for-hackers-secret-software-exploits/,* accessed on June 25, 2015. In the latter source, Greenberg provides an estimate of the price tags of various zero-day vulnerabilities for certain programs, usually being sold to U.S. or European governments.

17. Greenberg, "Kevin Mitnick, Once the World's Most Wanted Hacker, Is Now Selling Zero-Day Exploits;" Greenberg, "Microsoft Finally Offers To Pay Hackers For Security Bugs With $100,000 Bounty."

18. Paganini; Greenberg, "Shopping For Zero-Days: A Price List for Hackers' Secret Software Exploits."

19. Greenberg, "Kevin Mitnick, Once the World's Most Wanted Hacker, Is Now Selling Zero-Day Exploits;" Greenberg, "Shopping For Zero-Days: A Price List for Hackers' Secret Software Exploits."

20. Kaspersky Lab, "Distributed Network Attacks/ DDoS," available from *usa.kaspersky.com/Internet-security-center/threats/ddos-attacks*, accessed on April 19, 2015.

21. Kaspersky Lab, "How Could DDoS Affect You?" available from *kaspersky.com/business-security/ddos-protection,* accessed on April 19, 2015.

22. Nick Denton, "Church of Scientology Claims Copyright Infringement," Gawker, January 16, 2008, available from *gawker.com/5002319/church-of-scientology-claims-copyright-infringement,* accessed on April 19, 2015.

23. Dan Kaplan, "DDoS Hack Attack Targets Church of Scientology," *SC Magazine,* January 25, 2008, available from *scmagazine.com/ddos-hack-attack-targets-church-of-scientology/article/104588/,* accessed on April 19, 2015.

24. Mathew J. Schwartz, "Anonymous Says DDoS Attacks Like Free Speech," *Information Week*, January 11, 2013, available from *darkreading.com/risk-management/anonymous-says-ddos-attacks-like-free-speech/d/d-id/1108139*, accessed on April 19, 2015.

25. "Organized Crime Hackers Are The True Threat To American Infrastructure," *The Economist*, March 11, 2013, available from *businessinsider.com/organized-crime-hackers-are-the-true-threat-to-american-infrastructure-2013-3*, accessed on April 19, 2015.

26. Ellen Nakashima, "Indictment of PLA hackers is part of broad U.S. strategy to curb Chinese cyberspying," *The Washington Post,* May 22, 2014 available from *washingtonpost.com/world/national-security/indictment-of-pla-hackers-is-part-of-broad-us-strategy-to-curb-chinese-cyberspying/2014/05/22/a66cf26a-e1b4-11e3-9743-bb9b59cde7b9_story.html,* accessed on April 19, 2015.

27. Department of Justice, "U.S. Charges Five Chinese Military Hackers for Cyber Espionage Against U.S. Corporations and a Labor Organization for Commercial Advantage," May 19, 2014, available from *justice.gov/opa/pr/us-charges-five-chinese-military-hackers-cyber-espionage-against-us-corporations-and-labor*, accessed on April 19, 2015.

28. Michael S. Schmidt and David E. Sanger, "5 in China Army Face U.S. Charges of Cyberattacks," *The New York Times,* May 19, 2014, available from *nytimes.com/2014/05/20/us/us-to-charge-chinese-workers-with-cyberspying.html*, accessed on April 19, 2015.

29. "Bank robberies decrease as criminals switch to cybercrime," *United Press International*, December 27, 2013, available from *upi.com/Science_News/Technology/2013/12/27/Bank-robberies-decrease-as-criminals-switch-to-cyber-crime/UPI-51831388189252*, accessed on April 19, 2015.

30. United States Department of Justice, Federal Bureau of Investigation, Bank Crime Statistics 2014, Washington, DC: F.B.I. Headquarters, March 9, 2015.

31. Financial Web, "Online Banking vs Traditional: Which Is Better?" available from *finweb.com/banking-credit/online-banking-vs-traditional-which-is-better.html*, accessed on April 19, 2015.

32. Menn, VonAhn, and Dickson.

33. *Ibid*.

34. Lillian Ablon, Martin C. Libicki, and Andrea A. Golay, *Markets for Cybercrime Tools and Stolen Data: Hackers,* Santa Monica, CA: RAND Corporation, 2014, p. iii.

35. *Ibid*., p. ix.

36. *Ibid*., p. 6.

37. *Ibid*.

38. Andrew Harding, "'Chairman' Reveals Seedy World of Trafficking," BBC News, April 1, 2007, available from *news.bbc.co.uk/2/hi/asia-pacific/6507495.stm*, accessed on April 20, 2015.

39. Sunshine de Leon, "Cyber-Sex Trafficking: A 21st Century Scourge," CNN, July 17, 2013, available from *cnn.com/2013/07/17/world/asia/philippines-cybersex-trafficking/,* accessed on April 18, 2015.

40. United States Department of State, *Trafficking in Persons Report 2013,* Washington, DC: Office of the Under Secretary for Civilian Security, Democracy, and Human Rights, June 2013.

41. de Leon.

42. District of New Jersey U.S. Attorney's Office, "Leader of Large-Scale Identity Theft Ring Sentenced to 12 Years in Prison for His Role in Fraud Enterprise," February 11, 2014, available from *fbi.gov/newark/press-releases/2014/leader-of-large-scale-identity-theft-ring-sentenced-to-12-years-in-prison-for-his-role-in-fraud-enterprise*, accessed on April 20, 2015.

43. Interview conducted by the author with anti-money laundering expert, 2015; source requested anonymity.

44. *Ibid*.

45. Ken Silverstein, "Setting Up a Bogus Shell Corporation Is Really Easy," Vice, December 15, 2014, available from *vice.com/read/setting-up-a-bogus-shell-corporation-is-really-easy-1215*, accessed on April 21, 2015.

46. *Ibid*.

47. Glenny, p. 43.

48. Clay Michael Gillespie, "Circle Allows Prepaid VISA Cards to Purchase Bitcoin," CryptoCoinNews, September 30, 2014, available from *cryptocoinsnews.com/circle-allows-prepaid-visa-cards-purchase-bitcoin/*, accessed on April 21, 2015.

49. U.S. District Court of the Southern District of New York, "United States of America v. Liberty Reserve," May 28, 2013.

50. Jack Cloherty, "'Black Market Bank' Accused of Laundering $6B in Criminal Proceeds," ABC News, May 28, 2013, available from *abcnews.go.com/US/black-market-bank-accused-laundering-6b-criminal-proceeds/story?id=19275887*, accessed on April 20, 2015.

51. Dominic Rushe, "US prosecutors: Liberty Reserve ran $6bn money-laundering scheme," *The Guardian,* May 28, 2013, available from *theguardian.com/business/2013/may/28/liberty-reserve-accused-money-laundering*, accessed on April 20, 2015.

52. Kim Zetter, "Liberty Reserve Founder Indicted on $6 Billion Money-Laundering Charges," Wired, May 28, 2013, available from *wired.com/2013/05/liberty-reserve-indicted/*, accessed on April 21, 2015.

53. Brian Krebs, "U.S. Government Seizes LibertyReserve.com," KrebsonSecurity Blog, May 13, 2013, available from *krebsonsecurity.com/2013/05/u-s-government-seizes-libertyreserve-com/*, accessed on June 25, 2015.

54. Tal Yellin, Dominic Aratari, and Jose Pagliery, "What Is Bitcoin?" CNN (Money Section), available from *money.cnn.com/infographic/technology/what-is-bitcoin/*, accessed on April 21, 2015.

55. Perianne Boring, "Why Small Businesses - And President Obama - Would Be Wise To Jump On The Bitcoin Spaceship," *Forbes,* May 12, 2014, available from *forbes.com/sites/perianneboring/2014/05/12/why-small-businesses-and-president-obama-would-be-wise-to-jump-on-the-bitcoin-spaceship/*, accessed on April 21, 2015.

56. Blockchain.info, "Bitcoin Median Transaction Confirmation Time (With Fee Only)," available from *blockchain.info/charts/avg-confirmation-time*, accessed on April 21, 2015.

57. Ben Rooney, "Bitcoin prices top $1,000," CNN (Money Section), November 27, 2013, available from *money.cnn.com/2013/11/27/investing/bitcoin-1000/*, accessed on June 1, 2015.

58. Andy Greenberg, "'Dark Wallet' Is About to Make Bitcoin Money Laundering Easier Than Ever," Wired, April 29, 2014, available from *wired.com/2014/04/dark-wallet/*, accessed on June 1, 2015.

59. Bitcoin mining is the process of creating "blocks" on the block chain, a public record of all transactions using Bitcoin. In order to create the block, a user's computer must complete a series of increasingly complex equations designed to confirm the validity of all transactions. Once the block is created, it is broadcasted to all other users of Bitcoin and the computer that completed the block receives Bitcoins in return.

60. Criminals using Bitcoin prefer peer-to-peer exchanges because it provides the highest level of anonymity. In this exchange, two individuals meet in person and exchange cash for bitcoins.

61. Justin Norrie and Asher Moses, "Drugs bought with virtual cash," *The Sydney Morning Herald,* June 12, 2011, available from *smh.com.au/technology/technology-news/drugs-bought-with-virtual-cash-20110611-1fy0a*, accessed on June 1, 2015.

62. Donna Leinwand Leger, "How FBI brought down cyber-underworld site Silk Road," *USA Today,* May 15, 2014, available from *usatoday.com/story/news/nation/2013/10/21/fbi-cracks-silk-road/2984921/*, accessed on June 1, 2015.

63. Andy Greenberg, "New Silk Road Drug Market Backed Up To '500 Locations In 17 Countries' To Resist Another Takedown," *Forbes*, December 6, 2013, available from *forbes.com/sites/andygreenberg/2013/12/06/new-silk-road-drug-market-backed-up-to-500-locations-in-17-countries-to-resist-another-takedown/*, accessed on June 1, 2015.

64. Leger.

65. Andy Greenberg, "Silk Road Creator Ross Ulbricht Sentenced to Life in Prison," Wired, May 29, 2015, available from

wired.com/2015/05/silk-road-creator-ross-ulbricht-sentenced-life-prison/, accessed on June 1, 2015.

66. Evan Perez, "2 Former federal agents charged with stealing Bitcoin during Silk Road Probe," CNN, March 30, 2015, available from *cnn.com/2015/03/30/politics/federal-agents-charged-with-stealing-bitcoin/*, accessed on April 21, 2015. See also Brian Fung, "DOJ: These federal officials stole bitcoins from Silk Road while investigating Silk Road," *The Washington Post*, March 30, 2015, available from *washingtonpost.com/blogs/the-switch/wp/2015/03/30/doj-these-federal-officials-stole-bitcoins-from-silk-road-while-investigating-silk-road/*, accessed on April 21, 2015.

67. Greenberg, "New Silk Road Drug Market Backed Up To '500 Locations In 17 Countries' To Resist Another Takedown."

68. Chris Isidore, "Target: Hacking Hit Up to 110 Million Customers," CNN (Money Section), January 11, 2014, available from *money.cnn.com/2014/01/10/news/companies/target-hacking/*, accessed on May 30, 2015.

69. Point-of-sale malware scans the memory of point-of-sale terminals for stored Track 1 and Track 2 data associated with credit cards and debit cards. The compromised data is stored in a text file and then exfiltrated to FTP servers abroad.

70. Mathew J. Schwartz, "Target Breach: 8 Facts On Memory-Scraping Malware," *Information Week,* January 14, 2014, available from *darkreading.com/attacks-and-breaches/target-breach-8-facts-on-memory-scraping-malware/d/d-id/1113440*, accessed on May 30, 2015.

71. *Ibid*.

72. Brian Krebs, "Target Hackers Broke in Via HVAC Company," KrebsonSecurity Blog, February 5, 2014, available from *krebsonsecurity.com/2014/02/target-hackers-broke-in-via-hvac-company/*, accessed on May 30, 2015.

73. Sue Marquette Poremba, "Beware of the Plumber? Third-Party Contractors Pose Business Security Risk," *Business News Daily,* February 26, 2014, available from *businessnewsdaily.com/5986*

-does-your-business-employ-contractors-how-to-mitigate-risk.html, accessed on May 30, 2015.

74. United States Senate Committee on Commerce, Science, and Transportation, "A 'Kill Chain' Analysis of the 2013 Target Data Breach," Majority staff report for Chairman Rockefeller, March 26, 2014.

75. Krebs, "Target Hackers Broke in Via HVAC Company."

76. Michael Riley, Benjamin Elgin, Dune Lawrence, and Carol Matlack, "Missed Alarms and 40 Million Stolen Credit Card Numbers: How Target Blew It," Bloomberg News, March 17, 2014, available from *bloomberg.com/bw/articles/2014-03-13/target-missed-alarms-in-epic-hack-of-credit-card-data*, accessed on May 30, 2015.

77. *Ibid*.

78. *Ibid*.

79. N. Eric Weiss and Rena S. Miller, "The Target and Other Financial Data Breaches: Frequently Asked Questions," CRS Report for Congress, February 4, 2015, p. 3.

80. Nicole Perlroth, "Reporting From the Web's Underbelly," *The New York Times,* February 16, 2014, available from *nytimes.com/2014/02/17/technology/reporting-from-the-webs-underbelly.html*, accessed on May 30, 2015.

81. *Ibid*.

82. Riley *et al.*

83. Joseph Menn, *Fatal System Error: The Hunt for the New Crime Lords Who Are Bringing Down the Internet,* New York: Public Affairs, 2010, p. x.

84. Scott Berinato, "How a Bookmaker and a Whiz Kid Took On a DDOS-based Online Extortion Attack," CSO.com, May 1, 2005, available from *csoonline.com/article/2118109/fraud-prevention/how-a-bookmaker-and-a-whiz-kid-took-on-a-ddos-based-online-extortion-attack.html*, accessed on June 22, 2015.

85. *Ibid*.

86. *Ibid*.

87. A detailed, blow by blow account of the DDoS attack can be found in the first chapter of Menn's book *Fatal System Error* cited previously, in the article by Scott Berinato cited above, and the article by Evan Ratliff cited below. The investigative aftermath is also chronicled extensively by Joseph Menn in his book. All of these provide the main sources for the case study.

88. Berinato.

89. Evan Ratliff, "The Zombie Hunters: On the Trail of Cyberextortionists," *The New Yorker*, October 10, 2005, available from *newyorker.com/magazine/2005/10/10/the-zombie-hunters*, accessed on June 4, 2015.

90. *Ibid*.

91. Berinato.

92. *Ibid*.

93. *Ibid*.

94. *Ibid*.

95. *Ibid*.

96. *Ibid*.

97. *Ibid*.

98. *Ibid*.

99. *Ibid*.

100. *Ibid*.

101. *Ibid*.

102. Ratliff.

103. Berinato.

104. *Ibid*.

105. *Ibid*.

106. *Ibid*.

107. *Ibid*.

108. *Ibid*.

109. Berinato; and Menn, p. 25.

110. Berinato.

111. *Ibid*.

112. Berinato; and Ratliff.

113. Berinato; Menn, p. 35; and Ratliff.

114. Berinato; and Ratliff.

115. Menn, pp. 136, 141-144, 192.

116. "Eight Years for Extorting Millions," *Kommersant*, October 4, 2006, available from *kommersant.com/page.asp?id =709912*, accessed on June 23, 2015; Menn, p. 150.

117. *Ibid*.

118. Berinato.

119. *Ibid*.

CHAPTER 10

DIGITALLY ARMED AND DANGEROUS: HUMANITARIAN INTERVENTION IN THE WIRED WORLD

Ronald J. Deibert
John Scott-Railton

Ronald Deibert wishes to express his gratitude to Matthew Carrieri and Saad Khan for research assistance; and David Croft and Jeannie Phillips for helpful suggestions.

INTRODUCTION

Cyberspace has become the central nervous system for the planet—the Internet, cell phones, and social media permeate everything we do and constitute a new and highly dynamic ecosystem. As individuals adopt and use these new technologies, they emit a massive amount of data that leave behind a kind of "digital exhaust" that now exists on a separate ethereal plane, fed into by a continuously expanding number of data sources. That data includes that which we communicate intentionally, like the content of blog posts, emails, and tweets. However, they also include digital trails that most users either do not perceive or are unaware of—metadata—that is largely a byproduct of communications, and which dwarfs the actual content of that which is communicated. Moreover, individuals now connect to each other in dense and rich networks of unmediated bilateral and multilateral communications, much of which is open and broadcast globally over networks.

Although the digital divide runs deep, cyberspace is an ecosystem that does not discriminate as it is increasingly adopted by society's rich and poor, outstripping even the development of good governance over it. As liberal industrialized countries reach a saturation point, connectivity in the global south has become the focus and is occurring extraordinarily quickly. In these regions, development is different in character than that which occurred in the industrialized core, as infrastructure in the global South leapfrogs over older technologies. Mobile connectivity, for example, dominates the cyberspace of the global South. According to the International Telecommunications Union, mobile-cellular penetration rates measure 89 percent in developing countries as of 2013, while the number of mobile-broadband subscriptions in the developing world more than doubled (from 472 million to 1.16 billion) between 2011-13. By contrast, household Internet penetration rates average only 28 percent in developing countries, totaling 373 million households.[1]

Social media outlets penetrate all aspects of life; this is no less true when it comes to zones of armed conflict and violence. According to Sweden's Uppsala University, Department of Peace and Conflict Research, armed conflict is defined as:

> contested incompatibility that concerns governments and/or territory where the use of armed force between two parties, of which at least one is the government of a state, results in at least 25 battle-related deaths in one calendar year.[2]

They contrast armed conflict to "nonstate conflict," in which "none of the warring parties" is a government. Over the last several decades, scholars of armed conflict have noted a secular trend whereby the number of

traditional state-to-state armed conflicts has declined, replaced by long-festering nonstate conflicts that simmer for years seemingly without end and blur into a state of barely concealed omnipresent violence.[3] Not surprisingly, many of these types of long-festering conflicts occur in the most impoverished regions of the world—sub-Saharan Africa, South Asia, the Middle East and North Africa, and Central Asia. According to the World Bank's April 2011 report, insecurity:

> has become a primary development challenge of our time. One-and-a-half billion people live in areas affected by fragility, conflict, or large-scale, organized criminal violence, and no low-income fragile or conflict-affected country has yet achieved a single United Nations Millennium Development Goal.[4]

Conventional wisdom has long assumed these "black holes" are the least hospitable to new information and communication technologies. Bright, shiny mobile phones, cloud computing systems, and Twitter and Facebook accounts are all strongly associated with high-tech centers of entrepreneurialism, like Silicon Valley. However, zones of conflict—even in the most impoverished parts of the world—are deeply saturated with new information and communication technologies. Moreover, because of the absence of government capacity in some of those regions, innovation of digital technology use can vary substantially. It is remarkable that there exists little dedicated research on the uses of digital technologies in zones of conflict. Since most of the armed conflict today takes place in the global South, an analyst from the industrialized North might falsely assume that digital technology plays little role—that these cases of organized violence are more primordially than technologically

driven. However, this would be a mistaken assumption. Satellites, drones, mobile phones and other sensors of various kinds are now omnipresent features of the battlefield, transforming not only armed conflict but also peace building and humanitarian operations.

Conflict countries *Note: Countries in bold are listed as conflict zones where 1000+ individuals have died per year*	**Percentage of Individuals Using the Internet as of 2012**	**Mobile-cellular telephone subscription growth rate and average annual growth rate, from 2005-2012**
Colombia	48.98	508.34/71.62
Afghanistan	5.42	1,400.00/200.00
Somalia	1.38	31.60/4.51
Yemen	17.45	510.30/72.90
Pakistan	9.96	840.80/120.11
Mexico	38.42	113.85/16.26
South Sudan	n/a	n/a
Sudan	21	1,413.10/201.87
Iraq	7.1	1,645.34/235.05
Egypt	44.07	610.21/87.17
Syria	24.3	338.24/48.32
Iran	26	583.36/83.34
Philippines	36.24	196.16/28.02
North Korea (Data only available from 2009-2012)	n/a	2,354.48/336.35
South Korea	84.1	39.85/5.69
India	12.58	859.31/122.76
Israel	73.37	18.92/2.70
Palestine	n/a	435.78/62.25
Myanmar	1.07	4,126.88/589.55
Indonesia	15.36	501.07/71.58
Morocco	55	214.83/30.69
Algeria	15.23	175.90/25.13
Mauritania	5.37	439.65/62.81

Table 10-1: Ongoing Conflicts, Internet Penetration, and Mobile Phone Growth Rates.[5]

Conflict countries *Note: Countries in bold are listed as conflict zones where 1000+ individuals have died per year*	**Percentage of Individuals Using the Internet as of 2012**	**Mobile-cellular telephone subscription growth rate and average annual growth rate, from 2005-2012**
Western Sahara	n/a	n/a
Peru	38.2	426.35/60.91
The Gambia	12.45	516.70/73.81
Senegal	19.2	563/80.43
Turkey	45.13	55.20/7.86
Uganda	14.69	1,143.55/163.36
Democratic Republic of Congo	1.68	609.63/87.09
Central African Republic	3	970.22/138.60
China	42.3	179.61/25.66
Angola	16.94	508.34/72.62
Nigeria	32.88	506.76/72.39
Mali	2.17	1,817.73/259.68
Tunisia	41.44	120.05/17.15
Niger	1.41	1,566.05/223.72
Thailand	26.5	176.02/25.15
Russia	53.27	118.24/16.89
Bahrain	88	176.87/25.27
Lebanon	61.25	302.59/43.23
Libya	19.86	379.35/54.19
Guinea	1.49	2,429.63/347.09

Table 10-1: Ongoing Conflicts, Internet Penetration, and Mobile Phone Growth Rates.[5] (Cont.)

If it is not already so, collecting, interrogating, and analyzing all of this data will soon be a dedicated activity undertaken by multiple participants to any armed conflict in every region of the world. The combatants themselves leverage this data in different contexts, such as when insurgents use cellphones to organize, issue threats, directly trigger improvised explosive devices, or when counterinsurgency forces employ surveillance to engage in highly sophisticated acts of targeted killing. At the same time, humanitar-

ian groups, aid organizations, and conflict prevention and peacebuilding bodies use tools and data sources such as Ushahidi and other crowd-sourced maps to anticipate, predict, and respond to crises and organized violence. Even war studies scholars and other analysts use digital technologies to better understand the nature of conflict and crises today. As Micah Zenko puts it:

> As conflict unfolds today, the stream of images and videos from participants allow us to see what kinds of weapons are being used, how well-trained local forces are, evaluate morale, and examine conditions on the ground hour by hour. These images, movies, and words offer us something akin to Google's "Street View" on a real-time basis from nearly anywhere in the world to assess and manage conflict and its precursors in ways never before possible.[6]

Among those who do recognize the growing role of digital technologies in armed conflict, the reactions have generated considerable interest and enthusiasm about their potential to boost conflict prevention and humanitarianism. David Kilcullen and Alexa Courtney's views are representative in this respect:

> The ability to manipulate big data, visualize dynamics, and recognize patterns and signatures for conflict creates new opportunities for humanitarian and development assistance in the most complex and dangerous environments.[7]

Within the last few years, a growing number of projects, analytical tools and applications, conferences, Technology, Entertainment and Design (TED) talks, and journal articles have trumpeted the potential for what is now a burgeoning new interdisciplinary field: digital humanitarianism.

While excitement runs deep around the prospects for digital technologies to advance peacebuilding and humanitarianism, little explicit attention has been given to the role of technology in doing the opposite: facilitating violence and/or exacerbating the risks that aid workers, conflict monitors, and locally affected populations face. The argument we make in this chapter is that, while digital technologies, crowd mapping, and other new ways of exploiting information and communications technologies (ICTs) for benign ends do provide new opportunities, the risks to digital humanitarianism are growing. Armed protagonists are increasingly becoming more adept at exploiting these technologies for malignant ends. Indeed, going further, the headlong rush to adopt social media and other new tools without the proper understanding of these risks may end up doing more harm than good.

DIGITAL HUMANITARIANISM AND ARMED CONFLICT

Over the last several years as new digital technologies have exploded, their use in zones of conflict, disasters, crises, and other contentious situations has become more pronounced. Today, although the digital divide remains significant, crises and conflicts of all sorts take place in highly connected environments. Everyone can now participate in and use mobile phones, layered information, open street maps, crisis mappers, and other open source tools. At the same time, participants in crisis and conflict situations can use short message service (SMS) and social media platforms to communicate with one another or signal for help. Alongside these highly connected environments, aid, conflict prevention, crisis management,

and humanitarian organizations have begun to adopt increasingly sophisticated uses of these technologies to assist in, and even fundamentally transform their missions—now increasingly known as the field of "digital humanitarianism." As Patrick Meier notes:

> ICTs are changing the ways in which information is collected and processed; they are bringing new volunteer networks to the fore of humanitarian response; and, as a result, they are spurring organizational change within established humanitarian organizations.[8]

The following section provides a very brief overview of some important milestones in the evolution of digital humanitarianism, describes some of the key methods and technologies, and suggests a trajectory of where the field is headed.[9]

2010 Haiti Earthquake and Beyond.

The field of digital humanitarianism has its roots in many events and cases. Among the most important are the introduction of Google Maps and Google Earth in 2004; the Ushahidi open source platform, first developed around the 2007 Kenya elections to monitor human rights violations occurring in post-election violence; and the launch of Harvard Humanitarian Initiative's Crisis Mapping and Early Warning project in 2007. An essential turning point was the 2010 Haiti Earthquake Disaster. The Haiti disaster is widely recognized as a milestone in the use of crowd generated digital data to assist in humanitarian and relief operations. While not an armed conflict per se, there were significant incidents of violence, crowd stress, and insecurity as a result of the pressures on human populations and migration.

Immediately upon the earthquake, aid workers, observers, and others realized that there were numerous "sensors" that could provide insights into communities at risk, the movement of people, and how to target relief more efficiently to populations in need. Within hours, a live crisis map of Haiti was launched using the Ushahidi platform, organized primarily by volunteers at Tufts University in the United States. Information was gathered and collated from social media (e.g., Twitter and Facebook) to identify reports of trapped persons, medical emergencies, and specific needs for water, shelter, and other necessities. A number to which affected populations could send SMS messages was widely circulated (4,636) and used to send urgent life and death pleas for help. The U.S. Marine Corps and other intervening international organizations referenced the crisis maps to determine when and where to direct resources. An OpenStreetMap (OSM) was created for Haiti, exploiting high-resolution satellite imagery and allowing OSM workers to identify roads and better plot the locations of urgent messages for help. Likewise, expectations grew among the affected populations that social media would be a way to connect and send pleas for help. Entrepreneurs offering mobile phone charging stations sprung up in response. Although some organizations took advantage of the map, others were more reluctant and confused by how to process it, and some raised questions about the reliability of crowd-sourced information. (See Figure 10-1.)

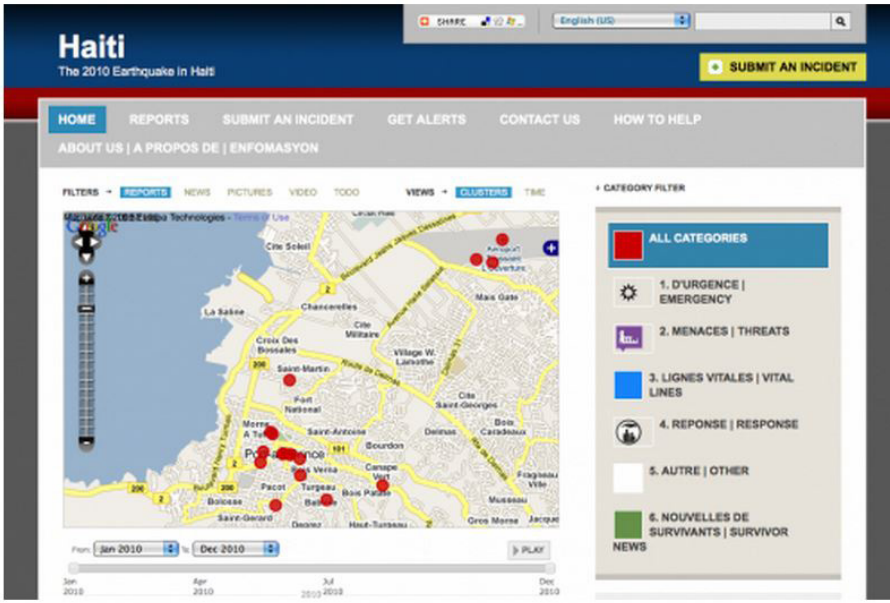


Figure 10-1. An Example of Ushahidi's Haitian Earthquake Crisis Map.[10]

In the aftermath of the disaster, the humanitarian community as a whole took notice. The United Nations Office for the Coordination of Humanitarian Affairs (UNOCHA) launched several studies and conferences, one of the results of which was the creation of the Standby Volunteer Task Force (SBTF), which has grown to more than 800 volunteers in 80 countries. Subsequently, similar crowd mapping and digital humanitarian efforts were launched around disasters, conflicts, and complex emergencies.

For example, in response to ravaging fires in the summer of 2010 in Russia, a group of Russian blogs inspired by the Haiti experience launched a live crisis map.[11] The Russians turned the map into a platform for both needs and offers of help. The offers of

help were overwhelming, with more than 600 reports mapped during the first week alone. A coordination and call center service was set up—in effect a citizen-based disaster response agency that served as a kind of "mutual aid" in the absence of Russian state capacity. These community-based, self-organized crisis maps contrasted with the information that was provided by the Russian government, which tried to shape, censor, and control as much information being released as possible about the disaster. (See Figure 10-2.)

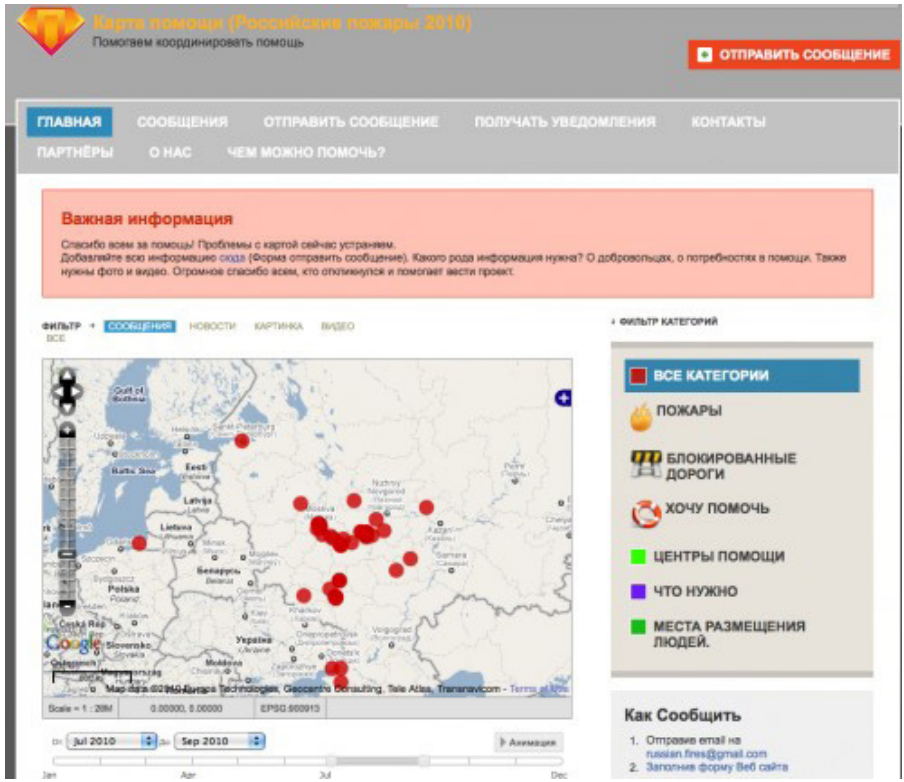


Figure 10-2. A screenshot of the "Russian Fires Crisis Map."[12]

Social media, crowdsourcing, and mapping were also used extensively in and around the Libyan civil war. Within hours of the conflict's onset, a live crisis map powered by the Ushahidi platform was launched.[13] Media monitoring, geolocation reports, and verification and analysis teams were organized to analyze and upload data. Other organizations, such as the International Organization for Migration, set up other crisis maps, which were in turn used by UNOCHA. Steps to secure the map were taken in light of its use in the context of an armed conflict. Concerns were raised for the first time about risks to information contributors whom the government might see as "informants" or "traitors." The Libya Crisis map was password protected and open only to established humanitarian organizations. Digital security issues surrounding the Libyan conflict will be described in more detail below.

The Japanese Tsunami was another major milestone in digital humanitarianism. According to Crisis Communication Management, there were more than 5,500 tweets per second about the disaster.[14] A Japan crowd map was instantly created, and over 3,000 people uploaded geo-located data to the map. Videos taken on cell phones were sent to news agencies and analyzed while information on nuclear radiation counts was collected by individuals with Geiger counters and uploaded to the RDTN.org website.

Incidents like these have brought about pressures on humanitarian agencies to exploit new social media. Traditional nongovernmental organizations and humanitarian institutions increasingly have been criticized for failing to take advantage of the opportunities that digital technologies present, and expectations have grown about the power that social media and

other digital tools represent. In March 2012, a Reuters news article titled "Will Twitter Put the U.N. out of the disaster business?" argued, "Many agencies have muddled along for decades with scarcely a nod toward communicating with the folks they're supposed to be representing."[15] The piece outlined how "many aid agencies don't have the time or resources to take all of this on, simply because it is not 'mainstreamed' into their activities."[16]

These pressures are not just based on outside observations and new technical opportunities, but on the impressions and expectations generated by the digitally equipped populations themselves who are often the victims. A 2010 American Red Cross survey found an alarming 75 percent of 1,058 respondents expected help to arrive within an hour if they posted a request on a social media site (American Red Cross, 2010).[17]

Alongside the growing criticisms, numerous conferences have brought together thought leaders and innovators who have explored case studies, discussed new projects, and developed new tools and web platforms.[18] These have led to recommendations that organizations should adopt social media as part of the digital humanitarian toolkit. For example, a report written by BBC World Service Trust called "Left in the Dark"(and a follow-up BBC analysis to that report) argued that information is a form of aid, and needs to be incorporated into the organization of traditional humanitarian operations in a much more comprehensive fashion.[19]

While the internal and external pressures on humanitarian and other organizations to adopt digital technologies have been escalating, the actual tools to engage in big data analysis have been growing in leaps and bounds, attracting venture capitalists and

the attention of large organizations and companies. Big data analysis has become a huge growth sector in the government and private sector, resulting in a wide variety of new tools under development for disaster, humanitarian aid relief, awareness of gender-based violence, and other uses. As acquiring data becomes increasingly feasible, new tools using big data analytics are bringing new opportunities for improving information sharing and transparency for organizations like the U.S. Agency for International Development and the World Bank. For example, users can call up the Data Visualizer, which tracks civil war, homicides, and terrorism, and collates them with socioeconomic, demographic, and political data to put it into context.[20]

One interesting dimension sometimes acknowledged as awkward for humanitarians, is that some of the most successful big data analytics innovations are coming from the defense, law enforcement, and intelligence sectors; what have been called elsewhere the cyber-military-industrial complex.[21] Does it matter that the tools that are being used by humanitarians have as their primary development impetus the needs of the very agencies that are sometimes the greatest contributors to armed violence? For example, the company Palantir has developed a very popular data analytics platform that is often touted as a potentially useful resource for humanitarian operations. Yet at the same time, the tool's primary mission is as a multidiscipline U.S. defense and intelligence agency data aggregator, sometimes providing valuable analytic insights that enhance lethal operations against identified threats.[22] This type of debate echoes ones that were held in the 1990s about the utility of employing military technologies and expertise for environment rescue operations.[23] In light of the recent National

Security Agency (NSA)/Snowden revelations and the scope of NSA organized surveillance, digital humanitarians may also be rightly concerned about the possible compromises of the data analytical platforms and tools that are adopted by them—a concern that warrants further encouragement of open source platforms. Can digital humanitarians, operating in zones of conflict, be confident that information collected through their platforms is not shared with agencies that might use that information to engage in acts of violence? Further concerns along these lines will be explored later in this chapter.

Stepping back and taking a broader view, we can see an evolution in the nature of early conflict warning, rapid response, disaster relief, and humanitarian operations, which are themselves part of a spectrum. Patrick Meier is probably the most widely recognized proponent of digital humanitarianism. He has described this evolution in terms of four generations of early warning and response—but in terms that apply to digital humanitarianism as well (see Table 10-2 below).[24] The first generation "monitors and analyzes conflict from outside the conflict regions . . . and are typically based in the West." Second-generation early warning systems "conduct monitoring within conflict countries and regions. However, analysis is still conducted outside conflict countries (in the West)." Third generation early warning systems "are created by people in conflict areas for themselves" and represent a fundamental turning point in the exploitation of digital media. Fourth generation early warning systems accelerate and amplify the third generation's tendency toward localization by featuring no predesignated field monitors, a reliance on the masses, and a drawing upon crowdsourcing and freely available

tools.[25] There is a clearly "people centered" and "social-media centered" focus of fourth generation early warning systems that defines today's digital humanitarian operation.

Generation	Location	Objective	Technology
1st Generation Since 1990s	Headquarters	Conflict detection	• Expensive, proprietary technology
2nd Generation Since 2000	Headquarters with stronger links to networks in the field	Conflict detection with limited response (mainly recommendations)	• GIS and satellites • Internet (email and websites)
3rd Generation Since 2003	Conflict areas with local networks included in the system	Conflict detection with stronger links to response mechanisms; monitors often serve as "first responders"	• Proprietary software with structures reporting and coding protocols • Mobile phones
4th Generation Since 2008	Conflict areas with less centralized organizational frameworks	Decentralized two-way information service for collection and dissemination	• GIS and open-source satellite imaging • Free and/or open source technologies, especially mobile phones

Table 10-2: Four Generations of Early Warning and Response.[26]

Although the field itself is fast moving, at the time of this writing, its cutting edge is about applying more fine-grained and immediate responses to affected populations in a highly interactive fashion in as near real-time as possible over social media. For example, a new project developed by Meier's Qatar Computing Research Institute hopes to provide financial assistance to affected populations over Twitter.[27] The project also talks about developing artificial intelligence programs to directly identify and locate needs as they spring up from Twitter. Likewise, Kilcullen and Courtney advocate a paradigm shift in "Design-

ing for Development," which combines several elements, including: integration of quantitative data, remote observation and analysis, use of new tools such as big data, crowd-sourced reporting, and interactive visualization with deep contextual understanding accomplished through on-the-ground observation and research. This integration should be "preferably carried out and directed by well-trained members of the local community."[28]

Naturally, this evolution and these pressures create an almost insatiable desire for more information and an enthusiasm for new technologies that can end with counterproductive results. For example, in an article entitled "How Emergency Managers Can Benefit from Big Data," the author advocates for less privacy around personal online data for emergency purposes. The author cites Carnegie Mellon University professor Ole Mengshoel's argument that it "would be a pity if big data's potential based off social media data streams wasn't reached because the companies were too protective of it."[29] Although he acknowledges inherent privacy concerns, he maintains that emergency specialists should have access to social media data in order to harness its full potential.

While there are security concerns and criticisms raised within the digital humanitarian community, they focus almost entirely on inefficiencies, lack of training, unwillingness to adopt, and a lack of capacity to learn. While those are all important, an entirely different set of concerns arises due to security issues. In one of the rare exceptions, George Chamales and Rob Baker argue in their piece, "Securing Crisis Maps in Conflict Zones," that deploying digital technologies in crisis zones "can be exploited by hostile actors who have developed and adopted network surveillance and attack capabilities."[30] Likewise, a recent UNOCHA

report on humanitarianism in the networked world briefly raised some concerns about security risks, noting that the Islamist group Boko Haram destroyed 24 mobile phone towers in Northern Nigeria in 2012 and that reports have surfaced of Syrian opposition groups having their computers targeted with malicious software.[31] The following section further explores the broader context behind some of those risks, including details from Citizen Lab research that underpin the UNOCHA reference to the Syrian conflict.

UNFORESEEN VULNERABILITIES IN ZONES OF CONFLICT

It is still widely assumed that digital technologies are the "dictator's dilemma"—an unavoidable part of the global economy, but one that brings about an inevitable flood of information that overwhelms authoritarian regimes. Authoritarian regimes were once widely considered too slow, cumbersome, and heavy-handed to deal with the Internet, but a growing body of research has shown that these assumptions require serious reexamination. Far from withering in the face of digital technologies, authoritarian and autocratic regimes are proving not only to be more robust than many anticipated, but also are actively acquiring censorship, surveillance, and computer network attack products, services, and capabilities in order to give themselves a distinct technical advantage. Indeed, all actors to armed conflict today increasingly are better equipped and more savvy about how to exploit big data for nefarious ends. As digital humanitarianism evolves, there are reasons to believe their operations will involve additional risks related to these capabilities.

In one of the few studies to address the issue directly, "Securing Crisis Maps in Conflict Zones," Chamales and Baker identify five types[32] of vulnerabilities associated with "crowdmapping," summarized as:

- **Identification of Reporters and Vulnerable Groups:** Information collected and uploaded by citizens and aid workers can be traced and then used to identify those individuals doing the reporting, as well as other vulnerable groups. Chamales and Baker mention the Taliban's threats to foreign aid workers responding to the 2010 floods in Pakistan as an example.
- **Control of Communication Networks:** Oppressive governments can use their control over the "high ground" of the communications infrastructure to selectively disable information systems at critical times. The OpenNet Initiative (a project in which the Citizen Lab participated from 2002-2013) refers to these types of selective disabling as "just-in-time" information controls. These controls have been documented in Egypt's Internet "blackout" during anti-Mubarak protests in 2011,[33] Burma in 2007 after protests in Rangoon,[34] and China's Xinjiang province after ethnic riots in 2009, among others.[35]
- **Programming Flaws in Crisis Mapping Platforms:** The very technologies used by the organizations may contain vulnerabilities that are exploited by adversaries, thereby putting people at risk. These platforms, in other words, may have improper or inadequate security vetting. These flaws will be elaborated upon further below with respect to the Libya and Syria cases.

- **Identification and Infiltration of the Crowdsource Workforce:** Hostile groups could pose as helpful workers allowing them to access internal information and sensitive systems.
- **Use of Unverified Reports:** The use of false reports, or unverified reports, can be a deliberate information operation strategy designed to confuse or spread misinformation.

While Chamales and Baker mostly outline hypothetical concerns, recent Citizen Lab research adds a wealth of empirical detail to these concerns.

With respect to the identification of vulnerable groups and exploitation of programming flaws in social media and other platforms, our research has documented a growing market for commercial surveillance and computer network exploitation products and services used in the context of a number of countries of concern. For example, in the reports *Behind Blue Coat*, *Planet Blue Coat*, and *Some Devices Wander by Mistake*, the Citizen Lab used a combination of technical forensics and wide-area scanning methods to map the worldwide locations of ProxySG and PacketShaper appliances, two devices manufactured by Blue Coat Systems Inc. based in Sunnyvale, California.[36] These devices can be used to secure and maintain networks, but also to implement politically motivated restrictions on access to information, and/or to monitor private communications. The ProxySG device even advertises the ability to intercept encrypted communications that use secure sockets layers, effectively identifying and then breaking into secure information flows. Our findings show Blue Coat devices on the public networks of 83 countries, including those with poor human rights records (such as Bahrain, China, and the United Arab Emirates) and those that are subject to U.S. sanctions

(including Iran, Syria, and Sudan). A few of the countries found to have Blue Coat on public networks are also in the midst of ongoing armed conflict.[37] These countries include Syria, Cote D'Ivoire, and Sudan, three countries listed as countries of special concern in Citizen Lab research due to extensive insecurity, pervasive human rights violations, and/or being in an ongoing or having recently emerged from a conflict situation.[38] (The map in Figure 10-3 details countries in which Blue Coat was found to be present.)

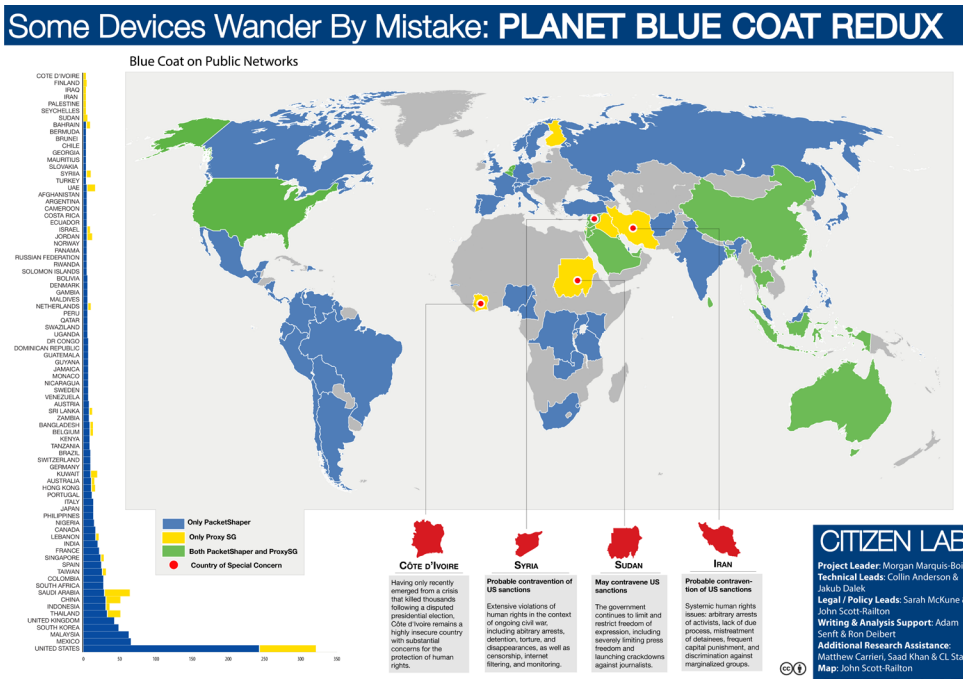


Figure 10-3. Map of Blue Coat Presence Worldwide.[39]

Sudan, in particular, is an interesting case of how social media can empower repressive practices as much as it can aid activists in organizing and spread-

ing information outside of state-controlled channels, especially with reference to the country's anti-government protest movement. In 2012, protests in response to growing austerity measures by the government had been curtailed, with journalists and bloggers deported, and news sites censored.[40] Meier cites an example where the Sudanese government reportedly set up a fake Facebook page calling for protests at a given time and location. Arrests were subsequently made, with many protesters reportedly tortured to further reveal their Facebook login credentials.[41] Pro-government Internet users have even compromised protest sites as a means of spreading disinformation, and to "triangulate the identities of the chief organizers" of the anti-government movement.[42] The success of the online anti-protest campaign by the regime and its supporters has led many protesters to abandon Facebook as a vehicle for organization in favor of face-to-face contact.[43] Since 2010, the Satellite Sentinel Project has mapped mass atrocities in both Northern and Southern Sudan through satellite imagery and analysis.[44] While defending their methodology, members of the project have been open about the need for ethical questions to be explored regarding their approach, including questions regarding the risks to civilians if data-mapping is wrong, or concerns regarding the hacking of sensitive data.[45] Various tips for activists on the ground have been developed to mitigate potential threats, including warnings against oversharing sensitive, personal information on Facebook and Twitter, especially on public groups.[46] That the regime now has access to an advanced deep-packet inspection tool manufactured by Blue Coat Systems should raise serious alarm bells.

Other Citizen Lab research reports have provided evidence of FinFisher remote intrusion and surveillance software targeting activists in several countries

where conflict has been occurring, including Pakistan, Turkey, Nigeria, India, and Ethiopia.[47] Developed by Munich-based Gamma International GmbH, FinFisher products are marketed and sold exclusively to law enforcement and intelligence agencies by the UK-based Gamma Group. We have also documented the global proliferation of FinFisher by finding command-and-control servers in 36 countries and analyzed variants of the FinFisher suite that target mobile phone operating systems. (See Figure 10-4 for a map of FinFisher's global proliferation.)

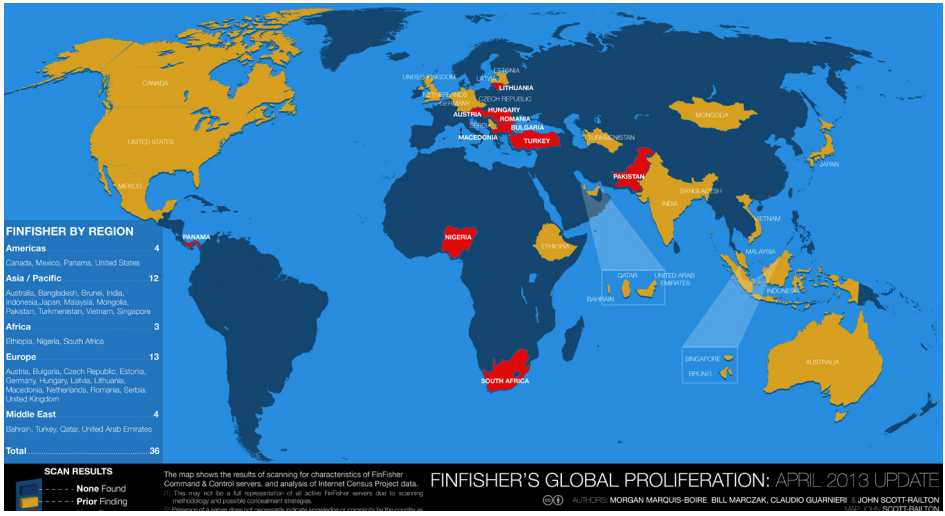


Figure 10-4. Map of FinFisher Presence Worldwide.[48]

Our research has only picked at the surface of a growing market. FinFisher remote intrusion and surveillance software, and others like it, typically use hyperlink and URL sharing—as well as other common channels of social media information exchange—as

vectors of exploitation, any one of which could be easily targeted toward digital humanitarian operations based either inside or outside of countries of concern. FinFisher brochures included in the SpyFiles advertise capabilities that include silent logging of keystrokes, screenshots of desktops, covert capture of audio and video, interception of Skype and other chat, as well as voice over Internet protocol (VOIP) tools, and extraction of all files from infected hard drives. Since the FinFisher tool also advertises itself as being largely untraceable by most known anti-virus products, it is possible many digital humanitarians (among others) could be infected without knowing it. Those capabilities in the hands of regimes or other protagonists could mean access to sensitive data not meant for public circulation, including the location of opposition groups.

Chamales and Baker's concerns are also supported by closer examination of two recent conflicts: the Libyan and Syrian Civil Wars. Citizen Lab research fellow John Scott-Railton has been undertaking detailed investigations of the information components of each conflict, which are summarized below.

Case study 1: Libya.[49]

The 2011 Libyan Civil War was marked by the use of ICT not only by digital humanitarians but also by members of the opposition and the Libyan government. From the days of the Egyptian uprising, the Muammar Gadhafi regime made efforts to limit the online information environment. The regime arrested a handful of activists who used the Internet, possibly in response to calls for a protest on February 17. The regime also took other actions to control the informa-

tion environment, including blocking Al Jazeera from regime-owned networks, jamming satellites, and barring foreign journalists from entering the country.[50] On February 13, 2011, the Internet was briefly shut down, followed by a longer lasting shutdown that was accompanied by wireless and landline shutdowns on March 3, 2011. Renesys—an Internet traffic monitoring firm—saw that not all traffic was blocked, indicating that the regime was likely still using the Internet in what the company described as a "warm standby."[51] The probable nature of leaving remaining Internet traffic open was made clearer by the emergence of the "Libyan Electronic Army", a pro-government electronic actor, whose electronic attacks against adversaries of the Gadhafi regime were undertaken with Internet protocol (IP) addresses originating from within Libya.

Protesters, citizen journalists, and anti-regime fighters used ICT technologies early on to spread information and coordinate attacks, an effort that spanned participants from within and outside of Libya. Although the Internet shut down severely affected these groups, they also quickly deployed a wide range of decentralized solutions to reestablish connectivity that routed around regime-controlled networks. Forms of communication used by the opposition varied. Some anti-regime fighters used colored flags as a means of communications. Others used very small aperture terminals (VSATs), broadband global area networks, radio, and satellite phones. Free Internet services (Facebook, Twitter, and YouTube) played an important role in getting information out of the country.

When Internet access was restored, blogs and websites were used to document the war. Before international correspondents were allowed into the coun-

try, citizen journalists took to the frontlines of war to document it. These reports were often uploaded on social media sites like YouTube and Facebook via VSAT terminals. Facebook was used in the early days of the war to call for protests from individuals as well as real-life and electronic groups. The official "Day of Rage" Facebook page called for the initial protests on February 17, 2011, and a plethora of Facebook pages sprung up supporting uprisings. The number of Facebook users in Libya increased dramatically, with a 588.86 percent increase in penetration from June 2011 to December 2011.

Similarly, the opposition used Twitter since the beginning of the conflict, with some feeds more objective than others. Aside from information, Twitter was also used to transmit satellite details and medical info, and even to communicate with North Atlantic Treaty Organization (NATO) forces. Common hashtags included #feb17, #Libya, and #Tripoli. Mainstream media began to pay attention to Twitter feeds as the conflict moved forward, using the platform as a means of breaking news, directing followers to stories, and reporting on events as "being reported on Twitter" before they were even confirmed or denied. Some used it to curate coverage of events, and some to exchange contacts and contact other users.

The most-followed Twitter account was that of the Libyan Youth Movement, which tweeted about NATO strikes and other NATO actions. Twitter reporting on NATO activities gave rise to questions of operational risks, such as the reporting of NATO forces' aircraft movement in real time. It was unclear, however, whether the Libyan government monitored the tweets for their own operational purposes. NATO also used post-strike damage assessments by Twitter users in their own briefings.

In many rebel-held territories, regionally based media committees sprung up as a means of spreading information through specific channels (for example, YouTube, Facebook, and Twitter). However, pro-government followers on social media would often flood the opposition-friendly pages, feeds, and videos with hostile comments. The aggressive posturing by pro-regime social media users backfired, however, and undermined the government's narrative characterizing the opposition as thugs.

The Internet played a role in supporting the opposition's communications strategy. Individual opposition members played the part of "nodes" that relayed information to the media, but also helped coordinate attacks (both NATO and opposition forces), thus serving as information clearinghouses for anti-government forces. NATO itself used Twitter for media messaging, as well as using open source Twitter information for planning and targeting attacks. NATO, however, made it a point to assure the public that social media was not the only source of information for its operations.

The opposition used Skype extensively. It connected Libyans with supporters in the Libyan diaspora and was often used as a substitute for cell and satellite phones, even when these forms of communication were more readily available. Opposition fighters also used Skype for organizational purposes and Facebook groups to share information, although it is difficult to determine their effectiveness due to the inherently closed nature of these groups. Email was not considered as useful as Facebook groups, nor as immediate as Skype, but was still used by the opposition to coordinate aid, and to communicate with foreign media and military, often either with personal accounts or pseudonyms.

With all the ingenuity used by the opposition to leverage these platforms, Libyan government authorities and their supporters were also adept at using technologies to target the opposition. Prior to 2011, some Libyans had already assumed that online communications were being monitored. While there had been little evidence of Internet filtering in Libya, there had been some evidence that authorities monitored Internet cafes actively. As the war wound down, however, evidence found in government centers revealed the existence of sophisticated network monitoring equipment. Specifically, Libyan government security forces were using Chinese ZTE and French Amesys equipment. The Amesys EAGLE system, a very advanced French network surveillance platform, cost 10 million euros to install and was fully functional by 2010. The system was installed in Libya as an "interesting laboratory" or test bed to try out the system with no limitations. Both the ZTE and Amesys monitoring systems are able to intercept email accessed by client software, VOIP calls, Web browsing, online emails, and chat programs. Photographic evidence of the ZTE's ZXMT system revealed that it could possibly store intercepted material, thus making it possible to subject material to historical link analysis and data mining. Opposition fighters also found that the regime used equipment capable of monitoring and tracking cellular phones, landlines, and Thuraya-brand satellite telephones. Technologies for interception and recording platforms included those provided by South Africa's VASTech and France's Thales.

As mentioned earlier, the government shut down of the Internet drove users to connect in ways that allowed users to bypass Libyan networks and the monitoring systems that were operating on the net-

works. VSAT services, for example, used Earth stations outside of Libya. The shutdown of landline and cellphone service also had the effect of neutralizing the regime's surveillance apparatus. Even in areas where phone networks remained active, the opposition moved their communications toward other decentralized forms. Unable to halt information communications, the Gaddafi regime responded by hacking users and websites in order to control the information environment. Pro-government forces, such as the Libyan Electronic Army (LEA) and mercenaries, targeted opposition groups through distributed denial of service (DDoS) attacks, malware, defacement, and hijacking accounts. They used inexpensive commercial malware designed for cybercrime, as well as simple hacking techniques. Employees of Libya Telecom and Technology reported that there was a room run by the Interior Ministry where hacking took place. These employees also described efforts to recruit hackers from overseas to perform phishing campaigns and develop malware to gain access to targeted computers.

It is possible the LEA is composed largely of volunteers. Apparently created at the urging of Gaddafi, the LEA had several locations in Tripoli, with volunteers and professional staff based both in Libya and overseas. The LEA used both simple and sophisticated attacks, from DDoS to code exploitation and malware attacks, to gain access to a target's computer. The various accounts of many individual Libyans were also compromised, sometimes through insecure passwords or weak account recovery questions, but also through malware attacks. One vector for the spread of malware was through hijacked accounts; once the LEA would takeover an account, it would then begin

sending contextually relevant messages to the users' contacts. A file transfer containing malware making reference to prior conversations would be sent and used to compromise the contact's accounts. The Libyan government also played audio of Skype calls on state television, claiming that they could intercept these calls as a means of fueling paranoia. Analysis of malware samples sent by LEA to opposition, targets showed that remote-access Trojans were often deployed. In one case study, Blackshades, which is available for purchase online, was used.

The Libyan Civil War showed the world how cyberspace has become a new realm for conflict and contention. As the opposition found novel uses to support their cause through digital technologies—from informing the world on the conflict outside of controlled channels to even actively supporting NATO attacks on government and military infrastructure—the government and its supporters also sought to use technological means of undermining opposition activists. The use of malware like Blackshades to compromise opposition technology and data speaks to the sophistication that pro-government actors cultivated in their efforts to fight their battles online. The use of familiar tools by the opposition—old Facebook and email accounts, for example, without the use of pseudonyms or cloaked identities—created vulnerabilities that made attacks and targeting by government authorities and pro-government forces relatively straightforward. Even mapping projects assisted by outside activists at the beginning of conflict proved to be rife with vulnerabilities. One such project for example, involving the mapping of cities where protests were occurring, raised concerns due to the irresponsible mapping of an attack by protestors against government mercenar-

ies.[52] Protecting protester identity and keeping information as vague as possible was one of many lessons learned from the exercise. While it is certainly true that technology was extremely useful to the opposition it is also true that "many of the tools used by the opposition, including social media, introduced substantial new risks, many of which weren't fully understood or mitigated during the conflict."[53] While the Gadhafi regime was ultimately toppled, digital humanitarians should not draw simple lessons from the widespread use of digital technologies as a contributing factor. Indeed, strong evidence suggests both they and key opposition groups, were significantly compromised by the regime before it fell.

Case Study 2: Syria.

After the Arab Spring, many believed the social media-enabled opposition would undermine authoritarian regimes. In August 2012, Scott Peterson of *The Christian Science Monitor* argued that the Syrian conflict was one defined by "endless images shot by mobile phone and volunteer videographers who know the importance of winning the media war," and that digital technologies would allow the rebels to gather support and circumvent restrictions on traditional media.[54] Similarly, *Time Magazine* published a feature on the U.S. State Department's training of Syrian rebels in digital security and use of information technologies on the battlefield, noting that such training has provided the opposition with tools necessary to defeat the Assad regime online.[55]

The Syrian civil war has also seen extensive use of crowdsourced mapping projects. Several Syrian activists based in the U.S. created the Syria Tracker Crisis

Map in 2011.[56] It relies on citizen reports and eyewitness accounts to map casualties and human rights violations, including chemical attacks. In another instance, the SBTF and Amnesty International USA's Science for Human Rights Program jointly launched a crowd map (see Figure 10-5) that relies on volunteers to analyze distributed satellite imagery for signs of military action, protest, and other civil unrest.[57] The Women's Media Center has also used crowdsourced maps to document instances of sexualized violence during the Syrian conflict.[58] Finally, Syria's Local Coordination Committees have documented the regime's violence against protesters, with blue dots showing active demonstrations, and red dots indicating violence.[59]

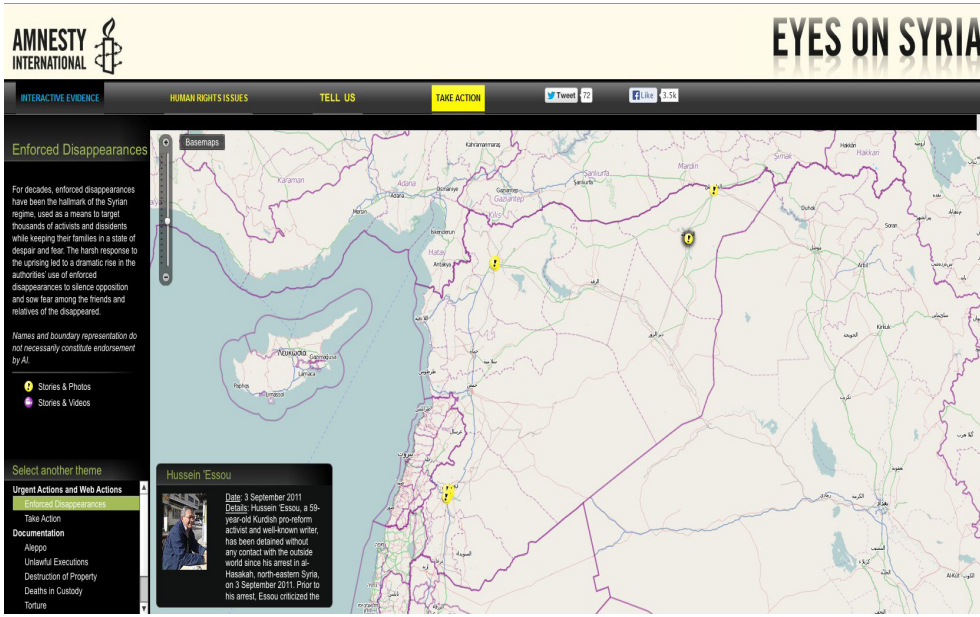


Figure 10-5. SBTF/Amnesty International "Eyes on Syria" Map.[60]

However, there have also been persistent and targeted electronic attacks against opposition and other groups connected to the Syrian conflict. The most widely known group in this respect is the Syrian Electronic Army (SEA), which is not an "army" in any conventional sense of the term, but rather a network of pro-government citizens that undertakes politically motivated attacks on website and social media accounts. While many of the SEA's seemingly random operations can be considered targets of opportunity, they have directed their efforts principally toward hacking two groups: local and foreign media sources that they consider unfriendly toward the Syrian government; and activists, dissidents, and rebels actively in opposition to the regime. In 2012 alone, the SEA gained access to and defaced the websites of Al Jazeera, Reuters, and Amnesty International, among others.[61] Since the start of 2013, there have been several major compromises of websites associated with Associated Press, Twitter, and *The New York Times*. In June 2011, Citizen Lab research found that the SEA had been using its Facebook page to call for sympathizers to download denial of service software and attack media targets considered hostile to the Syrian regime.[62]

Other types of targeted threats against Syrian activists have not been attributable directly to the SEA. Our research and that of the Electronic Frontier Foundation (EFF) has documented several instances of pro-Syrian government groups targeting Syrian activists and opposition with malware.[63] Typically, these attacks utilize a remote access tool (RAT) called Blackshades Remote Controller. If downloaded onto the victim's computer, RATs grant total control, allowing the attacker to take screenshots, log keystrokes, and

exfiltrate all kinds of data, including chat logs. Other incidents of malware targeting activists include the use of fake YouTube sites claiming to host opposition videos, fake Facebook pages used to phish login credentials of activists, fake "revolutionary documents" containing Trojan horses, and malware distributed via Skype.[64] Many others, from Telecomix to a range of security companies, have also contributed to research on Syrian malware. Meanwhile, the Syrian opposition, and several groups working closely with it, such as Cyber Arabs, have been active in attempting to identify potential threats and warn users. All of these digital attacks against the Syrian opposition are united by a common theme: "sophisticated social engineering that is grounded in an awareness of the needs, interests, and weaknesses of the opposition."[65] The attacker is often able to entice targets into opening cleverly masked files, sometimes distributed from the compromised accounts of people within the target's own social network.

The Syrian government has also taken overt steps toward monitoring dissidents and limiting digital communication between members of the opposition. Security officials reportedly demanded that detained dissidents provide them with their login credentials for social media and email accounts. In these cases, the Syrian government's decision to leave Facebook and other social networks unfiltered poses considerable risks to users, as they provide a ready-made surveillance platform and digital rolodex of potential enemies of the state. Additionally, according to an EFF post by Jillian York and Trevor Timm, there is a reason to believe that Syrian forces possess the capability to track satellite and cellular phones.[66] A number of publications reported that global positioning satellite

(GPS) tracking was likely used to determine the position of and then kill *Sunday Times of London* reporter Marie Colvin and French photographer Remi Ochlik in Homs, Syria. Given clear proof that the Syrian government has purchased Blue Coat products capable of advanced surveillance of online communications and has previously contracted Italian company Area SpA to install mass surveillance "monitoring centers," it is not difficult to believe that it has come into possession of similar technology for mobile phones.[67]

Drawing on the experiences in Egypt, Tunisia, Libya, and other Arab Spring hotspots, the Syrian Civil War has been a testing ground for the power of information communication technologies to undermine government control over media and communications during periods of civil conflict. However, the Syrian government and pro-government actors have proven adept at exploiting the very social media platforms and digital tools so enthusiastically supported by the U.S. Government and humanitarian organizations.

Social Media, Crowdsourcing, and Digital Technologies as Vehicles of Violence.

Apart from the type of targeted exploitation of social media described earlier, it is important to underline that widespread adoption of these technologies does not necessarily correlate to positive change or opportunities for humanitarian relief. In one case study in Assam, India, violence between Hindus and Muslims was exacerbated by the widespread circulation in urban centers of text messages warning of renewed attacks and photographs depicting gruesome deaths. As a result, panic at the prospect of imminent violence spread across several cities outside of the region. In

actuality, no violence had taken place in Assam, and the photos were altered images from previous crises and conflicts outside of India. Rebecca Goolsby of the Office of Naval Research has described this incident as an example of a "social cyber-attack," where loose collections of individuals within and outside of the country are able to "sow uncertainty in tense situations."[68] While digital humanitarians are keenly aware of the spread of misinformation, one can imagine systematic social cyberattacks becoming more common and less easily guarded against.

Another study focusing on cellular penetration in Africa found a consistent positive relationship between cell phone coverage and violent conflict, concluding that the "availability of cell phone coverage significantly and substantially increases the probability of violent conflict."[69] The authors argue that cell phone availability solves many of the logistical collective action problems in violent insurgencies by facilitating communication and coordination between potential conflict actors. While the authors caution that the spread of cellular technology may have a net positive effect, in the long run, they warn that their findings have deep implications for the development of violent insurgencies and civil conflicts in a region already blighted with them.

Latin America provides further examples of the ways in which social media and other digital technologies can be used to foment rather than contain violence. Latin America is undergoing a communications revolution. Internet and social media use, especially via mobile phone, has expanded rapidly among the youth demographic. At the same time, cyberspace has become fertile territory for criminal activity, as organized crime networks increasingly leverage digi-

tal technology for the purposes of narco-trafficking. Drug cartels and gangs have hijacked social media and blogs, using them to issue threats or to glorify and legitimize the lifestyle of organized crime.[70] Some cartels maintain their own fairly sophisticated telecommunications networks to coordinate drug shipments and assaults on security forces.[71]

The spread of digital technologies among organized crime has exposed journalists, activists, and other citizens to new vulnerabilities. The cartels reportedly employ in-house experts to monitor new websites, web forums, and social media for those who speak out against their activities. Cartels will often take violent retribution against those bloggers and social media users whom they have identified as antagonistic.[72] A survey by Freedom House on the attitude of 102 Mexican bloggers and journalists shows that:

> [N]early 70 percent have been threatened or have suffered attacks because of their work. In addition, 96 percent say they know of colleagues who have been attacked. Respondents to the survey also say they view cyber-espionage and e-mail-account cracking as the most serious digital risks they face. And while nearly all have access to and rely on the Internet, social networks, mobile phones and blogging platforms for their work, they also admit that they have little or no command of digital security tools such as encryption, use of virtual private networks (VPNs), anonymous Internet navigation and secure file removal.[73]

The authors of the report also argue that there is an:

> urgent need to introduce Mexican journalists and bloggers to new technologies and protocols and help newsrooms develop a culture of digital-security awareness to counter increasingly sophisticated threats and

attacks from both governmental agencies and criminal organizations.[74]

Given these threats, activists and researchers should properly reflect on the dangers of using social media and digital technologies to monitor criminal activity in hostile atmospheres. Projects such as MOGO, which provides information on Mexican drug cartel activity using Google's search engine, are just as vulnerable to violent retribution as are the journalists and civil society actors who have tried to expose their activities.[75] These activities have clear benefits for research and advocacy, but the potential risks to those involved in their creation must be evaluated.

Regardless of the location of these threats, it appears that nonstate actors, such as organized criminals, rebels, insurgents, and rioters have proved to be as adept at exploiting digital technologies for their own ends as have the governments that monitor them. Thus, the spread of digital technologies need not necessarily result in increased access to information, opportunities to better tailor humanitarian relief, or tools to employ in the struggle against authoritarian governments. Rather, increased access to ICTs offers new avenues for nonstate actors to engage in escalated violence against citizens and the state, as well as for state repression of opposition and insurgents.

CONCLUDING REMARKS

Violent conflict in the current era comes in many forms, including interstate wars, insurgencies, communal and sectarian violence, and conflicts between the state and powerful organized crime groups. The presence of digital technologies in armed conflict

should not obfuscate one central truth: war is war, and, as such, technology may transform the character of armed conflict, but it remains a persistent feature of human interaction where violence leads to death. The concept of a "clean" or "virtual" war is simply a nonexistent idea.

While there are many exciting opportunities for digital humanitarianism today, groups involved in the latter need to be keenly aware of the often harsh reality of armed conflict and other crises. Fortunately, awareness is growing, and "best practices" for the digital world are beginning to spread. The Committee to Protect Journalists, for example, has a security guide for journalists that includes information on information security.[76] The International Red Cross/Red Crescent released a study that includes a chapter on how to manage sensitive data online.[77] The paper warns aid workers of the potential consequences of posting sensitive information (e.g., pictures of people in crisis areas, Tweets disclosing locations of refugees, etc.) lest they are used to harm at-risk groups. The GSM association has also produced a code of conduct for SMS use in disaster situations.[78]

The evidence presented in this chapter, however, offers some disturbing trends. Work in the context of authoritarian, autocratic, or corrupt regimes, and even in stateless zones of conflict, can present formidable risks for the digital humanitarian. Indeed, some of the tools introduced into zones of conflict as part of digital humanitarian operations might even contribute to or exacerbate those risks, creating unforeseen vulnerabilities exploited by adversaries and protagonists to a conflict. In the context of natural disasters, Meier, for example, raises the issue of oversharing of personal data such as phone numbers, email addresses, and other personal information over social media chan-

nels in a crisis situation that one would not release in normal circumstances.[79] This concern holds true in armed conflict situations where relaying conflict-relevant information such as personal email or Facebook accounts over channels considered secure to parties considered trustworthy may be a more dangerous activity than participants fully realize.

Rather than holding out the prospect of a major advance in conflict prevention and humanitarian relief, this research suggests we are instead on the precipice of a major spiral toward a new and highly refined form of digitally armed conflict. Vulnerabilities of humanitarian activists, journalists, and other participants in conflict situations have been documented in so many disparate situations that one must conclude that it is too simple to make an argument that digital technologies are inherently benign. One must also contrast the positive uses of those technologies with the myriad of examples with which they can be used to make the safety, privacy, and general rights of human beings fundamentally more insecure.

ENDNOTES - CHAPTER 10

1. "The World in 2013: ICT Facts and Figures," International Telecommunication Union, February 2013, available from *https://www.itu.int/en/ITU-D/Statistics/Documents/facts/ICTFactsFigures2013-e.pdf*, accessed on September 20, 2013.

2. "Definitions," Uppsala, Sweden: Uppsala University, Department of Peace and Conflict Research, available from *pcr.uu.se/research/ucdp/definitions/*, accessed September 20, 2013.

3. "Chapter 7: Non-state armed conflict," *Human Security Report 2012*, Human Security Report Project, Vancouver, Canada: Simon Fraser University, p. 189, available from *hsrgroup.org/docs/Publications/HSR2012/HSRP2012_Chapter%207.pdf*, accessed on September 20, 2013.

4. "World Development Report 2011," Bretton Woods, NH: World Bank, p. 1, available from *siteresources.worldbank.org/INTWDRS/Resources/WDR2011_Full_Text.pdf,* accessed September 20, 2013.

5. Wikipedia contributors, "List of ongoing military conflicts," Wikipedia The Free Encyclopedia, available from *en.wikipedia.org/wiki/List_of_ongoing_military_conflicts*, accessed on September 23, 2013; International Telecommunication Union, "*Percentage of individuals using the Internet,"* available from *itu.int/en/ITU-D/Statistics/Documents/statistics/2013/Individuals_Internet_2000-2012.xls*, accessed on September 23, 2013; and International Telecommunication Union, "*Mobile Cellular Telephone Subscriptions,"* available from *itu.int/en/ITU-D/Statistics/Documents/statistics/2013/Mobile_cellular_2000-2012.xls*, accessed on September 23, 2013.

6. Micah Zenko, "Ask the Experts: Social Media and Conflict Prevention," Council on Foreign Relations, Washington, DC, January 23, 2013, accessed September 20, 2013, available from *blogs.cfr.org/zenko/2013/01/23/ask-the-experts-social-media-and-conflict-prevention/*.

7. "Big data, small wars, local insights," Washington, DC: McKinsey and Company, available from *voices.mckinseyonsociety.com/big-data-small-wars-local-insights-designing-for-development-with-conflict-affected-communities/*, accessed on September 20, 2013.

8. Patrick Meier, "New information technologies and their impact on the humanitarian sector," International Review of the Red Cross, No. 884, 2011, pp. 1239-1263, available from *icrc.org/eng/assets/files/review/2011/irrc-884-meier.pdf,* accessed on accessed September 20, 2013.

9. *Ibid*. Please note the following section relies on Meier's overview of information technology and the humanitarian sector.

10. Patrick Meier, "Our Efforts in Response to Haiti's Earthquake," Ushahidi, January 13, 2010, available from *https://www.ushahidi.com/blog/2010/01/13/our-efforts-in-response-to-haitis-earthquake.*

11. *Ibid*.

12. Project "Russian fires 2010" website hosted by Ushahidi, available from *russian-fires.ru/.*

13. Patrick Meier, "Using the New Ushahidi Platform to Crisis Map Libya," Ushahidi, March 6, 2011, available from *https://www.ushahidi.com/blog/2011/03/06/using-the-new-ushahidi-platform-to-crisis-map-libya.*

14. As cited in Julia Daisy Fraustino, Brooke Liu, and Yan Jin, "Social Media Use during Disasters: A Review of the Knowledge Base and Gaps," College Park, MD: University of Maryland, National Consortium for the Study of Terrorism and Responses to Terrorism, December 12, 2012, p. 4, available from *start.umd.edu/sites/default/files/files/publications/START_SocialMediaUseduringDisasters_LitReview.pdf*.

15. Tim Large, "Will Twitter put the U.N. out of the disaster business?" Reuters (blog), March 24, 2012, available from *blogs.reuters.com/the-human-impact/2012/03/24/will-twitter-put-the-u-n-out-of-the-disaster-business/.*

16. *Ibid.*

17. American Red Cross, "Social Media in Disasters and Emergencies," August 5, 2010, available from *i.dell.com/sites/content/shared-content/campaigns/en/Documents/Red-Cross-Survey-Social-Media-in-Disasters-Aug-2010.pdf.*

18. "Sensing and shaping emerging conflicts," Washington, DC: United States Institute of Peace, available from *usip.org/events/sensing-and-shaping-emerging-conflicts*, accessed September 24, 2013.

19. BBC Media Action, "Still left in the dark? How people in emergencies use communication to survive—and how humanitarian agencies can help," Policy Briefing #16, London, UK, March 2012, available from *downloads.bbc.co.uk/mediaaction/policybriefing/bbc_media_action_still_left_in_the_dark_policy_briefing.pdf.*

20. "World Development Indicators 2010," Bretton Woods, NH: World Bank, available from *devdata.worldbank.org/DataVisualizer/*, accessed September 24, 2013.

21. Ronald J. Deibert, *Black Code: Inside the Battle for Cyberspace*, Toronto, Canada: Signal, 2013, pp. 64-66; and Ron Deibert and Rafal Rohozinski, "The new cyber military-industrial complex," *The Globe and Mail*, March 28, 2011, available from *theglobeandmail.com/commentary/the-new-cyber-military-industrial-complex/article573990/*.

22. Deibert, *Black Code*, pp. 65-66.

23. Ronald J. Deibert, "From Deep Black to Green? Demystifying the Military Monitoring of the Environment," Washington, DC: Environmental Change and Security Program, 1996, available from *mercury.ethz.ch/serviceengine/Files/ISN/136131/ipublicationdocument_singledocument/ea16cf11-6a91-42e8-b39f-c912087b284a/en/ECSP report_2.pdf*.

24. Patrick Meier, "Fourth-Generation Early Warning Systems (Updated)," Conflict Warning and Early Response, March 6, 2009, available from *earlywarning.wordpress.com/2009/03/06/fourth-generation-early-warning-systems/*.

25. *Ibid.*

26. "Preventing Violence, War, and State Collapse: The Future of Conflict Early Warning and Response," Paris, France: Organisation for Economic Co-operation and Development (OECD), 2009; Meier, "*Fourth-Generation Early Warning Systems.*"

27. Patrick Meier, "Enabling Crowdfunding on Twitter for Disaster Response," iRevolutions, September 17, 2013, available from *irevolution.net/2013/09/17/crowdfunding-for-disaster-response/*.

28. "Big data, small wars, local insights."

29. Brian Heaton, "How Emergency Managers Can Benefit from Big Data," *Emergency Management*, July 23, 2013, available from *emergencymgmt.com/disaster/Emergency-Managers-Big-Data.html*.

30. George Chamales and Rob Baker, "Securing Crisis Maps in Conflict Zones," paper presented at the Global Humanitarian Technology Conference (GHTC), Seattle, Washington, October-November 2011, pp. 426-430.

31. "Humanitarianism in the Network Age," OCHA Policy and Studies Series, New York: UN Office for the Coordination of Humanitarian Affairs, 2013, available from *docs.unocha.org/sites/dms/Documents/WEB%20Humanitarianism%20in%20the%20Network%20Age%20vF%20single.pdf*.

32. Chamales and Baker.

33. Masashi Crete-Nishihata and Jillian C. York, "Egypt's Internet Blackout: Extreme Example of Just-in-time Blocking," *OpenNet Initiative*, January 28, 2011, available from *opennet.net/blog/2011/01/egypt's-internet-blackout-extreme-example-just-time-blocking*.

34. Stephanie Wang, "Pulling the Plug: A Technical Review of the Internet Shutdown in Burma," *OpenNet Initiative*, available from *opennet.net/sites/opennet.net/files/ONI_Bulletin_Burma_2007.pdf* accessed September 24, 2013.

35. Rebekah Heacock, "China shuts down Internet in Xinjiang region after riots," *OpenNet Initiative*, July 6, 2009, available from *opennet.net/blog/2009/07/china-shuts-down-internet-xinjiang-region-after-riots*, accessed on September 24, 2013.

36. Morgan Marquis-Boire, Collin Anderson, Jakub Dalek, Sarah McKune, and John Scott-Railton, "Some Devices Wander By Mistake: Planet Blue Coat Redux," *Citizen Lab*, July 9, 2013, available from *citizenlab.org/2013/07/planet-blue-coat-redux/*.

37. Lotta Themnér and Peter Wallensteen, "Armed Conflict, 1946-2011," *Journal of Peace Research*, Vol. 49, No. 4, 2012. The research cited here includes ongoing armed conflicts as of 2011.

38. See *citizenlab.org/storage/bluecoat/fig1.jpg*.

39. *Ibid.*

40. Eva Galperin, "Sudan Revolts, Government Cracks Down on Dissent," *Electronic Frontier Foundation*, July 10, 2012, available from *eff.org/deeplinks/2012/07/sudan-revolts-government-cracks-down-dissent*.

41. Patrick Meier, "How to Use Facebook if You Are a Repressive Regime," iRevolutions, February 10, 2011, available from *irevolution.net/2011/02/10/facebook-for-repressive-regimes/*.

42. Alan Boswell, "How Sudan used the Internet to crush protest movement," *McClatchy Newspapers*, April 6, 2011, available from *mcclatchydc.com/2011/04/06/111637/sudans-government-crushed-protests.html#ixzz1JFib5KYX*. Note that, in response to this article, a message posted on Ushahidi's blogsite by Patrick Meier did claim that assertions that the CrowdMap site he had worked on was phased out and not actually infiltrated, although he and other colleagues have acknowledged the precarious nature of such platforms in insecure environments. See Patrick Meier, "Sudan Crowdmap, Misinformation and Repression," Ushahidi, April 13, 2011, available from *https://www.ushahidi.com/blog/2011/04/13/sudan-crowdmap-misinformation-and-repression.*

43. Deepa Babington, "Sudan's cyber-defenders take on Facebook protesters," Reuters, March 30, 2011, available from *reuters.com/article/2011/03/30/us-sudan-internet-feature-idUSTRE72T54W20110330.*

44. "Our Story," Satellite Sentinel Project, available from *satsentinel.org/our-story*, accessed on September 24, 2013.

45. UN Office for the Coordination of Humanitarian Affairs.

46. "The security and ethics of live mapping in repressive regimes and hostile environments (updated February 15)," The Standby Task Force, February 5, 2013, available from *blog.standbytaskforce.com/2011/02/05/the-security-and-ethics-of-live-mapping-in-repressive-regimes-and-hostile-environments/*.

47. Morgan Marquis-Boire, Bill Marczak, Claudio Guarnieri, and John Scott-Railton, "For Their Eyes Only: The Commercialization of Digital Spying," Citizen Lab, April 30, 2013, available from *citizenlab.org/2013/04/for-their-eyes-only-2/*. Note that the United States, which was found to have the characteristics of FinFisher command-and-control servers in the past, is also considered a state engaged in ongoing conflict with reference to its war against al-Qaeda, according to the Uppsala Data Conflict Program (Lotta and Wallensteen, 2012).

48. See *https://citizenlab.org/wp-content/uploads/2013/04/TheirEyesMap-web.jpg*.

49. This section draws heavily from research conducted by John-Scott Railton on cybertechnology usage in Libya. See John-Scott Railton, *Revolutionary Risks: Cyber Technology and Threats in the 2011 Libyan Revolution,* Newport, RI: U.S. Naval War College, Center on Irregular Warfare & Armed Groups (CIWAG), 2013.

50. *Ibid*.

51. Jim Cowie, "What Libya Learned from Egypt," Renesys, March 5, 2011, available from *renesys.com/2011/03/what-libya-learned-from-egypt/*.

52. "Mapping Violence Against Pro-Democracy Protests in Libya," Arasmus, March 1, 2011.

53. Scott-Railton, *Revolutionary Risks*, p. 18.

54. Scott Peterson, "Syria's iPhone insurgency makes for smarter rebellion," *The Christian Science Monitor*, August 1, 2012, available from *csmonitor.com/World/Middle-East/2012/0801/Syria-s-iPhone-insurgency-makes-for-smarter-rebellion*.

55. Jay Newton-Small, "Hillary's Little Startup: How the U.S. Is Using Technology to Aid Syria's Rebels," *Time*, June 13, 2012, available from *world.time.com/2012/06/13/hillarys-little-startup-how-the-u-s-is-using-technology-to-aid-syrias-rebels/*.

56. Patrick Meier, "Crisis Mapping Syria: Automated Data Mining and Crowdsourced Human Intelligence," iRevolutions, March 25, 2012, available from *irevolution.net/2012/03/25/crisis-mapping-syria/*.

57. Neal Ungerleider, "The Syrian War Crowdsourcing Experiment," Fast Company, September 21, 2011, available from *fastcompany.com/1781570/syrian-war-crowdsourcing-experiment,* accessed on September 24, 2013.

58. "Documenting sexualized violence in Syria," New York: Women's Media Center, Women Under Siege, available from *womenundersiegesyria.crowdmap.com/main*, accessed on September 24, 2013.

59. "Today we commemorate the three months of sacrifice and bravery by Syrian citizens during the Syrian uprising," Local Coordination Committees, June 17, 2011, available from *lccsyria.org/373*, accessed on September 24, 2013.

60. "Eyes On Syria Map," New York: SBTF/Amnesty International, available from *eyesonsyria.org*.

61. "Qatar's Al Jazeera website hacked by Syria's Assad loyalists," Reuters, September 4, 2012, available from *reuters.com/article/2012/09/04/us-qatar-jazeera-hacking-idUSBRE8830ZI20120904*; "Reuters blogging platform hacked, false Syria blog posted," Reuters, August 3, 2012, available from *reuters.com/article/2012/08/03/reuters-syria-hacking-idUSL2E8J37CR20120803*; James Ball, "Amnesty International Web site hacked by supporters of Syrian government," *The Washington Post,* August 28, 2012, available from *washingtonpost.com/world/national-security/amnesty-international-website-hacked/2012/08/28/9628e83a-f121-11e1-a612-3cfc842a6d89_story.html*; and "2012 CyberWatch Year in Review: Middle East and North Africa, Southeast Asia, Latin America and the Caribbean," Citizen Lab, December 15, 2012, available from *citizenlab.org/2012/12/2012-year-in-review-cyberwatch/#cyberattacks*.

62. Information Warfare Monitor, "Syrian Electronic Army: Disruptive Attacks and Hyped Targets," last modified June 25, 2011, available from *https://opennet.net/syrian-electronic-army-disruptive-attacks-and-hyped-targets.*

63. Eva Galperin and Morgan Marquis-Boire, "New Malware Targeting Syrian Activists Uses Blackshades Commercial Trojan," Electronic Frontier Foundation, July 12, 2012, available from *eff.org/deeplinks/2012/07/new-blackshades-malware*.

64. "Fake Facebook Page Targets Pro-Revolution Syrian Users," *Information Warfare Monitor*, last modified August 29, 2011, available from *https://citizenlab.org/2011/08/fake-facebook-page-targets-pro-revolution-syrian-users/*; Eva Galperin, and Morgan Marquis-Boire, "Fake YouTube Site Targets Syrian Activists With Malware," Electronic Frontier Foundation, March 15, 2012, available from *eff.org/deeplinks/2012/03/fake-youtube-site-targets-syrian-activists-malware*; Eva Galperin, and Morgan Marquis-Boire, "New Trojan Spread Over Skype as Cat and Mouse Game Between Syrian Activists

and Pro-Syrian-Government Hackers Continues," Electronic Frontier Foundation, June 19, 2012, available from *eff.org/deeplinks/2012/06/darkshades-rat-and-syrian-malware*; and Eva Galperin and Morgan Marquis-Boire, "Trojan Hidden in Fake Revolutionary Documents Targets Syrian Activists," Electronic Frontier Foundation, May 31, 2012, available from *eff.org/deeplinks/2012/05/trojan-hidden-fake-revolutionary-documents-targets-syrian-activists*.

65. Morgan Marquis-Boire and Scott-Railton, "A Call to Harm: New Malware Attacks Target the Syrian Opposition," Citizen Lab, last modified June 21, 2013, accessed on September 20, 2013; Irene Poetranto "Behind Blue Coat: Investigations of commercial filtering in Syria and Burma," Citizen Lab, last modified November 9, 2011, accessed on September 20, 2013, available from *citizenlab.org/2011/11/behind-blue-coat/*.

66. Jillian C. York, and Trevor Timm, "Satphones, Syria, and Surveillance," Electronic Frontier Foundation, February 23, 2012, *eff.org/deeplinks/2012/02/satphones-syria-and-surveillance*.

67. "Behind Blue Coat;" Ben Elgin and Vernon Silver, "Syria Crackdown Gets Italy Firm's Aid With U.S.-Europe Spy Gear," Bloomberg Technology, November 3, 2011, available from *bloomberg.com/news/2011-11-03/syria-crackdown-gets-italy-firm-s-aid-with-u-s-europe-spy-gear.html,* accessed on September 20, 2013.

68. Rebecca Goolsby, "On Cybersecurity, Crowdsourcing, and Social Cyber-Attack," Washington, DC: The Wilson Center, available from *wilsoncenter.org/sites/default/files/127219170-On-Cybersecurity-Crowdsourcing-Cyber-Attack-Commons-Lab-Policy-Memo-Series-Vol-1.pdf*, accessed on September 20, 2013.

69. Jan H. Pierskalla and Florian M. Hollenbach, "Technology and Collective Action: The Effect of Cell Phone Coverage on Political Violence in Africa," *American Political Science Review*, Vol. 107, No. 02, May 2013, pp. 207-224.

70. John Burnett, "Mexican Drug Cartels Now Menace Social Media," NPR, September 23, 2011, available from *npr.org/2011/09/23/140745739/mexican-drug-cartels-now-menace-social-media*, accessed on September 20, 2013.

71. Jason Beaubien, "Mexico Busts Drug Cartels' Private Phone Networks," NPR, December 9, 2011, available from *npr.org/2011/12/09/143442365/mexico-busts-drug-cartels-private-phone-networks*, accessed on September 20, 2013.

72. Neal Ungerleider, "Mexican Narcogangs' War on Digital Media," Fast Company, October 6, 2011, available from *fastcompany.com/1785413/mexican-narcogangs-war-digital-media*, accessed on September 20, 2013.

73. Jorge Luis Sierra, "Digital and Mobile Security for Mexican Journalists and Bloggers," Washington, DC: Freedom House and the International Center for Journalists, available from *freedomhouse.org/sites/default/files/Digital and Mobile Security for Mexican Journalists and Bloggers.pdf*, accessed on September 20, 2013.

74. *Ibid.*, p. 4.

75. Michele Coscia and Viridiana Rios, "How and where do criminals operate? Using Google to track Mexican drug trade," Working Paper, Cambridge, MA: Harvard University, 2012.

76. Frank Smyth, "Journalist Security Guide," New York: Committee to Protect Journalists, available from *cpj.org/reports/2012/04/journalist-security-guide.php*, accessed on September 20, 2013.

77. "Professional standards for protection work carried out by humanitarian and human rights actors in armed conflict and other situations of violence," Geneva, Switzerland: International Committee of the Red Cross, last modified April 4, 2013, available from *icrc.org/eng/resources/documents/publication/p0999.htm*, accessed on September 20, 2013.

78. GSMA Disaster Response, Souktel, and The Qatar Foundation, "Towards a Code of Conduct: Guidelines for the Use of SMS in Natural Disasters," iRevolutions, last modified 2013, available from *irevolution.files.wordpress.com/2013/02/dr_sms_220213_spreads.pdf*, accessed September 20, 2013.

79. Patrick Meier, "Data Protection: This Tweet Will Self-Destruct In . . .," iRevolutions, September 6, 2013, available from *irevolution.net/2013/09/06/this-tweet-will-self-destruct/*.

CHAPTER 11

THE THREAT FROM INSIDE . . . YOUR AUTOMOBILE

Isaac R. Porche III

INTRODUCTION

Automobiles have a cybersecurity risk. The vulnerabilities stem from the abundance of software, computers, and networks that have been designed into automobiles beginning several decades ago. Published experimental results and real-world incidents substantiate the existence of vulnerabilities in today's commercial automotive fleet. Like the vulnerabilities of the Internet, these automobile-based ones are likely to persist. Security standards, federal motor vehicle regulations, and a new patching regimen by car owners will be needed to help mitigate the risk. Until then, it is not hard to imagine a day when a portion of the American automobile fleet is taken over by nefarious actors.

This chapter is organized into three parts. The first part is about the risks that exist from the computers and networks that are onboard today's commercial automobiles. The second part describes the implications of the risks. The third part presents a contrived scenario, where the vulnerabilities described are exploited to produce a catastrophic event.

AUTOMOBILES HAVE (CYBER) RISK

The first part of this chapter discusses the risks.

Embedded Computers and Networks in Automobiles Make Them Vulnerable.

Vulnerabilities have existed in automobiles for some time because of all of the software, computers, and networks that have been embedded in automobiles over the last 30 years. The Cadillac brand has hosted onboard networks since the 1980s.[1] The data rates on these networks continue to grow.[2] Today, modern automobiles literally run on millions of lines of software code and 30 to 100 computers.[3]

A big push for onboard networks—that spanned the entire U.S. automotive sector—came in the mid-1990s and was driven by new emission regulations. It was the start of regulations in the United States requiring an onboard physical connector to allow access to vehicle electronics.[4] These are called onboard diagnostic (OBD) connectors. They enable a mechanic, an inspector, or even the car owner to connect to the vehicle's onboard computers. These connectors have existed on U.S. vehicles for many years.

More recently, connectivity has expanded from the wired medium to the wireless world. Today, wireless communication devices are common on vehicles. University researchers[5] have explored the viability of exploiting all of the communication systems that reside in vehicles. The researchers showed that exploitation is possible using:

> Onstar-like cellular connections, Bluetooth bugs, a rogue android application that synched with the car's network from the driver's smartphone, or even a malicious audio file in the cars stereo.[6]

This finding is significant because these links enable access to onboard computers, which can control the vehicle via drive-by-wire systems (DBW).

A DBW trend is evident, i.e., automobiles are increasingly controlled electronically and not mechanically. "Active Park Assist" will parallel park a car using sensors to measure distances to the curb.[7] Other DBW features available today include electric power steering, electric throttle, and braking for adaptive cruise control. Ford plans a "Traffic Jam Assist" feature, perhaps in 2017,[8] to steer, throttle, and brake the vehicle automatically via computer control. The Berkeley PATH project demonstrated automated driving over 20 years ago[9] using vehicle-to-vehicle communication and onboard radars. Today, Google is actively demonstrating its own driverless car.

In the future, there will be more and more automation of the functions previously performed by the driver. All of this means that computers and networks are performing the functions and issuing the driving commands to the vehicle. Published experimental results[10] substantiate the existence of vulnerabilities in today's commercial automobile fleet. Table 11-1 below summarizes their findings.

Vulnerability Class	Channel	Implemented Capability	Visible to User	Scale	Full Control	Cost
Direct physical	OBD-II port	Plug attack hardware directly into car OBD-II port	Yes	Small	Yes	Low
Indirect physical	CD	CD-based firmware update	Yes	Small	Yes	Medium
	CD	Special song Windows media audio (WMA)	Yes	Medium	Yes	Medium-High
	PassThru	Wi-Fi or wired control connection to advertised PassThru devices	No	Small	Yes	Low
	PassThru	Wi-Fi or wired shell injection	No	Viral	Yes	Low

Table 11-1. Attack Surface Capabilities.[11]

Short-range wireless	Bluetooth	Buffer overflow with paired Android phone and Trojan app	No	Large	Yes	Low-Medium
	Bluetooth	Sniff media access control (MAC) address, brute force personal identification number (PIN), buffer overflow	No	Small	Yes	Low-Medium
Long-range wireless	Cellular	Call car, authentication exploit, buffer overflow (using laptop)	No	Large	Yes	Medium-High
	Cellular	Call car, authentication exploit, buffer overflow (using iPod with exploit audio file, earphones, and a telephone)	No	Large	Yes	Medium-High

Source: Checkoway *et al*., 2011.
Note: According to their notes, "the Visible to User column indicates whether the compromise process is visible to the user (the driver or the technician); we discuss social engineering attacks for navigating user detection in the body. . . . The Scale column captures the approximate scale of the attack. . . . The Full Control column indicates whether this exploit yields full control over the components connected controller area network (CAN) bus (and, by transitively, all of the engine control units in the car). Finally, the Cost column captures the approximate effort to develop these attack capabilities."

Table 11-1. Attack Surface Capabilities.(cont.)[11]

History of Local Area Networks within Automobiles.

In-vehicle networks were introduced decades ago to enable diagnostic queries, emission checking, and the sharing of the sensors and other data between multiple in-vehicle computers.[12] A predominant networking protocol used for automobiles today is the CAN bus. It was developed by Bosch in the 1980s and became an International Organization for Standardization standard a decade later. Many new European and North American cars have a CAN bus.[13] CAN

was designed to handle up to 800 kilobits per second (kbps) of network traffic. For higher data rates, there are other networks onboard like media oriented systems transport (MOST).[14] CAN is known as a standard which makes it easy to access and exploit. Specifically, these networks are well-studied by car enthusiasts and computer hackers alike.[15] For example, there was a workshop on how to hack into CAN. It was held at DEFCON (defense readiness condition) 19, which is a well-known annual hacker conference. A website (*www.canbushack.com*) still exists.

Protocols and Standards for In-vehicle Networking Are Defined.

Government and industry standards have enabled a degree of interoperability between available devices and commercial in-vehicle networks. A sample of some are listed below:

- **SAE J1962 –** The OBD-II connector standard has been required on most vehicles since 1996. It allows a hand-held scanner to plug physically into a car's networks easily from the passenger compartment. The connector can be converted into a USB port to enable any ordinary laptop to be connected. Today, this connector is not relied upon as much for diagnostics but is being increasingly used to log data for insurance companies and others.
- **SAE J1850 –** This is a network protocol used with the OBD-II connector.
- **SAE J2534 –** The "PassThru" standard for reprogramming engine and other onboard computers is the newer prevailing standard for diagnostic and vehicle interrogation.

These standards promote universal connectivity and ease of use. However, this invites security compromise.

In-vehicle Networks Are Designed for Easy Physical Access.

The use of onboard connectors and the existence of onboard networks and networking protocols makes it easy to interrogate vehicle networks and reprogram vehicle computers. Mechanics use commercially available devices to read the networks for trouble codes, as do clerks at many auto parts stores.

Potential Consequences of Exploiting These Networks Has Been Demonstrated.

In 2010, a 20-year-old disgruntled employee remotely disabled over 100 vehicles.[16] He did so by illegally accessing a website that could send wireless signals to the security systems installed on these vehicles.

In an article published by the Institute of Electrical and Electronics Engineers (IEEE), University of Washington researchers[17] exposed numerous flaws in the prevailing standard for in-vehicle networks. The flaws enable a bypass of "rudimentary network security protections." The researchers were able to embed malicious code in safety-critical systems sufficient to facilitate disablement of the braking system.

In 2013, two Defense Advanced Research Projects Agency-funded researchers in Indiana demonstrated how to "exploit" a Ford Escape. They connected a MacBook laptop to the OBD connector to override the driver's commands and divert the vehicle into a vacant field.[18] The same researchers co-opted a Toyota

Prius and controlled its acceleration, steering, seatbelt tightness, horn, and brakes.

Parallels with Insecurity of Internet.

There are similarities when comparing the modern security problems of the Internet and the emerging security problems of networked vehicles. Two reasons are: (1) both have to support multiple access points (physical and virtual), and (2) have to support connection with unknown entities. These requirements result in the complexity of the system design. As the saying goes, "complexity is the bane of security." The second reason is that vehicle networks increasingly are a part of the Internet. They are interconnected through handheld devices and other wireless communication nodes embedded in the vehicle to support telematics, vehicle diagnostics, and other functions.[19] Vehicle networks and the Internet inherit each other's security posture.

In the field of information technology, there is an established history of adopting operating systems that are easier to work with but less secure. Arguably, the Internet itself grew from a design philosophy where the need for interoperability, usability, and connectivity trumped the need for a more secure design.

An important example from 50 years ago is Multiplexed Information and Computing Service (MULTICS), which was replaced by a family of multitasking, multiuser computer operating systems known as UNIX. Early on, UNIX was the operating system used by many of the Internet's servers. Developers chose the name UNIX because it is an "emasculated MULTICS." The original name was spelled UNICS, which stood for UNiplexed Information and Computing Service.[20]

Bruce Scheier summarized the advantages of MULTICS: "MULTICS was an operating system from the 1960s, and had better security than a lot of operating systems today."[21] According to a review by Paul Karger and Roger Shell, "MULTICS had a primary goal of security from the very beginning of its design."[22] Their review, completed 20 years ago, asserted that MULTICS security features from the 1960s were not designed into products current today (i.e., those developed around the millennium). MULTICS was replaced with UNIX due to usability. According to Ken Thompson, the esteemed co-developer of MULTICS and UNIX, "[MULTICS was] . . . overdesigned and overbuilt and over everything. It was close to unusable."[23]

For these reasons, it is fair to say that the Internet was not designed with the most robust security design. This flaw can be blamed on the usability of security in general.[24] The bottom-line is this: There is no reason to hope that vehicle networks will "grow up" to be any more secure than the Internet, which is not very secure.

Risk from the Computerized Transportation Infrastructure.

Increasingly, risks also come from the information technology (IT)-laden road infrastructure, which, in some cases, is coupled to vehicle technology. This includes:

- Computer controlled traffic lights that are either:
  - hard-wire networked to enable updates and changes,

  - dynamically changeable via wireless communication devices (for emergency responders and police),
  - and/or updated by plugging in a laptop.
  - This includes ramp meters at freeway entrances.
- Advanced traveler information systems (ATIS), which includes their websites. Note: A transit system's ATIS was recently hacked in 2011 by the group, Anonymous.[25]
- Other field devices like "toll tag readers, cameras, and roadside equipment [that] are quite susceptible to tampering."[26]

Edward Fok provides a more complete overview of the cybersecurity issues in modern transportation systems.[27]

IMPLICATIONS

The second part of this chapter speculates on the implications of the risk.

The Role of Cars in Society is Large.

What would be the impact on the economy if no commuter's car started in the morning? According to the census bureau, the average driver's commute to work is just under a half-hour. We can assume this means driving is a necessity for a large portion of automobile commuters. Although many large metropolitan areas have mass transit, it is not likely that many cities could handle the ridership increase if a significant fraction of automobile commuters switched modes.

The economic impact of the attacks that occurred on September 11, 2001, is estimated to be over $100 billion.[28] The reasonable question is to ask, "Will the same magnitude of loss occur after a temporary loss of automobile usage and highway access due to a massive cyberattack on the commercial fleet?" Arguably, an equal amount of economic paralysis seems possible if any transportation sector becomes of limited use, even for a few days.

The Automobile is a Cyber-Physical System.

The National Science Foundation uses the term "cyber-physical system," to describe "a system of collaborating computational elements controlling physical entities."[29] Supervisory control and data acquisition (SCADA) systems come to mind, and there is considerable research on the robustness and cybersecurity of SCADA systems.

Automobiles today are "mobile cyber-physical systems." As argued by Qaisar Shafi,[30] the robustness of such systems to threats posed is critical. This threat is critical because the increased electronic content that controls an automobile today can render it, literally, into a remotely controlled precision guided missile. It is a missile that is laden with liquid fuel.

A coordinated cyberattack on a large number of automobiles could crash the road network they traverse by congesting it with remotely triggered accidents or remotely triggered disablements. The psychological impact on highway commuters of even a small demonstration of this vulnerability could persuade most drivers to abandon automobile use at least temporarily.

SCENARIO

Given the risks described in this chapter and speculation on the implications of the risks, a scenario is developed for consideration.

Threat from Automobiles.

Consider a future scenario that involves:

- thousands of multi-ton projectiles,
- laden with liquid fuel and explosives,
- loitering in a holding pattern at high speeds,
- around sensitive targets in the national capital region (e.g., Metro, DC),
- waiting for electronic instructions to seek and destroy assets important to the U.S. Government.

Many people would think this is referring to a new smart weapon employed in a Hollywood movie. However, it could refer to rush hour traffic on the DC beltway, leveraging vehicles that could be exploited and controlled. In Steven King's 1973 short-story titled *Trucks*, the story-line is similar.

The Road to Calamity.

The year is 2019, 1-year before the calamity.

(Day-365): Foreign operatives, educated and living in the United States, join FakeCompanyScanX (FCS-SXN) as software developers. FCS-SXN is a maker of a device sold in auto parts stores. When that device (or tool) is plugged into a vehicle's onboard network, the device will report on the health of the automobile. It allows individual car owners to monitor and check

their own cars for repair issues. The FCS-SXN scanner is also used in many auto repair shops. In Virginia, it is used by nearly all the repair shops and dealerships for annual vehicle inspections.

The operatives, working as developers at the company, design the FCS-SXN scanner so that, upon connection to a vehicle, it will surreptitiously upload malicious code into each car's computer system, where it will remain dormant. The FCS-SXN device works in almost all commercial vehicles sold in the United States as a result of standards and protocols adopted over several decades.

Around the same time, a free, popular "smart-app" is circulating on the Internet. It is designed to work on any Android or iPhone. The smart-app was also created by FCS-SXN, and it allows the smartphone it resides on to "pair" with most vehicles that use Bluetooth. The smart-app provides an automatic status check to the owner's phone and other helpful features. Unknown to the owners of the phone, the smart-app can "talk" to the malicious code inside the infected vehicle. The smart-app also talks to a central server over the Internet (using the phone's wireless connection).

(Day-30): It is the year 2020. Over the last year, 10 percent of commuters in the Metro, DC, area have had their cars scanned by the FCS-SXN tool and have become infected. In addition, many of those car-owners have been solicited by FCS-SXN with advertisements offering them the free smart-app. Ten percent of them have downloaded it to their smartphone.

(Day-0 or D-Day): At 7:30 a.m., a central server under the control of foreign adversaries issues a command over the Internet to all cell phones running the smart-app. The smart-app commands any infected vehicle in the range of its blue-tooth signal to set the vehi-

cle's throttle to the maximum opening. This command affects 0.5 percent of the commuting vehicles in the DC area. These cars are instantly accelerated. By 8:00 a.m., there are over 5,000 accidents across the Metro, DC, area. Witnesses report that in nearly all cases, the drivers' cars suddenly accelerate out of control. This begins the attack. In the aftermath, disabled cars, collisions, or emergency responders snaking through the calamity block all major throughways.

(Day+1): The congestion is overwhelming, and the road network is unusable in many parts of the Metro, DC, area.

(Day+2): The nefarious actors send text messages to the affected smartphones to take credit for the auto cyberattack. This is reported by the media and commuters and confirms many suspicions.

(Day+3): Drivers in many metropolitan areas across the United States abandon their use of automobiles and flock to other forms of transportation that are perceived to be "safe" like rail or bicycle.

(D+180): Software patches to cars and smartphones are sufficiently distributed, and normalcy is returning to the DC area. However, the economic consequences are devastating.

CONCLUSIONS AND RECOMMENDATIONS

There is a growing awareness of the need for cybersecurity in automobiles[31] and transportation systems in general.[32] Officials in the government are certainly alarmed. In his testimony to the Senate in May of 2013, David Strickland, head of the National Highway Traffic Safety Administration (NHTSA) said, "These interconnected electronic systems are creating opportunities to improve vehicle safety and reliability, but

are also creating new and different safety and cybersecurity risks." According to the testimony, "hackers could potentially tap into these systems to steal cars, to eavesdrop on conversations or even to cause collisions."[33] Strickland is proposing a new division in NHTSA to address the concerns.

This newfound awareness of the need for automobile cybersecurity is news.[34] What is not new is the vulnerability, which has existed for some time and is likely to persist. This chapter highlights cybersecurity risks in modern automobiles and explores the implications. A scenario is presented that considers how the risks could be exploited. The purpose of presenting such a scenario is to make the point that the transformation of automobiles over the last few decades from mechanical drive to electronic drive, has also transformed them into millions of critical cyber-physical systems.

To prevent such a scenario from possibly occurring in the future, a number of things need to take place. First, revised motor vehicle safety standards are needed that address the cybersecurity of the modern automobile. Second, increased consumer awareness of the need for proper "auto-cyber-hygiene" is needed. In addition, higher consumer expectations are needed to allow market forces to pressure automakers to provide more guarantees. Third, there is a need for a commercial base of providers of anti-malware software that scans and secures vehicle computers and networks.

DISCUSSION: OTHER THREATS AND IMPLICATIONS

As noted by Isaac Porche, Jerry Sollinger, and Shawn McKay, similar threats apply to many other physical systems including smart homes and smarter cars:

> Neither 'wire' nor consent is required for one to be represented in cyberspace. Air gaps are difficult to maintain and thus no longer sufficiently protect devices from nefarious actors who operate in cyberspace . . . [a]s long as a device is not dumb (that is, as long as it contains a processor and some memory), it can be accessed, affected, and controlled to some degree by anyone who can overcome the air gap.[35]

The list of at-risk systems that fall into this category is long and includes medical devices, home automation systems, and other appliances being integrated into automobiles.

Smart thermostat products, like Nest (see *https://nest.com/thermostat/life-with-nest-thermostat/*), offer the user a monitoring system that tracks home activity. The system automatically adjusts the in-home temperature accordingly. Similar systems allow users to adjust home temperatures (or appliance settings or door locks) remotely from a smartphone. In a *Forbes Magazine* article,[36] Kashmir Hill describes her ability to turn on the bedroom lights of a complete stranger. These homes are only as secure as the underlying software and smartphones that facilitate access.

As noted in a 2013 article in *The Telegraph*, theoretically, "hackers need only to obtain the serial number of a pacemaker to force it to deliver an 830-Volt shock directly to a person's heart."[37]

ENDNOTES - CHAPTER 11

1. According to General Motors (GM):

> In Model Year 1981, all GM Passenger Cars for the U.S. market used a similar data link to a test connector for assembly line diagnostics. The value of this data in diagnosing emission systems after customer delivery was quickly identified and scanner tools were made to view and interpret the data stream. . . . In the 1985 model year, Cadillac FWD "C" vehicle had a electronic system that had point to point data links between five electronic modules and a dedicated assembly line diagnostic connector. . . . On the 1988 and 1989 model year Buick Reatta and 1986-89 model year Buick Riviera, touchscreen cathode ray tube (CRT) equipped vehicles, an 8,192 bit/sec data bus was implemented between the body computer module and the assembly line connector, climate control module, and CRT controller. This was GM's first multi-drop data bus.

Ronald Cox, "Development of First GM Vehicle Data Links," Detroit, MI: General Motors Corporation, available from *history.gmheritagecenter.com/wiki/index.php/Development_of_First_GM_Vehicle_Data_Links*.

2. In the early-1980s, the data rate on GM cars was 80 bits per second link. The data rate increased to over 8000 bits per second by the end of that decade. The controller area network (CAN) bus enables data rates to go up between 25 kilobytes per second (kbps) to one megabits per seconds on a single or dual-wire communication line (see canbuskit.com, undated).

3. According to Jim Motavalli, the first onboard computers in automobiles were in the mid-1970s: "The 1977 Oldsmobile Toronado had a very simple computer unit that was used for spark-plug timing, and the next year the Cadillac Seville offered an optional trip computer that used a Motorola chip." See Jim Motavalli, "The Dozens of Computers That Make Modern Cars Go (and Stop)," *The New York Times*, February 4, 2010. There is at least one European automaker with onboard computing or networking even earlier.

4. For the purpose of checking emissions through an onboard diagnostic (OBD) connector.

5. Karl Koscher, Alexei Czeskis, Franziska Roesner, Shwetak Patel, Tadayoshi Kohno, Stephen Checkoway, Damon McCoy, Brian Kantor, Danny Anderson, Hovav Shacham, and Stefan Savage, "Experimental Security Analysis of a Modern Automobile," Institute of Electrical and Electronics Engineers (IEEE) Symposium on Security and Privacy, 2010, pp. 447-462; Karl Koscher, Alexei Czeskis, Franziska Roesner, and Tadayoshi Kohno, "Comprehensive Experimental Analyses of Automotive Attack Surfaces," San Diego, CA: Center for Automotive Embedded Security Systems, 2011, available from *autosec.org/pubs/cars-usenixsec2011.pdf*.

6. Andy Greenberg, "Hackers Reveal Nasty New Car Attacks--With Me Behind the Wheel," *Forbes*, August 12, 2013, available from *forbes.com/sites/andygreenberg/2013/07/24/hackers-reveal-nasty-new-car-attacks-with-me-behind-the-wheel-video/*, accessed on October 2, 2014.

7. Stephen Edelstein, "Future Fords May Steer Owners Out of Traffic Jams," June 28, 2012, available from *digitaltrends.com/cars/future-fords-may-steer-owners-out-of-traffic-jams*, accessed on October 2, 2014.

8. *Ibid.*

9. Isaac Porche, Kwang Soo Chang, William Li, and Pravin Varaiya, "Real-Time Task Manager for Communications and Control in Multi-Car Platoons," Proceedings of the SAE and IEEE Intelligent Vehicles Conference, Detroit, MI, June 1992, pp. 409-414.

10. Stephen Checkoway, Damon McCoy, Brian Kantor, Danny Anderson, Hovav Shacham, Stefan Savage, Karl Koscher, Alexei Czeskis, Franziska Roesner, and Tadayoshi Kohno, "Comprehensive Experimental Analyses of Automotive Attack Surfaces," San Diego, CA: Center for Automotive Embedded Security Systems, available from *autosec.org/pubs/cars-usenixsec2011.pdf*, accessed on October 02, 2014; and Koscher *et al*., "Experimental Security Analysis of a Modern Automobile," pp. 447-462.

11. Checkoway *et al*.

12. Ronald W. Cox, "Local Area Network Technology Applied to Automotive Electronics Communications," *IEEE Transactions on Industrial Electronics*, Vol. IE-32, No. 4, November 1985, pp. 327-333.

13. "CAN History," *CAN in Automation*, available from *cancia.de/index.php?id=161*, accessed on October 2, 2014.

14. According to its supporting cooperative (e.g., Audi, Daimler, BMW, and others), MOST (media oriented systems transport) is "the de-facto standard for multimedia and infotainment networking in the automotive industry." MOST Cooperative, available from *mostcooperation .com/home/index.html*, accessed on October 2, 2014.

15. Robert Leale, "CanBusHack," undated, available from *canbushack.com*, accessed on October 2, 2014.

16. Kevin Poulson, "Hacker Disables More Than 100 Cars Remotely," Wired, March 17, 2010, available from *wired.com/threatlevel/2010/03/hacker-bricks-cars/*, accessed on October 2, 2014.

17. Koscher *et al*., "Experimental Security Analysis of a Modern Automobile," pp. 447-462.

18. Greenberg, p. 1.

19. Telematics is a widely used industry term relating to information technology functions being integrated into automobiles, e.g., navigation systems. See *telematicsresearch.com/PDFs/TRG_ITSWG-Telematics.pdf,* which associates the term with "solutions [i.e., capabilities] based on information flowing to and/or from a vehicle."

20. See discussion at *unix.org/what_is_unix/history_timeline.html*.

21. Bruce Schneier, "The Multics Operating System," September 19, 2007, available from *schneier.com/blog/archives/2007/09/the_multics_ope.html*, accessed on October 2, 2014.

22. Paul Karger and Roger Shell, "Thirty Years Later: Lessons from the Multics Security Evaluation," available from *acsac.org/2002/papers/classic-multics.pdf*, accessed on October 2, 2014.

23. This is according to an interview conducted by Peter Seibel, *Coders at Work: Reflections on the Craft of Programming*, New York: APress Publications, 2007.

24. J. D. Tygar, and Alma Whitten, "Why isn't the Internet Secure yet?" *ASLIB Proceedings*, Vol. 52, No. 3, March 2000, pp. 93-97.

25. Edward Fok, "An Introduction to Cybersecurity Issues in Modern Transportation Systems," *ITE Journal,* No. 7, July 2013, p. 18.

26. *Ibid.*

27. *Ibid*.

28. Shan Carter, and Amanda Cox, "One 9/11 Tally: $3.3 Trillion," *The New York Times*, September 8, 2011, available from *nytimes.com/interactive/2011/09/08/us/sept-11-reckoning/cost-graphic.html?_r=0*, accessed on October 2, 2014.

29. Edward A. Lee, "Cyber-Physical Systems—Are Computing Foundations Adequate?" 2006, available from *ptolemy.eecs.berkeley.edu/publications/papers/06/CPSPositionPaper/*, accessed on October 2, 2014.

30. Qaisar Shafi, "Cyber Physical Systems Security: A Brief Survey," 12th International Conference on Computational Science and its Applications, 2012, available from *ieeexplore.ieee.org/xpl/articleDetails.jsp?arnumber=6257627*, accessed on October 2, 2014.

31. Alberto Sangiovanni-Vincentelli, "Cybersecurity for the Automobile: Is the Car of the Future Still a Car?" presented at I&C Research Days, Lausanne, Switzerland, June 21, 2012, available from *ic.epfl.ch/files/content/sites/ic/files/pdfs/Presentations%20RD%202012/A.Sangiovanni.pdf*, accessed on October 20, 2014.

32. Fok, p. 18.

33. Brooks Hays, "Federal officials want to beef up cybersecurity for motor vehicle communication systems," Gimby.org, May 23, 2013, available from *gimby.org/blogs/gimby-news-focus/20130523/federal-officials-want-beef-cybersecurity-motor-vehicle*, accessed on May 23, 2012.

34. Jim Finkle, "Insight: Experts hope to shield cars from computer viruses," Reuters, August 20, 2012, available from *reuters.com/article/2012/08/20/us-autos-hackers-idUSBRE87J03X20120820*, accessed on October 2, 2014.

35. Isaac Porche, Jerry Sollinger and Shawn McKay, "*A Cyberworm that Knows no Boundaries*," Santa Monica, CA: RAND Corporation, 2011.

36. Kashmir Hill, "When 'Smart Homes' Get Hacked: I Haunted a Complete Stranger's House Via the Internet," *Forbes*, July, 2013, available from *forbes.com/sites/kashmirhill/2013/07/26/smart-homes-hack/*, October 2, 2014.

37. "Pirates of Cyberspace," *The Telegraph*, March 10, 2013, available from *telegraphindia.com/1130310/jsp/7days/story_16654680.jsp#.U2E41PldX_E*, accessed on October 2, 2014.

PART III

RESPONDING TO THREATS IN CYBERSPACE

CHAPTER 12

REFLECTIONS ON CYBERDETERRENCE

Martin Libicki

INTRODUCTION

In April 2007, General James Cartwright, then head of the Strategic Command, testified that in cyberspace, as with any other warfighting domain, the best defense was a good offense. Accordingly, he asked Congress to support his belief that the United States should develop an offensive cyberwar capability whose purpose was to discourage other countries from attacking the United States in cyberspace.

By way of response, *Cyberdeterrence and Cyberwar* was written. The monograph argued that many problematic aspects of retaliation, notably (but not exclusively) the difficulties associated with attributing attacks, meant that the threat of retaliation and, therefore, cyberdeterrence, could not be expected to play a strong role in defending the United States from cyberattack. This was not the same as arguing that the United States should never retaliate. Nor did it refute the claim that the general tendency of the United States to react harshly to sufficient provocation (e.g., Pearl Harbor, HI, on December 7, 1941, the Twin Towers, NY, on September 11, 2001 [9/11]) would inhibit sufficiently damaging cyberattacks. General statements that the United States reserves the right to respond to a cyberattack with retaliation[1] are quite defensible positions. Yet, the doubts introduced by this and similar arguments seemed to weaken the logic for building a deterrence capability.

Alas, in Washington, debates rarely really resolve issues; they tend to linger and recur until they are overtaken by events in the real world. Consider, for instance, the following report given mid-testimony in March 2013:

> The chief of the military's newly created Cyber Command told Congress on Tuesday that he is establishing 13 teams of programmers and computer experts who could carry out offensive cyberattacks on foreign nations if the United States were hit with a major attack on its own networks, the first time the Obama administration has publicly admitted to developing such weapons for use in wartime.[2]

Now, it is entirely possible that these teams may also be used, and their construction perhaps motivated, for offensive operations that have nothing to do with any preceding cyberattack against the United States (e.g., U.S. policy considers attacks on dual-use infrastructure fair game in war such as the operations against Baghdad's electric power supply in 1991 and 2003). Nevertheless, the notion of building up a deterrence capability must still have some resonance to be cited publicly as a rationale.

So, matters have not been settled. Yet, since cyberspace never stops evolving, it may be worthwhile reviewing the case for and against cyberdeterrence to see what has changed.

We consider four issues. The first is whether the assumption that attribution is difficult still holds, and, if not, whether the case for a deterrence policy has flipped from probably-not to certainly-yes. The second is whether deterrence can work when the issue is not one of keeping an attack from taking place but stopping another country from carrying out

obnoxious acts in cyberspace. The third is whether true attribution is all-important in comparison to satisfying third parties (which may include potential attackers in cyberspace) that the attacker being identified is the right one. The fourth asks why attribution should discourage a deterrence policy for a cyberattack when similar attribution problems may plague other types of attack—in this case, a suitcase nuclear bomb—in which the rightness of a deterrence policy is generally accepted.

ATTRIBUTION IS GETTING BETTER, ISN'T IT?

Former Defense Secretary Leon Panetta, in mid-October 2012, observed:

> In addition to defending the department's networks, we also help deter attacks. Our cyber adversaries will be far less likely to hit us if they know that we will be able to link to the attack or that their effort will fail against our strong defenses. The department has made significant advances in solving a problem that makes deterring cyber adversaries more complex: the difficulty of identifying the origins of that attack. Over the last 2 years, Department of Defense has made significant investments in forensics to address this problem of attribution and we're seeing the returns on that investment.[3]

The consensus of observers is that attribution **is** getting better. So, what does that do to the cyberdeterrence argument?

The answer of "not so much" is a nuanced one. First, is that a **credible** declaration that attribution exists usually works to the advantage of defenders, irrespective of how important deterrence is within the

entire panoply of defensive measures. It is human nature that saying something is true tends to be correlated up to a point with others believing that it is true. The urge to ask whether flexing muscles is what people do when they lack the real muscles to flex (e.g., are North Korea's newly belligerent statements circa March 2013 an attempt to substitute the appearance of greater will for the reality of stagnant capability?) does not really apply in the case of deterrence. In that case, to paraphrase *Dr. Strangelove*, it is pointless to have such a capability if it is not talked about.

The problem for deterrence comes when an attack actually takes place. The stronger the statement about how well a cyberattack can be attributed, the harder it is to suffer an attack and not retaliate without causing observers to wonder why no retaliation followed. Perhaps the attack did not cross a red line—in which case, where **is** the red line? Perhaps, alternatively, the country that had to decide on retaliation does not have the stomach for retaliation given the likelihood of counter-retaliation; alternatively, it lacks a capability for retaliation (hard to believe in the case of the United States). Finally, deterrence may have been a bluff all along. Note that the more unambiguously the red line is stated, the more that observers will have to conclude that the third reason—it was all a bluff—provided the true explanation of why no retaliation followed the attack.

Risking being called out on a bluff is the price a country pays for the benefits of posing a deterrence policy that it is not prepared to back up. This, then, puts all of a country's **other** deterrence policies in play—and if its nuclear retaliatory policy is cast into serious doubt, the only other defense the United States has against the nuclear threat is the iffy capa-

bility of its missile defense shield. After all, the entire Cold War was fought without any country calling any other country's bluff[4]—despite serious questions about whether any sane country would retaliate in full against a nuclear attack that destroyed something if, by retaliating, it would risk the destruction of everything. No one really wanted to call anyone's bluff in the nuclear arena, because the price of being wrong was catastrophic. Catastrophe is nowhere near such a threat in a cyberwar; hence, it is a testable proposition unless the attacking country fears that a U.S. response could ultimately escalate to the nuclear level (a prospect not to be dismissed casually).[5] Bluffs may well be called.

So, can the United States actually achieve good attribution? It is hard to say (from the outside). The United States Cyber Command exudes confidence (which has to count for something), but it has yet to prove an attribution in a court of law, or even the court of public opinion. A better perspective may arise from understanding exactly what is being attributed. There is fairly high confidence within the global cybercommunity (apart from China's) that attacks that are popularly attributed to China, in fact, arise from China. However, one of the reasons for such reliable attribution is that Chinese attackers keep carrying out similar attacks, persist for a long time within target systems, exfiltrate a large quantity of data back, and seem to exercise very poor operational security because they act as if they are immune from punishment. Indeed, they individually should fear no consequences as long as their activities are condoned, or, as argued in the Mandiant report,[6] carried out by the government.

Each of these four characteristics—repetition, persistence, exfiltration, and impunity—makes attribu-

tion easier. Repetition means that characteristics of earlier attacks can be matched against later ones that have been attributed to the same source; the more attacks, the more likely that they will leave incriminating clues (not least of which is attacking a target, such as the Free Tibet movement, that is of interest to only one state).[7] Persistence means that communications between the attacker and the target frequently recur, even through potential changes in the attacker's masquerading activities.[8] Exfiltration, particularly in large quantities, means that there is a route from target to the attacker that is traversed by large volumes of data; even if individual volumes are kept small to avoid triggering suspicion (and that step is often skipped), then the frequency correspondingly must be greater. Finally, the aura of impunity (discussed further) means that attackers can afford to get sloppy or may be willing to trade the possibility of ultimate attribution to gain a higher degree of assurance that they can get their files and do so quickly.

Now compare such attributes to the attributes of something that was a destructive cyberattack, Stuxnet. With Stuxnet, the number of attacks was in low single digits. There was very little if any, communication between the malware and the controller, although there appears to have been some updating activity. There was no exfiltration of large files, and the authors of Stuxnet seemed to have taken some pains not to be discovered. However, that depends on whether the clues in the code were put there deliberately.[9] At the time of discovery, there were no forensic clues that definitively linked Stuxnet to any country. The assumption that the United States and Israel were behind Stuxnet was based on the sophistication of the code and the presumption that no other two countries were as motivated to hobble Iran's nuclear program.[10]

In other words, a one-time fire-and-forget attack[11] by a country that actively wanted to avoid blame offers different and far less promising attributes for attribution than a repeated persistent intrusion set whose aim is to exfiltrate large amounts of data.[12] Therefore, advances in attribution associated with the latter may not necessarily mean that attribution against the kind of cyberattack that would merit retaliation has gotten significantly easier.

RESPONDING TO PERSISTENT ESPIONAGE

The standard case for deterrence assumed that what was to be deterred was an attack—something that might be considered tantamount to an act of war, something the United States (or its major allies) had yet to encounter. Espionage was considered different—every nation that can does it, it has been carried out for, literally, millennia, and has never been considered a proper *casus belli*.

Rising tensions between the United States and China (circa early-2013) suggest that this assumption does not complete the discussion. The United States has called out the Chinese Government for condoning, abetting, and, more recently, conducting economically motivated cyberespionage (EMCE). The U.S. claimed that (1) such cyberespionage has no national security rationale. (2) is not done by other states, (3) contravenes the spirit, if not the script, of trade agreements that China has signed, and (4) is taking place in such large quantities that it has become, in Hegelian fashion, something entirely different in quality. The U.S. *International Strategy in Cyberspace* (2011) hinted that such behavior was off limits; later that year the United States named China as an EMCE threat.[13] Shortly after

the Mandiant report was issued, the U.S. Government issued its *Administration Strategy of Mitigating the Theft of U.S. Trade Secrets*. This was followed by a tough speech by National Security Advisor Tom Donilon,[14] and Treasury Secretary Jack Lew was dispatched to China, in part to reinforce this point.

Let us, therefore, suppose that the United States is prepared to do more than talk (as events after this monograph may bear out). What would we be asking China to do? How likely is it that the United States would succeed? What risks would be run in trying (or succeeding)?

Attribution, one would imagine, is less of a problem—at least in the sense that few Americans think that China is **not** carrying out EMCE. So, the fear that the wrong perpetrator is being identified is next to nonexistent. However, in a world in which everyone spies on everyone else, and where countries other than China seem to be carrying on EMCE—e.g., Russia, perhaps France and Israel—the issue is not who is doing it, but who is doing too much of it. China's initial reaction to being accused is not to deny that no Chinese has ever penetrated the network of a U.S. corporation, but that China, itself, is a victim of cyberespionage in great quantities coming from the United States. Furthermore, to quote Qian Xiaoqian, a vice minister and deputy director of the State Internet Information Office:

> Our opposition to all forms of hacking is clear and consistent . . . Lately people have been cooking up a theory of a Chinese Internet threat, which is just an extension of the old `China threat' and just as groundless.[15]

To paraphrase: our accusers never liked us anyway. Furthermore, many Chinese say they believe that the United States carries out EMCE even if China has yet to announce publicly an incident that traces back to U.S. complicity, as well as the many attacks on U.S. organizations that can be traced back to China and appear to be condoned, if not supported by the Chinese Government. Indeed, the Chinese, in fact, may believe as much. This point is the downside for the United States of having such a vaunted reputation for good operational security (OPSEC). The absence of evidence does not equate as well to evidence of absence, as it might for a country (such as China) whose OPSEC is weaker.

The release of the detailed Mandiant report was fortuitous for the U.S. intelligence community, which had been arguing for years that the Chinese were carrying out EMCE, but were quite reluctant to release the evidence that would make the case to those outside their reporting chain. From time to time, some very interesting pieces of information would leak out. In late-2011, for instance, one such tidbit was the conclusion that most of the EMCE was carried out by 12 specific Chinese outfits.[16] The point of amassing evidence would not be to prove that China carries out a great and disproportionate amount of EMCE—because establishing as much requires a great volume of evidence. Furthermore, to some extent, it would be trying to prove a negative: that states that other countries do not conduct EMCE, or, if so, far less. Instead, the point would be to amass enough of a case to establish China's unwillingness to prosecute hackers that attack foreign systems. It may not be necessary to amass enough evidence to prove a case against a particular individual. The revealed data is anyway much better

at indicating which country the attack originated from than it is at saying which individual carried out the attack. But enough does have to be proven, again, to establish China's unwillingness to investigate hackers that attack foreign systems—unless, of course, China goes ahead and does exactly that.

If the intelligence community, however, does not want to make its information public, then building **popular** pressure behind or, at least, the acquiescence of those not briefed by the intelligence community to, potentially risky confrontational strategies will be that much harder. The credibility of the intelligence community took a beating over the Iraq War, and it may not have fully recovered.

If we ignore the problem of attribution, and posit that the solution is demonstrable to others once certain steps are taken, then the leftover problem is one of defining a standard for appropriate behavior, and some response threshold that both sides agree is legitimate. The United States undoubtedly carries out national security-related cyberespionage, deems it legitimate, and cannot reasonably ask that others abjure cyberespionage as a matter of principle (it could respond unilaterally by kicking out the ambassador, but it can do that for any reason or no reason at all). The question then becomes what is the boundary between national security-related cyberespionage and other and presumably less well-legitimized EMCE. This distinction carries several problems. First, it is by no means clear that China deems the distinction as important as does the United States.[17] Second, what constitutes national security for China may not necessarily be viewed the same way in the United States. Chinese apparently carried out cyberespionage against *The New York Times* because a reporter for the latter wrote that the family

of Wen Jiabao (China's prime minister at the time) had amassed an unexpectedly large amount of money.[18] To a state that fears popular agitation over having their officials exposed as corrupt, this is a national security matter; to the United States with its first amendment, not at all. A narrower case may be China's purported penetration of Lockheed's F-35 production works.[19] Its legitimacy as national security cyberespionage rather than EMCE may rest on exactly why China wanted the information. The national security component is most clear if China was trying to figure out the aircraft's performance characteristics so it could assess the threat that such a jet may pose to its air defenses. A characterization as national security cyberespionage is also probably defensible if China's purpose were to look for vulnerabilities in the F-35 that Chinese weapon systems could exploit. Moreover, it would still be somewhat defensible if its purpose was to steal technologies for use in its own weapons systems—but probably over the line if the primary purpose was to make better aircraft that it would then sell in competition with U.S. sales of the F-35. However, since the last is unlikely, the case that mutual abjuration of EMCE would prevent China from trying to steal the secrets from producers of military aircraft is probably hard to make. Indeed, national security may even cover China's penetration of Google's networks to the extent that its purpose was to uncover the email of dissidents rather than steal Google's source code (it was probably both).

When it comes to EMCE, however, there is another difficult feature—the Chinese may gain more than the United States loses. One can imagine situations in which both the United States and China conclude that both sides would be better off if neither were to steal—

which is to say, copy—intellectual property from one another. Neither would need to spend so much money on cyberdefense, and the returns to the effort to generate intellectual property would be higher since both sides would get unique possession of what they had generated (in some cases, invented). But that world is not here yet: U.S. companies have a lot more intellectual property than their Chinese counterparts do; far more Chinese read English than Americans read Chinese; and the *de facto* legal basis for carrying out EMCE (including passing files to private companies) is much more accommodating in China than it is in the United States. Today's EMCE (especially when it is used to transfer intellectual property rather than proprietary business data) can be seen as illicit technology transfer—but technology transfer nonetheless. U.S. companies are not deprived of its use (they are deprived of its **exclusive** use). The Chinese, for their part, learn something they would otherwise have not learned (or at least not so easily). U.S. firms can still convert the usual production factors into value-added at the same rate, but Chinese firms can now convert such production factors into value-added at higher rates than they could have prior to benefitting from EMCE. The second-order effects may well be negative for the United States; for instance, Chinese production could displace U.S. exports, but what U.S. producers lose, Chinese producers gain (and consumers of whatever product the United States and China compete in also gain). Granted, there may be additional deadweight losses (as economists call it) for U.S. corporations if they have to spend more on cybersecurity in a newly insecure world, or if U.S. firms cut back on research and development that they would have carried out were they confident in being able to realize

the unhampered flow of income that such intellectual property produced. Even so, Chinese interests, quite plausibly, gain more than U.S. interests lose at this point.

It is difficult to eradicate a practice, regardless of how obnoxious, in which the winners gain more than the losers lose. Were it otherwise, it would be possible for the losers to bribe the winners to quit. Yet, if China gains $2 and the United States loses $1 from EMCE, any offer less than $2 to China (so that it henceforth would behave) will be rejected as insufficient, and any offer more than $1 will be irrational on the U.S. part.[20] The possibility that China gets more out of EMCE than the United States loses says that the United States cannot offer something (e.g., a more relaxed attitude about the sales of Chinese equipment into the national communications infrastructure) to China to get it to stop—but that something has to be worth a lot more to China than giving it over costs the United States.

That leaves confrontation, in which the United States tries to get China to abandon its EMCE or face consequences. One line of consequences is that the continuation of EMCE will imperil U.S. friendship, which our government would have to presume is worth more to the Chinese than whatever the Chinese would gain from EMCE. Perhaps needless to say, anything that imperils China's relationship with the United States will almost certainly imperil the U.S. relationship with China. Such a threat would have a better chance of working against a small and weak China than it does against today's China, whose gross national product (GNP) is approaching the U.S. GNP. But that does not yet mean that a full-fledged confrontation with China will see the United States yield before China is ready to yield, either. That China might

value the spoils of EMCE more than the United States loses does not mean that China would win a confrontation—a lot depends on who is more stubborn and who has the greater need to demonstrate that it cannot be pressured. In the end, the threats wielded may greatly exceed the value of whatever it was the threats were originally about (after all, how valuable are the Senkaku/Diaoyudao Islands anyway?).

ATTRIBUTION: WHO NEEDS TO KNOW?

The Chinese also have a wonderful aphorism about killing the chicken to scare the monkeys, something that speaks to the importance or lack thereof in constructing a cyberdeterrence policy. In a world in which the United States has, at least, two potential opponents, one of the purposes of a deterrence policy is to put other potential opponents on notice that they cannot act with impunity. Presumably, accurate attribution is part of this equation. If the third party believes that the target of U.S. retaliation is not the attacker, it may conclude that carrying out a cyberattack is only weakly correlated with the risk of suffering retaliation.

The more important lesson is that being on bad terms with the United States when the United States has just suffered a major cyberattack is a bad idea. If being on bad terms is something the third party cannot or will not do much about, then even a misguided act of retaliation by the United States provides a reason to see to it that your own people are not the reason that the United States has become very angry. That is, even if the U.S. capability for attribution is weak, carrying out an attack on the United States may yield the pain of retribution because the United States is predis-

posed to make assumptions about the attack that are biased against you. In theory, it should also motivate you to suppress the desire of other U.S. foes to carry out such cyberattacks as well, but this assumes that foes of the United States are allied with one another, which, despite the connotations of the term "axis of evil," is probably far-fetched.

If retaliation for a cyberattack also comes via a cyberattack of its own, the weeks and months required to generate such an attack will bias any retaliator toward responding to its past foes—that is to say, those it has already made plans to retaliate against. This bias is enhanced if the retaliator feels pressure to retaliate quickly (which is characteristic of retaliation as an element of crisis management) rather than wait until enough evidence is in (which is characteristic of retaliation as the administration of justice). By contrast, if the retaliation is kinetic, such as a bombing run, such actions can be easily be generated within days.[21] Although the notion of retaliating against a state based, in part, on having the attack in place seems like looking for one's keys under the lamppost, both approaches can be rational as long as they are understood to be parts of more sophisticated calculations.

A corollary observation is that whom third parties think did it may not necessarily equate to who actually did it. This works both ways: third parties may not believe the case that the United States (as victim and investigator) builds; in other circumstances, third parties (perhaps the same third parties) may buy a weak case presented by the United States that should not convince them, but does anyway. There will also be the occasional third parties that will choose to believe that a particular country (usually one they, themselves, do not like) was the source of the attacks regardless of what the United States says.

Which third parties, then, matter? Some third parties (which should include U.S. citizens disinclined to take the government's say-so on such matters) have no interest in carrying out cyberattacks and have no great fear of them, but are interested in the justice (or lack thereof) of U.S. retaliation as well as the likelihood that retaliation, especially unwarranted retaliation, will mire the United States in conflict. Other third parties are less interested in justice but want to know how the United States may respond as a way of judging U.S. seriousness about cyberattacks. Some such states are allies and wonder if the United States would come to their defense if their only complaint is having come under cyberattack from another country (rather than cyberattack being an element of a broader offense). Other such states are potential foes, and wonder if they can escape retaliation because the United States is afraid to start a fight in a medium where the attacker has little to lose, but the United States has a great deal to lose.

These considerations can rightfully be factored into the decision to retaliate. To wit: an objectively weak case for attribution, which is nevertheless believed to be strong by potential attackers, may be good enough to justify retaliation. However, two practical considerations merit note. First, as hard as it is to make a good confidence estimate (that X did it) for oneself based on evidence, it is harder to determine what confidence estimates others have come up with.[22] There is the normal human tendency to mirror image others (if I am convinced, then the case is convincing, and thus they should be convinced), for lack of a better alternative. The other consideration is the tendency of attribution estimates to get better over time (even if complete certainty is forever elusive). Thus, a strategy that advises

in favor of retaliation on the theory that others will place unwarranted confidence in your powers of attribution may look good in the short run but not so good in the long run when more facts are known. Whereas this short run applies largely to the will of the United States to oppose cyberattacks, the reputation of the United States, in general, will be what survives into the long run. The longer the odds that cyberattacks are a temporary artifact of today's incompletely secured software, the less important the former vis-à-vis the latter.

MAYBE IFFY ATTRIBUTION IS NOT THE REAL COUNTERARGUMENT TO A DETERRENCE POLICY

A professional colleague of mine, who is far more hawkish on cyberdeterrence than I am, posed an interesting question that inadvertently touched a core principle associated with the problem of cyberdeterrence: the importance of attribution or lack of confidence therein.

Consider the suitcase nuclear bomb delivered to a U.S. city and detonated. Technical attribution, he argues, can be quite difficult, not least because such a bomb could wipe out all the hardware associated with its composition (hence origin) and placement. Yet, there is no doubt in anyone's mind that the United States would retaliate, and harshly if it found the perpetrators. Conversely, no one would quibble over whether the United States would announce as much.[23] Why should a cyberattack be any different?

Upon further contemplation, I found it possible to generate a few critical distinctions, but whether they were decisive enough is something left to the reader.

Regrettably, they did not necessarily convince me, which leads into the second part of the argument. **First**, there are reasonable grounds that attribution will get continuously better as time progresses after a suitcase nuclear detonation, whereas such grounds do not exist as strongly for a cyberattack of comparable scope (if not necessarily comparable effect). The difference between the two is that a cyberattacker that does not want to be tagged could adopt the ruse of looking like another known purveyor of mischief in cyberspace. Since the governments of many countries have suffered cyberattacks by many other countries, they have a great deal of evidence that allows their cyberattacks to look like a cyberattack carried out by someone who attacked them in the past. With a suitcase nuclear bomber—something that would be unprecedented—no such knowledge exists. The best forensics rely on the post-detonation pattern of radiation and fallout debris, but duplicating the patterns of another country may be impossible without having gotten hold of another country's device (or the fallout from a recent test of theirs). Thus, with suitcase nuclear attacks, attribution will only get better, with a reasonable promise of inevitable judgment. With cyberattacks, they may plateau without the target being able to dispel the notion that the faux attacker set up by the real attacker is actually the real attacker. Furthermore, there are a lot fewer plausible candidates to play the role of the attacker for a suitcase nuclear weapon than there are for a cyberattack.

Second, forensics on the weapon or at the scene of the explosion are only a small part of how we track terrorists (figuring out where the box cutters for the 9/11 attacks were bought did not play a major role in the investigation). The full range of police meth-

ods is used, and for non-nuclear terrorists, that sort of investigation pays fairly good dividends. Terrorists who used a suitcase nuclear weapon are likely to have characteristics more similar to that of other terrorists than cyberattackers would (today's terrorist groups still do not carry out many cyberattacks). This is another way of saying that the difficulty of using forensics for a suitcase nuclear bomb has little to do with the ability to attribute an attack; to wit, the odds of attribution are, therefore, higher with the suitcase nuclear weapon.

Third, a suitcase nuke requires a larger infrastructure to pull off than a comparable cyberattack does. Such people have to interact with the rest of the world by traveling, moving objects, casing the detonation site, and perhaps by purchases. By interacting with the rest of the world, the chances that investigators will get a break are far higher than they would be in a cyberattack, where the only thing that moves is code and little, if anything, need be bought.

Assuming that all three arguments hold water, they suggest that the odds of finding the perpetrator of a suitcase nuclear weapon would be higher than the odds of finding the perpetrator of a comparably broad cyberattack. Nevertheless, are the odds different enough to justify certainty that a deterrence posture makes perfect sense in the case of the former, but dubious sense in the case of the latter? Perhaps they are not. So, let us dig further.

Fourth, because the seriousness of detonating a suitcase nuclear weapon is likely to far exceed the seriousness of carrying out a cyberattack, it is much more plausible to hunt down anyone who had **any** culpable role in the former. By contrast, whereas many people could have a comparable role in the latter (e.g., by

exchanging information on hacking techniques with the attackers), the moral taint in the latter case is unlikely to be large enough to merit hunting them down for prosecution.

That argument, however, tends to be less about deterrence and more about criminality (even if it could be applied to states that aided and abetted the detonators)—e.g., implicating Pakistan for A. Q. Khan's help to the Democratic Peoples' Republic of Korea rather than deterring a North Korean attack. It is perfectly permissible to argue that certain crimes have no statute of limitations and that, while justice grinds slowly, it grinds fine—in both cases. The aura of criminal deterrence legitimately can widen for a more heinous crime, but this does not necessarily speak to the wisdom of strategic deterrence, at least not yet.

Another approach is to basically shrug and argue that we can no more rely on **strategic** (vice criminal) deterrence to ward off a nuclear threat than we can in the case of cyberattack. In the former, a plausible approach to minimize the threat is to go after the many precursor steps to detonating a suitcase device (e.g., by rounding up loose nuclear material), concentrating fire on terrorist groups with an interest in such devices, and closely monitoring states (North Korea? Someday Iran?) with a nonzero interest in planning such a device. Against cyberattacks, the best methods are defensive ones (whereas defenses against a nuclear detonation are nonexistent, although there are resiliency and recovery methods). Finally, whereas the deterrence of nuclear actors with the conventional delivery means (e.g., missiles) is reason enough for the United States to have a nuclear deterrent, there may be no good argument for having an offensive strategic cyberwar capability other than to retaliate for similar attacks.

On the other hand, perhaps the real reason that a deterrence policy may make sense against suitcase nuclear detonations, but not cyberattacks, has essentially nothing to do with attribution. In both cases, the United States would pursue individuals who did it without much regard for any statute of limitations, just as it pursued the bombers of PanAm 103 (Lockerbie). In both cases, if a state were deemed ultimately responsible, then the act would be considered quite hostile and would justify corresponding treatment by the United States of such a country. However, if a country were found responsible for detonating a nuclear weapon inside the United States, it would be hard **not** to consider such a detonation an act of nuclear war that would merit even nuclear retaliation. If U.S. nuclear weapons cannot be contemplated as retaliation for such actions, for what actions **can** they be contemplated? If the answer is none, what was the point in having them? Indeed, what is the point of having **any** retaliation policy? Furthermore, what would then keep any nuclear power from attacking the United States with impunity?

However, with a cyberattack, different considerations come into play, not least of which is whether it is worthwhile making this a *casus belli*. Retaliation meant to convey great ire at having been attacked may lead to counter-retaliation, which may set off a cycle of tit-for-tat which might stay in cyberspace, or might not. This consideration is not an argument against establishing a deterrence policy, but it is a caution. Consider the question: is retaliation, if only to bolster deterrence, the most cost (and risk) effective way to reduce the future threat? In nuclear deterrence, it appeared to be the only way, and a suitcase nuclear weapon is essentially the same problem albeit with

a different delivery mechanism. But with a cyberattack, there are many other options to consider. Some of them are reactions that are outside the definition of hostilities, but are hardly friendly: organized trade sanctions, or kicking them off the Internet. Some of them focus, not on the attacker but on improving the defenses of U.S. systems so that a similar attack next time either fails or is not so devastating.

So, we return to the core dilemma of any deterrence policy—worthwhile as long as it serves to reduce the odds that others will misbehave, but problematic if it has to be carried out, particularly against a country with the capability to strike back. With a suitcase nuclear bomb, the prospect of retaliation ought to be so painful that deterrence should hold—as it has since 1949. With a cyberattack, the many ambiguities associated with it—thresholds, responsibilities, and, yes, attribution—mean that the assumption that deterrence will always hold cannot be assumed. The consequences of carrying out retaliation have to be considered. Because cyberattacks sit toward the bottom rather than the top of the escalation ladder, such consideration may argue against a deterrence policy for a cyberattack while not affecting the wisdom of a deterrence policy for a suitcase nuclear weapon attack.

CONCLUDING THOUGHTS

Policies are children of their time and place. When the circumstances change, and the assumptions that bolstered policies change, their reconsideration may have merit. When new considerations are brought into play, their reconsideration may also have merit. The initial presumptions on the author's part that deterrence really would not work for cyberattacks and, therefore, should not be an arrow in the U.S. strategic

quiver is also a child of its time and place. This chapter has examined two new circumstances and two new considerations against the original argument. It has tried to show that, while they may cause the original argument to bend, it is not clear that they cause it to break.

ENDNOTES - CHAPTER 12

1. *International Strategy for Cyberspace*, Washington. DC: The White House, 2011, p. 14:

> When warranted, the United States will respond to hostile acts in cyberspace as we would to any other threat to our country. . . . We reserve the right to use all necessary means—diplomatic, informational, military, and economic—as appropriate and consistent with applicable international law, in order to defend our Nation, our allies, our partners, and our interests.

2. Mark Mazzetti and David Sanger, "Security Leader Says U.S. Would Retaliate Against Cyberattacks," *The New York Times,* March 12, 2013, available from *nytimes.com/2013/03/13/us/intelligence-official-warns-congress-that-cyberattacks-pose-threat-to-us.html*.

3. Leon Panetta, "Remarks by Secretary Panetta on Cybersecurity to the Business Executives for National Security, New York City," LawFare, October 11, 2012, available from *https://www.lawfareblog.com/secdef-panetta-speech-cybersecurity*.

4. See, for instance, Evan Thomas, *Ike's Bluff: President Eisenhower's Secret Battle to Save the World,* New York: Little Brown and Company, 2012.

5. *The Defense Science Board Task Force Report on Resilient Military Systems and the Advanced Cyber Threat* at one point argues: "Cyber risk can be managed through the combination of deterrence (up to a nuclear response in the most extreme case) and improved cyber defense." Washington, DC: Defense Science Board, 2013, p. 32.

6. Mandiant, *APT 1: Exposing One of China's Cyber Espionage Units*, available from *intelreport.mandiant.com/*, released February 2013.

7. Shishir Nagaraja and Ross Anderson, *The Snooping Dragon: Social-Malware Surveillance of the Tibetan Movement*, Technical Report No. 746, Cambridge, UK: University of Cambridge, Computer Laboratory, March 2009.

8. Note another benefit that persistence yields to attribution. Marc Ambinder, "Inside the Black Box," *Foreign Policy*, March 13, 2013, available from *foreignpolicy.com/articles/2013/03/06/inside_the_black_box*:

> For years, and in secret, the NSA has also used the cover of some American companies—with their permission—to poke and prod at the hackers, leading them to respond in ways that reveal patterns and allow the United States to figure out, or 'attribute,' the precise origin of attacks.

9. E.g., was the reference to "Myrtus" in the Stuxnet code, a wink at the Biblical character Esther (under her name of Myrtle) or did it stand for My RTUs (RTU = remote terminal unit)?

10. It took later discovery of the fact that modules of the Flame worm (and to a lesser extent, the Duqu malware) resembled modules of the Stuxnet worm (and were written earlier) coupled with the pattern of its distribution within the Middle East before there were technical forensics to link Israel to Stuxnet.

11. As a general rule, any penetration attack will be preceded by some surveillance, which may offer some prospect for attribution even if the attack, itself, does not. However, the quantity of surveillance may be much less than what is associated with an advanced persistent threat.

12. It also makes a difference that China has been studied for at least 10 years and few other countries have had that level of scrutiny.

13. "Foreign Spies Stealing National Economic Secrets in Cyberspace," Washington, DC: Office of the National Counterintelligence Executive, November 2011.

14. Mark Landler and David Sanger, "U.S. Demands China Block Cyberattacks and Agree to Rules," *The New York Times*, March 12, 2013, available from *nytimes.com/2013/03/12/world/asia/us-demands-that-china-end-hacking-and-set-cyber-rules.html*.

15. See *https://www.yahoo.com/news/us-says-hacking-undermines-chinas-interests-093148708.html?ref=gs;* see also *chinadaily.com.cn/china/2013-04/10/content_16388107.htm*.

16. Lolita Baldor, "A few hacker teams do most China-based data theft," *The Washington Times*, December 12, 2011, available from *washingtontimes.com/news/2011/dec/12/few-hacker-teams-do-most-china-based-data-theft/?page=all*. The Mandiant report suggested (1) that these hacker teams could individually actually number thousands of individuals, and (2) the true number may be closer to 20 rather than 12.

17. "They say that the topic of economic espionage is 'embarrassing' for them," said James A. Lewis, a cybersecurity expert at the Center for Strategic and International Studies, who has participated in such discussions. They say, "In the US, military espionage is heroic and economic espionage is a crime, but in China, the line is not so clear," available from *bits.blogs.nytimes.com/2013/03/14/cyberattacks-prominent-in-obama-call-with-new-chinese-president/*.

18. Nicole Perloth, "Hackers in China Attacked The Times for Last 4 Months," *The New York Times*, January 31, 2013, available from *nytimes.com/2013/01/31/technology/chinese-hackers-infiltrate-new-york-times-computers.html*.

19. Siobhan Gorman, August Cole, and Yochi Dreazen, "Computer Spies Breach Fighter-Jet Project," *The Wall Street Journal*, April 21, 2009, available from *online.wsj.com/article/SB124027491029837401.html*.

20. That being so, one need not ponder the problem that paying someone not to be bad sets the wrong precedent.

21. True, it takes intelligence on the target to determine the targets that are most **militarily appropriate**. But this is a criterion for warfighting rather than signaling displeasure.

22. A true assessment has to factor out the influence of information that you know but you believe that they do not know, plus what they know that you do not know, and then try to factor in your guess as to how much weight they give your assurance (or lack thereof) so as to calculate what you think **they** think is the probability. After all that, it is a lot easier to assume that their certainty equals yours and be done with it.

23. They might quibble with a declaration that promises a nuclear response, but that is another issue.

CHAPTER 13

FRAMING CYBERWAR AND CYBERSECURITY: COMPELLING METAPHORS AND DUBIOUS POLICY TEMPLATES

Davis B. Bobrow

INTRODUCTION[1]

It has been, and promises to continue to be, a gloriously rich period for American cyberwar and cybersecurity voyeurism. Most days bring a new or recycled leak, press release, incident report, or policy statement with variants on a common theme of a profound and intensifying threat to America.

A cynic might note that this drumbeat of threats seems to be curiously coincidental with U.S. political campaigns, executive-congressional wrestling, intense competition for national security budgets and program authorities, and attempts to revive pertinent controversial legislation stalled in Congress. An especially jaded observer might note the domestic political attractiveness of making credible some major form of U.S. defense and offense activism that does not involve U.S. "boots on the ground" or even air and naval applications of force. A national security expert surely would note the frequent references to governments already high on the U.S. enemies list (China, Iran, North Korea, and Russia). Such contextual factors are not about to disappear.

Whatever the reasons, cyberwar and cybersecurity, for the foreseeable future, will rank near or at the top of U.S. charts of threat and power projection hot sellers. That was illustrated in President Barack Obama's

State of the Union address in February 2013. A few weeks later, cyberattacks were accorded the status of most immediate dangerous threat by the highest-ranking U.S. intelligence official. Near the end of the year, Federal Bureau of Investigation (FBI) Director James Comey testified that "in the future, resources devoted to cyber-based threats will equal or even eclipse the resources devoted to non-cyber-based terrorist threats."[2]

That status has brought with it appetites for a frame or frames that could offer several benefits. Policy dialogue and planning could be elevated above the rapidly changing, technologically fluid, and very numerous specifics of cybersecurity measures and countermeasures. Doing so would provide a basis for thinking and justifying choices in strategic and not just tactical terms. Indeed, proper framing could enhance the credibility of claims that the cyberdomain is of very great security importance, and will be for the foreseeable future. It could foster confidence that American security elites can and will manage cybermatters in ways that extend U.S. supremacy and security when they are given the resources of money, technology, and decision authority they claim to be needed. Especially pertinent professional and commercial specialists could benefit almost immediately from a halo of history that persuasively validates ongoing increases in public and private sector resources and priorities for cybersecurity and cyberwar products and services.

The claims for benefits often originate in organizations and individuals who are part of what amounts to an emerging "virtual iron triangle." The triangle links relevant techno-industrial for-profit and nonprofit organizations, government bureaus with relevant missions, and elected officials seeking supporters from

among those who want a bigger push for cybersecurity and cyberwar capabilities. Actions that respond positively to the claims tend to boost their policy legitimacy. That legitimacy, in turn, reinforces deference to the triangle and its members who made the claims in the first place. The results, other things being equal, are likely to be increased demands by and influences from the emerging virtual iron triangle for research and development (R&D) investment, for procurements from it, and for broadening and deepening the jurisdiction and powers of the military and civilian institutions with cyberexploitation mandates.

While some of the parties to the triangle may be skeptical about cyberwar, they do support efforts to enhance capabilities for cyberwarnings, active and passive defense, and offense if only for deterrence purposes. That amounts to support for U.S. operational readiness including training and exercises for a cyberpreemptive attack, defensive damage limitation, and retaliation. Particular frames can seem especially attractive to cybervendors and government cybersecurity managers and commanders if they provide a robust rationale for two developments. One has private and nonprofit sector executives convinced that their responsibilities include pursuing cybersecurity to limit damage to countervalue, i.e., nonmilitary, targets as well as counterforce ones. The second has them accepting cyberregulation by the national authorities charged with assuring cybersecurity and conducting cyberwar, and indeed executing assignments from them. Those accommodations are made more palatable by growing cyberspending and supportive regulatory and trade actions of commission and omission. Those developments can become institutionalized, routine practices if only rare events (e.g., the Snowden

revelations) call attention to their scope and potential implications.

The predominant frames in mainstream U.S. policy circles and punditry are selectively drawn from Cold War nuclear weapons approaches and from the attack on Pearl Harbor, HI. Those two templates (what I will call The Odd Couple or TOC) already have been shaping general U.S. conceptions of cyberwar and cybersecurity as well as more specific choices about how to pursue them. The consequences (actual and perceived) have and will affect how the rest of the world chooses to treat cyberwar and cybersecurity. U.S. interpretations of cyberacts of commission and omission by others will be filtered through our TOC screens. Others for their part will interpret U.S. cyberacts of commission and omission as chosen in light of what seems to be our accepted construction of TOC.

Before we accept locking policy into a TOC frame, we need to have confidence that it will provide the benefits mentioned above. Warranted confidence ought to come after, not before, due diligence consideration of three types of factors. One, of course, recognizes the considerations that make TOC appealing. A second concerns the historical accuracy and completeness of TOC prevailing construction. It calls attention to elements TOC omits or downplays from the actual experience of nuclear weapons and Pearl Harbor. The third considers TOC dissimilarity with cybertechnologies and operational processes in being and on the horizon. Gross differences cast doubt on whether even an improved version of TOC illuminates more than it distorts coping with prospects for cyberwar and cybersecurity.

THE APPEALS OF TOC

For more than a half century, well before high profile cyberwar and cybersecurity, public U.S. security frameworks have featured nuclear weapons posture and Pearl Harbor. The conventional wisdom versions of each posture in the United States offer dramatic, self-justifying, and motivating imagery about America's national security and world role. Those, in turn, contribute to a mandate for some crucial and arguably attainable policy imperatives for immediate and long run pursuit. America has vulnerabilities and finite time to ameliorate them, so it should give doing just that priority and reject both despair and relaxation. Spreading or extrapolating those images and imperatives to frame cyberwars and cybersecurity extends to them an essential and almost sacrosanct security role.

That role brings with it a hard to challenge obligation to provide funds, program mandates, and voice to the parts of the technological, industrial, military, and intelligence communities relevant for cyberwar and cybersecurity. TOC brings with it assurance that time is available for steps to close security gaps. Our security situation is serious but not desperate. For example, Director of National Intelligence (DNI) James Clapper, in testimony also given by Comey mentioned earlier, combined the high threat status accorded to cyberattacks with assurances both that there was only a "remote chance" of a major cyberattack in less than 2 years (i.e., before 2016) and admissions of lags in America's ability to "mitigate potential risks."[3]

The nuclear weapons themes in the mainstream Washington security community version of the TOC evoke several attractive but demanding aspirations and expectations for American cyberactivities. For

decades, the United States should and can have cyberdestructive force projection so awesome as to deter state actors from a direct attack on it, and, indeed for the most part, on allies clearly under our defense umbrella. For decades, the United States should and can credibly imply that it might actually use that destructive force on others and seek superiority while also making it credible that we prefer successful and stable deterrence. In other words, the United States can and should convince others that we will refrain from attack if they behave themselves, and simultaneously maintain the option of inflicting great damage if and when we choose to do so. American credibility in terms of the will to use our cyberassets and their damage inflicting potency should and can be made clear with a few illustrative acts. A combination of declaratory statements including rejection of no first use commitments, an occasional show and tell of readiness, and visible weapons/delivery system modernization will suffice. The combination can enable America to control escalation even with a major adversary in a protracted ideological and geopolitical conflict. In effect, the U.S. card of being able and willing to inflict assured destruction will make us safe so long as we have a monopoly.

If and when an adversary eventually catches up, the worst realistic case is that we can persuade it to settle for deterrence through mutually assured destruction (MAD) rather than craziness and instability. There will be time to work all that out in an oligopolistic fashion. Further, we can sustain oligopoly power for a considerable time, albeit with considerable effort, by persuading would be proliferators to reduce or delay their cyberambitions through threats of "sticks" and glimpses of "carrots." Even with eventu-

ally limited success in avoiding proliferation, the nuclear world has been made rather stable by three legs to support nonuse. Those stabilizers by analogy can be applicable to the cyberworld. The first consists of mutual restraint arrangements including: robust command and control by the highest civilian authorities; technological and personnel fail-safe arrangements; confidence building measures featuring transparency and reliable communications; weapons inventory reductions; and deployment compromises. The second develops defensive systems capable of degrading an attack. The third leg ensures low to no confidence in being able to destroy effectively the nuclear weapons capacities of a target by a first strike. That is, there will be too grave a risk of the target launching retaliatory nuclear weapons either when anticipating or reacting to being attacked. By analogy with nuclear weapons, an eventual waning of a U.S. cybermonopoly and then oligopoly will take decades. In short, there will be ample time to bolster each of the three legs making for crisis containment and stability.

The Pearl Harbor part of the TOC as reinvigorated by September 11, 2001, makes the positives just summarized conditional but still achievable. The conditions call for robust vigilance about threats from abroad, enhanced warning, and continuous improvements of American means to preempt an attack by foreigners, limit damage from it, and mount a crushing response to it. Pearl Harbor evokes, again in the U.S. preferred version, imagery of a peaceful trusting America and nasty, sneaky others. Avoiding surprise attack makes warning capacity crucial, sustained vigilance obligatory, and operational readiness essential. There is no other reliable way to avoid America again being victimized by surprise attack. Prudence and

collective responsibility call for deployed and alerted defenses that can disrupt and curtail damage from an attack, and a techno-industrial base that can quickly replace lost assets.

TOC appeals for Americans also include de-emphasis of, and indeed aversion to, several lines of policy and support for others. TOC true believers are skeptical to hostile with regard to security strategies that require lengthy deployments in combat zones and American casualties incurred by foreign interventions. Their priorities favor technologically sophisticated, complex, and expensive weapons systems and platforms with primarily U.S. or offshore basing. Those "big ticket items" central to the triad of U.S. nuclear forces tend to have long lead times to procurement, protracted procurement schedules, and long operational lifetimes. TOC proponents favor having a "big stick" of military long reach force projection in being at all times with high readiness levels. They oppose reducing the centrality of military instruments and institutions in U.S. security policy and security spending. TOC supporters are reluctant to count heavily on foreign promises verbal or written of good behavior. They tend to doubt the wisdom of the United States in deferring punitive unilateral action until after creating at least the appearance of a supportive multilateral coalition.

TOC core conception of security is about threats posed and threats blunted, increasing and reducing pain and damage. At least in relative terms, TOC appeals to those skeptical about the United States undertaking positive transformational roles internationally as well as about the prospects for sustained international amity and fully compatible agendas. That basket of policy preferences provides TOC advocates

with some substantial sources of political support in the United States, and mobilizes little, if any, potent opposition.

In short, for those who view cyberspace in national security terms and especially military terms, TOC holds out the prospect of having their cake (managed insecurity) and eating it too (resources and status). The frame offers a curious mix of fearful danger and soothing assurances. It justifies ongoing and substantial resource allocations for endless vigilance about surprise attacks, strong and quick action based on warning, deployed and highly ready active and passive defensive systems, and war sustainability including production-surge capabilities to replace lost assets rapidly.

In TOC perspective, it is imperative that the United States seize the first-mover advantage by a dramatic demonstration of the fearful potency of our cyberweapons. That will make for a lengthy period of initial cybersuperiority.[4] By analogy with the nuclear experience, appropriate demonstrations of U.S. potency and resolve now may secure more than a half century of conflict limitations. The perceived and actual destructiveness of nuclear weapons seem to make them great exemplars as stabilizers and escalation dampers. That, of course, requires attributing massive damage inflicting properties to cyberinstruments as recent U.S. policy rhetoric does.[5]

As for the longer term, TOC offers tolerable precedents for security after nuclear dominance. After a decline to oligopolistic sufficiency, a set of national intelligence collection systems, conceptions (deterrence) and conventions (safeguards) will work against surprise attack and rogue state triggered conflict. Beyond that, albeit not easily achievable, advances in active

defense systems may eventually enable the United States to move from oligopolistic deterrence sufficiency to unilateral or alliance damage denial and imperviousness to retaliation. By analogy to the favored TOC narrative, most governments with major cyberweapons capabilities will have reliable command-and-control capacities to assure each other that retaliation will be unavoidable, and initiation (first use) will be avoidable. They will not find it both necessary and feasible to achieve improvements in their strike capabilities that equal let alone surpass U.S. advances in cyberdefense. Of course, most governments and movements will forego fielding and using cyberweaponry altogether, especially if we provide an extended cyberumbrella.[6] We may not need to settle for a mutually hostile world but instead, progress toward damage denial options to complement our damage inflicting ones. Of course, there may be a few hair-raising moments along the way, like the Cuban Missile Crisis, but that incident shows they can be managed.[7]

In the previous story line, TOC then offers, first, a rationale for immediate exploitation of U.S. damage inflicting capabilities. Second, it envisions longer-term "tolerable anxiety" conducive to increased cyberwar and cybersecurity budgets, contracts, and government powers, but not a sense of urgency or robust feasibility for pursuing major cooperative security measures. In international affairs, we will have much to offer to others—shelter under a deterring umbrella and containment of their enemies so long as they accept cyber-inferiority. The known occurrence of surprise attacks and rapid technological changes does call for rapidly building up permanent military and intelligence institutions to manage national cybersecurity. That build up need not and should not wait for supportive con-

sensus from civil society and the private sector before installing greater cybersecurity discipline and regulatory supervision.[8]

TOC CHERRY PICKING

Before accepting TOC frames, we ought to recognize both potentially positive and highly negative, or at least troubling, features of the nuclear weapons and Pearl Harbor experiences masked or omitted in the appealing narrative just summarized. Those slighted aspects will add balance and historical depth to any projections we make from TOC to cyberwar and cybersecurity. Of course, the wisdom of relying on an even more balanced and complete account should depend on the similarities and differences between cybertechnologies, institutions, and procedures and those central to America's nuclear weapons and Pearl Harbor experiences. Those considerations will be discussed later.

The nuclear weapons experience has not been as orderly, free of controversy and course corrections, or security providing as TOC would have it. More generally, the half-life of America's near monopoly was shorter than anticipated. The nuclear weapons or near weapons club has continued to grow in ways driven by regional dynamics and advantaging some new member regimes the United States views as hostile (North Korea) or domestically unstable (Pakistan). While the club has grown much more slowly than early post-World War II estimates expected, some member states have abetted proliferation by exports of technologies and technologists. U.S. nuclear capacity has not sufficed for America to avoid costly and protracted foreign wars (Korea, Vietnam, Iraq, and Afghanistan).

Nor has it been usefully employed to wage them, or provided us with clear victories in them. On important occasions, constructed memories of Pearl Harbor have not led to credible warning and forestalling actions (Korea and Afghanistan) or together with nuclear weapons fears have led to unwarranted anticipatory actions (the invasion of Iraq).

In spite of years of effort, there is not yet a reliable effective defense against either a massive sophisticated homeland nuclear attack or a small scale unconventionally primitive one.[9] For at least the last decades of the Cold War, U.S. domestic infrastructure (electrical grid, water supply, pipelines, and communication networks) repeatedly were found vulnerable to simple acts of physical disruption—and they still are.[10] At no point has there been a credible, substantial urban population and civil asset damage limiting system. Common nuclear weapons and common cyberweapons narratives have shared tendencies to discover vulnerabilities and present them as previously nonexistent, new and additional justifications for enhanced programs. Yet some of those vulnerabilities in important respects existed before and continue to exist during and after the deployment of each family of nuclear and cyberinnovations.[11]

In short, nuclear war has been avoided as have large scale conventional military attacks on each other's homelands by nuclear armed powers—great but limited accomplishments. Threats, however, have not become locked onto steep paths of sustained decline, nor have defensive measures achieved widespread fruition. Further, the appealing TOC narrative discussed earlier scants on some of the self-constraining choices associated with avoiding a post-World War II nuclear attack. Those choices of omission and com-

mission have focused on escalation control, crisis management, and stable deterrence. They have been subject to domestic political opposition that has watered them down, delayed them, or imposed linkages minimizing their stabilizing effects. Those requiring multilateral, as distinct from unilateral or bilateral, negotiation and sustained implementation have had long gestation periods and been vulnerable to erosion and defection. Overall, such insecurity management moves have lagged threat technology advances and deployments, and been subjected to draining burdens of justification.[12] For the cyber-realm, the security consequences from adopting TOC framing without at least as effective insecurity management options and positive adoption prospects may well be even worse. With the benefit of hindsight, we can see that the options, let alone their adoption and implementation, usually came after an uncomfortable, scary experience or imminent prospect of one. Insecurity management measures prominent in the TOC were reactive and lagging. The risks from that sluggishness were ameliorated by the slow to ripen nature of changes in nuclear postures.

In trying to make nuclear insecurity manageable, the United States and some other nuclear-armed states have attempted to establish and disseminate mutually accepted, operationally clear distinctions between various nuclear weapon systems' physical properties, different intended uses, and strategic and doctrinal alternatives and practices. The rationales accompanying these possibilities often claimed to make actual weapons use and thus deterrence—especially extended deterrence—more credible. That would come from a menu of more incremental nuclear options better suited to a proportionate, less than annihilating exchange.

There would be less possibility of misunderstandings about the tipping points for initiating war, escalation ladders, breakpoints, ceasefires, truces, or terminations. Such elaboration surely is underway in the cyberworld but is neither rapid nor fully accepted.

Yet, many less than "all against all" nuclear postures eventually have been shelved or abandoned whatever the capabilities of the technologies involved and the rigor of the advocates' reasoning. Possibilities lost support for a variety of reasons. One was concern that a doctrine of incremental use would weaken rather than strengthen deterrence since there would be less "shock and awe," less fear of a World War I-like drift to Armageddon. It has been hard to identify clear and widely acceptable standards and metrics for appropriate proportionality of damage.[13] Skepticism remains about premises that a coolly calculating, rational, centralized decision-making authority would operate at all times in all the conflicting parties. Similarly, there are doubts that diplomatic, military, and intelligence networks faced with deception, intentional disruption, and incidental technical malfunctions would work as designed to delay, initiate, wage, interrupt, or terminate a conflict.

Another set of choices conducive to escalation control, crisis management, and stable deterrence has involved transparency of weapons programs and military operations, and even foregoing some of the secretiveness conducive to genuinely surprising attacks. Some governments have found ways to convince others that they have pulled back from nuclear club membership for domestic as well as international reasons. Some have found persuasive ways to demonstrate distinctions between their civil and military nuclear programs. A number have taken technological and

personnel measures to guard against loss of control of weapons and their critical ingredients. Others eventually resorted to unilateral and cooperative confidence building measures that cut against opportunistically using weapons at a time and place of one's choosing.

Major reciprocal steps to control nuclear weapons such as Dwight Eisenhower's Open Skies (1950s) and the U.S.-Union of Soviet Socialist Republics hot line (1960s) only came a decade or more after Hiroshima and Nagasaki, Japan. We do know that it took fortuitous, unplanned actions to cool the Cuban Missile Crisis and deployment concessions by both the Soviet Union (Cuba) and the United States (Turkey). Whatever else, that and other unexpected events provided a spur for conceptual strategic innovation (e.g., arms control), and support for a variety of reassurance provisions and crisis management confidence building measures. By mutual agreement, the United States and Russia have reduced their nuclear arms inventories, albeit not as much as envisioned in the Non-Proliferation Treaty, and even cooperated to safeguard those inventories through strengthened controls. Further, they have evolved a substantial degree of transparency about capabilities and strategic doctrines, and urged newer members of the nuclear club to do so as well. Nevertheless, the measures taken largely have been reactions to growing threats of deterrence failure. Once in place, many have been allowed to erode (as with U.S. nuclear weapons custodianship). Even when not neglected, such approaches have often failed to develop policy momentum for broader participation or deeper monitoring and compliance.

Current treatments of cyberwar and cybersecurity are not devoid of analogies to some of the choices made in the nuclear domain to bolster escalation con-

trol, crisis management, and deterrence stability.[14] Yet, cybersecurity and cyberwar have yet to develop the elaborations and put into practice many of the hedges developed over more than 6 decades of coping with nuclear weapons. While not completely ignored, self-limiting steps are marginal to apparent U.S. cybersecurity priorities.[15] They do not feature in the prevailing TOC narrative discussed earlier with two negative exceptions. In the first, those self-constraining choices are viewed as a mirage and their supporters naïve.[16] In the second, cease and desist demands are made of foreigners unaccompanied by provisions for commensurately valued accommodations by the United States.[17]

The preconditions for giving a serious push to hedges involving self-restraint and multilateral mechanisms seem to be only embryonic and lagging far behind the evolution of threats. If that continues or becomes even more pronounced, we should have less confidence in being able to avoid major future international cyberconflicts as we have managed to do with nuclear weapons.

As for the Pearl Harbor part of TOC, the narrative presented earlier is incomplete in important respects with respect to impact, feasible damage limiting, and the attacker's calculus. All three are important considerations for cyberwar and cybersecurity. With all said and done, the attack did not prove decisive, or strike at the American techno-industrial base or our basic civil infrastructure. What impact the attack had beyond immediate casualties and damage to ships was on the U.S. ability to project force by sea. That took time to replace but again not so much as to allow Japan to win the Pacific part of World War II. In retrospect, the pertinent U.S. forces had the capacity to blunt the Japanese attack, and U.S. Navy intelligence

officers did provide warning. Problems lay more with organizational routines and leadership styles than with technology backwardness and shortages or lack of relevantly trained personnel. Finally, the Japanese attacker believed with good reason that the United States was hostile to it and actively was seeking to reduce its future security initially through economic sanctions. The attack was less motivated by optimism about long run prospects than seizing a waning opportunity to buy time in the hopes of some more positive prospect emerging.

That suggests we should add several lessons to the Pearl Harbor part of TOC when applying it to cybermatters. First, immediate long-run estimates of recovery periods from an attack may be excessively pessimistic. Second, timely responses to warning are hindered by bureaucratic layering, and a low alert level. Third, foreign regimes and groups convinced U.S. policies are and will be hostile to their cardinal interests will try to push us back at times and places of their choosing, ones that may sharply differ from those we have concentrated on preparing for.

COUNT THE WAYS: CRUCIAL DIFFERENCES FROM TOC

Does TOC as a frame for cyberwar and cybersecurity simply need improvement by making more of the experiences and considerations discussed in the preceding section? That possibility seems tempting in terms of future policy adoption, and, in some respects, would resemble what has happened over more than half a century with the nuclear weapons and Pearl Harbor frames. The temptation should be resisted. After all, the likely net benefits even of a more com-

plete TOC are not superb in security terms and seem to have at best modest prospects of becoming so in the foreseeable future. More fundamentally, as argued below, cyberwar and cybersecurity differ so basically from the nuclear and Pearl Harbor templates that relying on them lacks realism and thus security wisdom.

Nuclear weapons effects are far more direct, severe, long lasting, and less reversible. Compare the casualties from Stuxnet against Iran and Iranian attacks on the Saudi Arabian Oil Company (ARAMCO) with Hiroshima and Nagasaki. Imagine how Georgia or Estonia would have fared if the often discussed Russia based cyberattacks on them had instead used nuclear weapons. As it was, even the defenders and their allies who lacked substantial experience with such attacks were able to recover without lasting damage by using resources located elsewhere. It is instructive to note that Clapper, in the testimony cited earlier, provided as his example of a major cyberattack on the United States only "a regional power outage."[18] If fear makes for pulling back from a nuclear brink, a sort of deterrence multiplier, commensurate incentives are not present for a cyberbrink.

Damage to production and storage facilities for nuclear weapons, some weapons materials, and civil nuclear power facilities can itself be a source of widespread, long-lived, physical harms (consider Chernobyl, Ukraine, and Fukushima, Japan). That is not so for facilities that play similar roles in the cyberdomain. Governments then have far weaker incentives to regulate them. Private sector owners and operators have far weaker incentives to accept or promote tough safety cultures. The United States and its opponents have far weaker escalation control reasons to forego attacking them.

Nuclear weapons, advanced delivery systems, special materials, and their core technical personnel are more readily subject to being kept distinct from other national security and civil economy assets. They and their personnel are, with relative ease, subject to extraordinary checks against unauthorized use, access, or diffusion.[19] Compare, for example, the ease of tracking and finding "loose nukes" or weapons-relevant radioactive material with the difficulty of tracking and finding thumb drives containing malware. To a large extent, nuclear weapons-related human capital and physical facilities are susceptible to monitoring by the United States and others in part because governments may have greater confidence in control measures that concentrate such resources in a few locations. Cyberinstruments are often incorporated into widely distributed military and civil assets in the United States and globally. Cyberassets, be they products or R&D and production facilities or skilled personnel, are widely dispersed, not easily identifiable by remote observation, internationally sourced, and, in important respects, highly mobile. Indeed, in striking contrast to the big science of the nuclear domain, the cybersecurity domain has a substantial degree of garage science, of self-selected innovators working largely on their own or in informal networks with little, if any, affiliation with large private or public sector organizations. In short, the cyberdomain is far more difficult to control and manage in a single government's jurisdiction let alone the jurisdictions of multination functional groupings, regional institutions, or security alliances.

Nuclear weapons programs pose far higher development and production barriers to entry, demonstration, and capability enhancement than do cyberprograms with weapons and security implications. The

club of governments whose residents are capable of inflicting cyberdamage on others has, and will have, many more members than its nuclear counterpart. An even greater contrast already is the widespread presence of nonstate cyberplayers, organized and unorganized, with means to share quickly important technical knowledge and publicize their cyberfeats in a status building David versus Goliath fashion.[20] Further, both state and nonstate actors can more quickly develop, adopt, and use more challenging means of cyberoffense and defense. In effect, the quick tempo from initial conception to fielded asset to being leapfrogged rests on an innovation and application process radically different from the lengthy, highly bureaucratized system for nuclear weapons and advanced delivery systems. That for the cyberworld advantages the nimble, and the nimble are often those with few members, horizontal organization, and disrespect for mainstream conventional practices and establishment institutions.[21]

Together, these phenomena make construction of international codes of cyberconduct with credible verification and compliance mechanisms even more difficult than it has been for nuclear matters. We know many years have been needed to conclude relevant nuclear conventions, and many more to implement them. Yet arsenals for cyberoffense and defense are likely to change through technical innovation much faster than their nuclear analogues. Cooperative cybersecurity measures are more likely to be obsolete at birth, if not before. For the most part, cyberweapons pose a far more difficult set of challenges to a National Command Authority and surely no less so to establishing even a small enrollment international system of robust stable deterrence, non-diffusion, and target restraint.

The current dynamism and ubiquity of the cyberdomain in the United States lodges primarily in the private sector, regardless of initial government provided impetus. At this point, cyberinnovations flow more toward government rather than from it. The civil market is far larger than the military market. Production is globalized, and sales are international. Cyber use is pervasive and important for firm profitability in numerous sectors. In contrast, the nuclear domain seems narrow, modest, and stagnant. The cyberproducts and services industry is immensely important in U.S. international trade and foreign direct investment. In these respects, it contrasts with the U.S. nuclear industry.

Not surprisingly, the cyberindustry and those dependent on it have very substantial economic and political clout. The American government's capacity to regulate the cyberindustry, and the cyberbehavior of its customers, amounts to much less than for the nuclear industry. Even though 85 percent of relevant targets of cyberattacks are in private sector hands,[22] the U.S. Chamber of Commerce has opposed intermittent Federal attempts to set even voluntary cybersecurity standards for infrastructure firms, and the Congress has rejected setting them. Although often less than comprehensive and imperfectly enforced, the U.S. Government has had far greater success in setting mandatory standards for both the military and civil parts of the nuclear domain. Unwillingness to require major sustained improvements in cybersurvivability and cybersecurity outside of American national security institutions apparently remains as robust as it was when then White House Advisor Richard Clarke broke his sword on similar issues more than a decade ago. That continuing unwillingness follows in part

from prospects of damage to international trade and sourcing from controls on exports, imports, foreign direct investment, and technology transfers. Those concerns may be fueled by corporate and host government worries about possible special arrangements by the United States and other governments to exploit exported and domestic cybergoods and services.[23] The opposition of firms who are not themselves cybervendors could also follow from concerns about making corporate proprietary information and financial practices more transparent to government agencies. Privacy interests, ranging from civil libertarians to criminal cartels, surely are wary of legal or opportunistic government cybersurveillance.[24]

Nuclear weapons are not tools for assisting political dissidents in other countries to achieve destabilization and regime change or for facilitating regime suppression of dissidents. Cyberinstruments can and are serving both purposes as firms and governments develop, give, sell, and operate them for both purposes.[25] In that sense, they are hyped-up analogues of historically common means to give aid and comfort to apparently useful regimes and dissidents and weaken those viewed as hostile or dispensable.[26] That makes cyberinstruments weapons (if non-kinetic ones) in political conflicts. When supplied to partisans of regime change, it is understood to amount to foreign intervention to reduce a target regime's security in informational ways, to lessen a government's information security. The immediately affected regime and its international supporters have little doubt about the intent of foreign hosts who facilitate political unrest and economic volatility. When the transfer enables regime suppression, dissidents and their domestic and international supporters view it as inimical to their cyber-

security. Any broadly inclusive international cooperative security arrangement for cyber-arms-control or disarmament will for now at least be stillborn unless it engages political as well as military and economic uses.[27]

Once invented or even detonated, the key components of nuclear weapons do not quickly become substantially available in readily accessible open sources. In contrast, key cyberweapons and cybersecurity elements, including key Stuxnet algorithms, have and do migrate to and from open sites.[28] In effect, cyberattacks facilitate copying and emulation of their instruments in a rather direct fashion. Before long, those who lead in the use of a particular cyberweapon may well lose any first-mover advantage. They should expect the instrument to be thoroughly dissected, reconstructed, and then used by others including against its originating organizations. Cybersecurity sources and methods are hard to keep proprietary. Lots of able persons and informal networks around the world are committed to breaking down asserted cyberproperty rights.

Nuclear weapons rarely, if ever, have been used to collect intelligence, disrupt others' intelligence operations, engage in economic sabotage, or conduct commercial espionage.[29] Employing a nuclear weapon solely to attack economic targets without previously or simultaneously striking at a government's retaliatory military capacity seems highly unlikely. Confusing historically well-established types of intelligence intrusions or economic troublemaking with a nuclear attack on national security seems farfetched. In contrast, cyberweapons have and are being used in ways that could amount only to military and other types of intelligence collection or could be gambits to gain commercial advantages in the world economy—or could

be precursors to or early stages of attacks on national security.[30] Some, often cybervendors and executives of government cybersecurity programs, have even suggested that the United States faces a cybereconomic Pearl Harbor countervalue attack, and has already suffered from a massive outward wealth transfer engineered by foreign government-sponsored cyberagents and organizations.[31] Numerous nongovernmental cybersecurity penetrators, including commercial rivals, issue-centered cause groups, hacker virtuosos, and gangs seeking something to sell or to extort protection payoffs, compound the chances of confusion.

There are, at least for now, few, if any, internationally well-established criteria for distinguishing between very different possible purposes of a cybersecurity occurrence immediately when it occurs or is noticed. Controversy and uncertainty pervade the pursuit of timely high confidence judgments that a given cyberaction or R&D program does and will serve only intelligence and economic competitiveness goals. Prudence can suggest reacting to the "if" of it being used to reduce significantly a target's military performance or weaken its leadership. Further, the physical and decision-taking origin of an attack may be obscure, let alone whether, when, and why high level officials provided informed authorization. Greater uncertainty and confusion about the who, when, and why of cyberactions make for greater chances of mistakes in preparation, attribution, and reaction than with nuclear weapons. Perhaps recognition of that is why the United States and China apparently have lived with what each claims are thousands of cyberattacks from the other before recently increasing the quite limited response of indignant rhetoric and calls for codes of conduct.[32] It is hard to imagine Washington or Beijing

adopting a similarly modest response to a homeland attack by even one nuclear weapons device.

A NEED TO RETHINK

The differences reviewed suggest that, at this point in international security affairs, only a Pollyanna or a Micawber would assume that sturdy, stability enhancing cyberdeterrence strategies and policy mechanisms are in reach intellectually or operationally.[33] Even if they were well understood and formulated in practical terms, severe problems of compatibility with the speed of technological change, commercial agendas, and low barriers to entry would remain. Cyberwar and cybersecurity do not lend themselves to being accommodated within even the most complete and balanced frames based on American understandings of nuclear weapons and of Pearl Harbor.

The core of deterrence strategy after all is a combination of assured damage and assured restraint. The former calls for several convictions being shared by the potentially hostile parties about retaliation: a) the target will have a sufficiently damage-capable surviving force; b) those responsible for the attack are known, locatable, and value highly what will be lost to retaliation; and c) the target's surviving force will, with high probability, retaliate on the real attacker in a timely fashion. At this point, the second and third convictions seem a stretch in the cyberworld. The second core feature, assured restraint, also rests on several convictions: a) no party will attack unless it believes it has been or will definitely be attacked imminently; b) no party will mistakenly and irreversibly draw that conclusion and be wrong; and c) binding go and no-go decisions about any substantial weapons release and

launch will be at the highest governmental levels best aware of what is at stake and with the benefit of accurate information and some means to confirm it. All three of those convictions are on shaky cyberground.

Regrettably, the already shaky convictions are receiving less than fully credible verbal affirmations or being further undercut by policy emphases. For example, in October 2012, then Secretary of Defense Leon Panetta asserted that the United States can determine the source of any cyberattack or security violation and hit back. His public testimony to that effect did not indicate how long it might take to do so, how confident we would be about the attribution to specific physical locations and operators, how well we would understand who authorized the attack and why they did so, or how massive our punitive response would be relative to the attack we experienced.[34] There is as yet no coherent set of public commitments about the U.S. stance on extended cyberdeterrence to cover foreign economies, governments, or nongovernmental groups. That means, of course, murkiness about the sorts of tripwires that would make those commitments credible.

Of very serious concern, the United States has left obscure publicly, and perhaps not just publicly, how it will deal with the implications of seeking to make cyberwar and cybersecurity decisions at cyberspeed.[35] Time is indeed of the essence, but crisis management that seeks to control escalation often has favored slower rather than faster security action-response cycles. With cyberspeed and the greater prospect for genuinely surprising attacks, the rationale for delegation to software of preauthorized preemptive, preventive, or retaliatory authority gains persuasiveness.[36] The U.S. history of authorization to launch (or not) nuclear

weapons has evolved over 6 decades to feature fail-safe constraints and elevation to the highest political level in the immediate context of a particular critical situation. Unleashing cyberweapons may well unfold in an opposite way. Rules for the use and nonuse of cyberweapons lag their deployment (as they did for nuclear weapons). Rules of engagement, including who can authorize what uses, when, and how, or command halts, might be vague, missing, or fragile. Arrangements may well be chosen to make weapons use assured in the face of what are thought to be rapidly closing windows of opportunity. Those can take away authority from senior officials and affect decisions in ways that make crisis management and escalation control more difficult and brinkmanship more risky. A particularly troubling possibility is near automatic attribution by preauthorized cyberweapons users that other parties are engaging in informed and intentional hostile action.[37]

Official public U.S. cybersecurity posture as of March 2013 does more to erase than to establish distinctions helpful for deterrence. That is true with regard to the distinction between cyberintelligence and cybermilitary operations. The U.S. Cyber Command charged with the latter has been co-located with the National Security Agency ([NSA], a military-led entity) charged with much of the former. They have been put under the same commanding general.[38] The distinction between defensive and offensive intentions has become more strained when that general seeks congressional funding for some units to engage in offensive cyberoperations while others will conduct "surveillance and monitoring."[39] There also have been public announcements of R&D programs to yield more than defensive cybercapabilities, of military

personnel training for non-defensive cyberoperations, and expert appraisal of offensive options.[40] Foreigners readily can find indications that, at least for the near-term, U.S. cyberpolicy will tilt toward offensive operations of a (sort of) covert or clandestine nature. After all, the Obama administration hardly rejects credit for damaging potential foreign threats at times and places of our choosing by means of what amount to unannounced surprise attacks with no declaration of hostilities against the government of the targeted area. Indeed, it is at work to institutionalize those practices.[41]

Not unreasonably, we can liken the U.S. approach to cyberwar and cybersecurity to people who live in very nice glass houses, and regularly throw rocks at the less nice glass houses of others, are lethargic or resistant to installing some rock deflection devices on their homes, and upbraid the police for not stopping others who easily can also come up with lots of rocks to throw at the glass houses and instead fill e-mail with security tips. Indeed, we even invest in glass houses far from our primary residence. How that all goes together in a rational security maximizing sense escapes me, but it surely warrants neither outraged innocence nor even surprise when some homeowner we have previously damaged, tosses a big one shattering a lot of glass at our distant investment or our primary residence.[42]

CONCLUSION

The selective TOC frame has strong political, psychological, and economic attractions as an encouraging metaphor; encouraging in terms of disasters avoided, limited successes achieved, and sustained capabilities. That follows in no small part from invok-

ing a very pro-American, laudatory version of TOC. Unfortunately, that invocation accepts some dubious history, omits some very important aspects of the nuclear weapons and Pearl Harbor experiences, and assumes some important but unwarranted technology and procedural equivalences. Accordingly, TOC does not provide a prudent guide for American cyberwar and cybersecurity policy in the 21st century. It, at best, might provide a few important but incomplete chapters.

Far more likely, however, is that TOC's emphases, omissions, and unwarranted assumptions will reinforce self-damaging policy illusions. Those will carry with them substantial direct economic and security costs associated with a cyber-arms-race marked by leapfrogging defense and offense measures and countermeasures. Directly and indirectly, those competitive patterns increasingly will undercut proclaimed U.S. goals of a tolerant and cooperative cyberworld marked by individual informational freedom and mutually beneficial, peaceful cross-border flows. They will further motivate others to modify or organize alternative international cyberinstitutions with different priorities than those of currently American controlled bodies.[43]

It takes little effort for the rest of the world to note the NSA's intent to "aggressively pursue legal authorities and a policy framework mapped more fully into the information age." That would help to achieve its goal of universal access ("anyone, anytime, anywhere") and "reach previously inaccessible targets and makes tempting a brute force approach of in effect 'everyone, all the time, everywhere'." The road to those goals, as asserted, features "leveraging global business trends in data and communications services" and countering "indigenous cryptographic programs." That confirms

perceptions of cyberspace less as a global commons and more as a Hobbesian contested field. [44]

With a few clicks of a mouse, any user of the World Wide Web can read that the Defense Advanced Research Projects Agency seeks contributions to its Foundational Cyberwarfare (Plan X) that will reduce the role of humans in cyberoperations.[45] It is asserted that doing so will enable the United States to take responsive actions at machine speed, not human speed. That shift to synchronous from asynchronous action-response patterns, if and when achieved, will curtail situational crisis policy discretion and executive political control over escalation in the cyberdomain or in responses to cyberevents that involve other domains. In effect, it amounts to an invitation to others to join in preparing not only for a Hobbesian prospect but one whose intelligence will at best be artificial.

ENDNOTES - CHAPTER 13

1. The main arguments made here were presented at the conference on "Cyberspace: Malevolent Actors, Criminal Opportunities, and Strategic Competition," Pittsburgh, PA, November 1-2, 2012.

2. Director of National Intelligence (DNI) James Clapper testified on March 12, 2013, to the Senate Intelligence Committee. See Mark Mazzetti and Scott Shane, "Intelligence Official Cites Threat of Cyberattacks on U.S.," *The New York Times*, March 13, 2013, available from *nytimes.com/2013/03/13/us/intelligence-official-warns-congress-that-cyberattacks-pose-threat-to-us.html*. Shortly after that, public reports appeared of newly destructive attacks on major parts of the U.S. financial system. See Nicole Perlroth and David E. Sanger, "Cyberattacks Seem Meant to Destroy, Not Just Disrupt," *The New York Times*, March 29, 2013, available from *nytimes.com/2013/03/29/technology/corporate-cyber-attackers-possibly-state-backed-now-seek-to-destroy-data.html*. Comey is quoted in Greg Miller, "FBI chief sees online attacks emerging as top security threat," *The Washington Post*, November 13, 2013, p. A18.

3. Mazzetti and Shane. That first rank seems less than firmly established. Within a few days, the Pentagon announced that it would bolster missile defenses on America's West Coast against a North Korean nuclear attack—a buildup to be completed in 2017. Shortly after that, the Russian government announced that the United States would use defense systems otherwise planned for basing in Eastern Europe purportedly to be used against much opposed Iranian missiles. Then the United States announced moving Terminal High Altitude Area Defense anti-missile assets to Guam within weeks, well ahead of schedule.

4. The United States arguably has tried to do that with the Stuxnet and Olympic Games activities beginning with the George Bush II Administration. See David E. Sanger, John Markoff, and Thom Shanker, "Cyberwar: U.S. Steps Up Effort on Digital Defense," *The New York Times*, April 28, 2009, available from *nytimes.com/2009/04/28/us/28cyber.html*.

5. For example, then Secretary of Defense Leon Panetta said there was a real prospect of a "cyber-Pearl Harbor that would cause physical destruction and loss of life, an attack that would paralyze and shock the nation and create a profound new sense of vulnerability." See Elizabeth Bumiller and Thom Shanker, "Panetta Warns of Dire Threat of Cyberattack on U.S.," *The New York Times*, October 12, 2012, available from *nytimes.com/2012/10/12/world/panetta-warns-of-dire-threat-of-cyberattack.html*.

6. In a way, the United States and the North Atlantic Treaty Organization (NATO) did respond to the needs of Estonia and Georgia faced with cyberattacks from Russia several years ago, for example, with sanctuary servers, and establishing a cooperative cybersecurity think tank in Tallin.

7. Analysis of that crisis has become a cottage industry. Without a lengthy diversion, suffice it to say that President John Kennedy was not aware of steps taken by the U.S. military that intensified threats to the Soviet Union before and during the crisis, and that a peaceful outcome resulted in part from command-and-control breakdowns on the Soviet side. See Michael Dobbs, "The Price of a 50-Year Myth," *The New York Times*, October 16, 2016, available from *nytimes.com/2012/10/16/opinion/the-eyeball-to-eyeball-myth-and-the-cuban-missile-crisiss-legacy.html*; Sheldon M.

Stern, *The Cuban Missile Crisis in American Memory*, Stanford, CA: Stanford University Press, 2012. For a thoughtful exploration of the challenges of a cyberequivalent of the Cuban Missile Crisis, see Phil Williams, "Strategy for Infrastructure Protection and Crisis Management in the Cyber Age: An Elusive Quest?" in Denis Caleta and Paul Shemella, eds., *Counterterrorism Challenges Regarding the Process of Critical Infrastructure Protection*, Ljubljana, Slovenia: Publishing Houses Institute for Cooperative Security Studies, and Center for Civil-Military Relations, Monterey, CA, September 2011.

8. General Keith B. Alexander, "MEMORANDUM FOR RECORD, Subject: United States Cyber Command (USCYBERCOM) Commander's Strategic Assessment for Operating in Cyberspace—Preventing a Pearl Harbor Environment," Ft. Meade, MD: United States Cyber Command, March, 2012; General (Ret.) Larry Welch, "Keynote Address: Strategic Cyber Deterrence," Nov. 1-2, 2007, Sheraton Premier at Tysons Corner, VA. Secrecy was a central feature of the nuclear weapons program during and after World War II, including about the effects of weapons development facilities and weapons tests on U.S. citizens.

9. I have in mind far less conventional attacks than the missiles intercepted by Israel's defensive systems (e.g., Iron Dome) originating from adversaries in locations which are less readily monitored than those in Gaza. As with Patriot systems in the Gulf War, initial reports of the high effectiveness of Iron Dome are suspect.

10. Reports concluding that the U.S. infrastructure is highly vulnerable to simple physical threats have appeared at least since the early-1970s. The National Academy of Sciences recently found an abundance of such vulnerabilities. See Matthew L. Wald, "Terrorist Attack on Power Grid Could Cause Broad Hardship, Report Says," *The New York Times*, November 15, 2012, available from *nytimes.com/2012/11/15/science/earth/electric-industry-is-urged-to-gird-against-terrorist-attacks.html*; and his "Attack Ravages Power Grid (Just a Test.)," *The New York Times*, November 15, 2013, available from *nytimes.com/2013/11/15/us/coast-to-coast-simulating-onslaught-against-power-grid.html*.

11. For example, conventional weapons during World War II certainly were instruments of mass destruction for residents of Dresden and Hamburg, Germany, and Tokyo, Japan.

12. Even the vaunted evaluation process in the Richard Nixon White House associated with strategic arms control breakthroughs with the Soviet Union paid more attention to the risks from possible agreements than the risks from not having agreements. A number of arms control agreements negotiated under various U.S. presidents have never been ratified by the Congress, or only after tortuous bargaining to extract increased spending on nuclear weapons.

13. For example, in defending West Germany, NATO tactical nuclear weapons might well have devastated Germany and Poland more than Russia. If Russia accepted a limitation to West European targets, the United States would have been left intact. More simply, how would one attach a valid score to losing a cultural treasure versus damage to a factory? Even if feasible, officials of the attacker and the target might well disagree.

14. In general, the Russians have taken the initiative to conclude cyber "arms limitation" agreements. Negotiations begun with the United States in 2009 concluded in a bilateral agreement in June 2012. The agreement has narrow information exchange provisions like early nuclear agreements intended to curb possible misjudgments about threats and make cyberspace more stable. The length of negotiations and their limited focus hardly suggests urgency. See Ellen Nakashima, "In U.S.-Russia Deal, Nuclear Communication System May Be Used for Cybersecurity," *The Washington Post*, April 16, 2012, available from *https://www.washingtonpost.com/world/national-security/in-us-russia-deal-nuclear-communication-system-may-be-used-for-cybersecurity/2012/04/26/gIQAT521iT_story.html*; Elizabeth Montalbano, "U.S., Russia Forge Cybersecurity Pact," *Information Week*, July 12, 2011 available from *darkreading.com/risk-management/us-russia-forge-cybersecurity-pact/d/d-id/1098871*.

15. Attempts to create a broader international government-centered regime have foundered, as with the recent Dubai International Telecommunications Conference. In that case, the United States rejected an agreement it largely had shaped

apparently to avoid any whiff of changes in the current Internet regime. See Eric Pfanner, "U.S. Rejects Telecommunications Treaty," *The New York Times*, December 14, 2012, available from *nytimes.com/2012/12/14/technology/14iht-treaty14.html*; Eric Pfanner, "Message, if Murky, From U.S. to the World," *The New York Times*, December 15, 2012, available from *nytimes.com/2012/12/15/technology/in-a-huff-a-telling-us-walkout.html*. Less government centered initiatives continue, for example, the Worldwide Cybersecurity Initiative of the East West Institute, eastwest.ngo/. The Institute played a not dissimilar track 2 role on other security matters during the Cold War.

16. For example, see Jack Goldsmith "Cybersecurity Treaties: A Skeptical View (February 2011)," in Peter Berkowitz, ed., *Future Challenges in National Security and Law*, available from *futurechallengesessay.com*; Adam Segal and Matthew C. Waxman, "Why a Cybersecurity Treaty Is a Pipe Dream," Council on Foreign Relations (CFR), October 27, 2011, available from *cfr.org/cybersecurity/why-cybersecurity-treaty-pipe-dream/p26325*.

17. For example, National Security Advisor Thomas Donilon's call for China to get tough on hackers based there and negotiate "acceptable norms of behavior in cyberspace." See Mark Landler, "U.S. Demands That China End Hacking and Set Cyber Rules," *The New York Times*, March 12, 2013, available from *nytimes.com/2013/03/12/world/asia/us-demands-that-china-end-hacking-and-set-cyber-rules.html*.

18. Mazzetti and Shane. A cynical resident of the Washington, DC, area might suggest foreigners could just subcontract to PEPCO, a major regional electricity provider.

19. Those checks are no doubt unlikely to be perfect under any regime or military institution. That does not negate the desire of current power holders in governments democratic or not, civilian or not, theological or not, to retain control. For power holders, that makes them more receptive to offers of fail-safe technologies. For foreigners trying to hold them accountable, it means that proliferation conducive provisions from a state were explicitly or implicitly permitted by its nuclear custodians.

20. Consider the example of Sven Olag Kamphuis, the self-styled "minister of telecommunications and foreign affairs for the Republic of Cyberbunker" or that of Julian Assange. See Eric Pfanner, "Provocateur Comes Into View After Cyberattack," *The New York Times*, March 2013, available from *nytimes.com/2013/03/30/business/global/after-cyberattack-sven-olaf-kamphuis-is-at-heart-of-investigation.html*.

21. The Department of Defense has put cyberweapons development and one assumes procurement on a rather fast track, waiving some time consuming process requirements. See Ellen Nakashima, "Cyberweapons on Pentagon Fast Track," *The Washington Post*, April 10, 2012, available from *highbeam.com/doc/1P2-31117119.html*. It remains to be seen whether these steps will surmount prevailing institutional culture and the downside of accepting and using less than fully tested cyberinstruments.

22. That is according to then Obama advisor John Brennan who has become director of the Central Intelligence Agency. See John O. Brennan, "Shoring Up Cyberdefenses," *The Washington Post*, April 15, 2012, available from *https://washingtonpost.com/opinions/time-to-protect-against-dangers-of-cyberattack/2012/04/15/gIQAdJP8JT_story.html.*

23. There is generally little new about such concerns as with China's Huawei firm building in trap doors to telecom equipment. See John Pomfret, "Between U.S. and China, a Trust Gap: NSA Warned AT&T Against Using Chinese Firm for Fear of Spying," *The Washington Post*, October 8, 2010, available from *washingtonpost.com/wp-dyn/content/article/2010/10/07/AR2010100707210.html*. The Snowden materials provide ample grounds for foreigners to have similar concerns about major U.S. information technology and telecommunications firms For examples, see Nicole Perlroth and John Markoff, "N.S.A. May Have Hit Internet Companies at a Weak Spot," *The New York Times*, November 25, 2013, available from *nytimes.com/2013/11/26/technology/a-peephole-for-the-nsa.html.*

24. The Obama administration continues to press for cybersecurity standards to be required of firms. The experience with encryption software raises the possibility that the standards would ensure electronic U.S. Government access. Statements from the U.S. Cyber Command and actions by other agencies suggest the

goal of authorization for officials to pursue cybersecurity and cybersurvivability through blanket access to cyberflows into the United States. See Mark Mazzetti and David E. Sanger, "Security Leader Says U.S. Would Retaliate Against Cyberattacks," *The New York Times*, March 12, 2013, available from *nytimes.com/2013/03/13/us/intelligence-official-warns-congress-that-cyberattacks-pose-threat-to-us.html*. The Administration backed Cyber Intelligence Sharing and Protection Act would further reduce privacy protections for electronic communications. See Grant Gross, "Civil Liberties Groups: Cyberthreat Sharing Bill Still Attacks Privacy," PCWorld, April 17, 2012, available from *pcworld.com/article/253967/civil_liberties_groups_cyberthreat_sharing_bill_still_attacks_privacy.html*.

25. American firms and government bureaus have supported the use of social media and the Internet more generally to facilitate dissident efforts at mobilization and securing international support including the Greens in Iran and initial stages of the Arab Spring—activities widely known in international information security circles. At the same time, the United States has not obstructed export to most countries of surveillance, tracking, and filtering technologies that a regime can use to control opposition. Neither has Britain. See Sharon LaFraniere and Jonathan Ansfield, "China Alarmed by Security Threat from Internet," *The New York Times*, February 11, 2012, available from *nytimes.com/2010/02/12/world/asia/12cyberchina.html*; Nicole Perlroth, "Software Meant to Fight Crime Is Used to Spy on Dissidents," *The New York Times*, August 30, 2012, available from *nytimes.com/2012/08/31/technology/finspy-software-is-tracking-political-dissidents.html*; John Markoff, "Rights Group Reports on Abuses of Surveillance and Censorship Technology," *The New York Times*, January 16, 2013, available from *nytimes.com/2013/01/16/business/rights-group-reports-on-abuses-of-surveillance-and-censorship-technology.html*.

26. Almost no form of foreign cyberinterference in the internal affairs of other countries and communities lacks precedents using older means. Interference ranging from propaganda operations to currency manipulations has a long, if not necessarily honorable, history.

27. As illustrated by the collapse of the Dubai negotiations when the United States would not accept any indication of add-

ing the political basket (information security) to the economic/commercial one. Narrowly, military instruments and uses may or may not be separable either technologically or in terms of arriving at and implementing self-restraint agreements.

28. Ronald Deibert, "Cybersecurity: the new frontier," *Great Decisions*, 2012 Ed., New York: Foreign Policy Association, 2012, pp. 45-58.

29. Governments have undoubtedly manipulated intelligence about nuclear weapons through intentional actions of transparency as well as deception.

30. Nicole Perlroth, David E. Sanger, and Michael S. Schmidt, "As Hacking Against U.S. Rises, Experts Try to Pin Down Motive," *The New York Times*, March 3, 2013, available from *nytimes.com/2013/03/04/us/us-weighs-risks-and-motives-of-hacking-by-china-or-iran.html*.

31. The Pearl Harbor analogy was used by Panetta, and the wealth transfer claim was made by Alexander. See "Remarks by Secretary Panetta on Cybersecurity to the Business Executives for National Security, New York City," LawFare, October 11, 2012, available from *https://www.lawfareblog.com/secdef-panetta-speech-cybersecurity; Cybersecurity and American Power*, Washington, DC: American Enterprise Institute, July 9, 2012, available from *aei.org/events/cybersecurity-and-american-power/*.

32. The call by Donilon, noted previously, was met with a Chinese call for "rules and cooperation" that was accompanied by the Foreign Minister calling out Washington—"Anyone who tries to fabricate or piece together a sensational story to serve a political motive will not be able to blacken the name of others nor whitewash themselves." See David Barboza, "In wake of Cyberattacks, China Seeks New Rules," *The New York Times*, March 10, 2013, available from *nytimes.com/2013/03/11/world/asia/china-calls-for-global-hacking-rules.html*.

33. The essential difficulties have been recognized repeatedly. See Zalmay Khalilizad, "Defense in a Wired World: Protection, Deterrence, and Prevention," *Strategic Appraisal: The Changing Role of Information in Warfare*, Zalmay Khalilizad, John P. White, and

Andrew Marshall, eds., Santa Monica, CA: RAND, 1999, pp. 403-37; Martin C. Libicki, *Cyberdeterrence and Cyberwar*, Santa Monica, CA: RAND, 2009; Committee on Deterring Cyberattacks, "Letter Report from the Committee on Deterring Cyberattacks: lnforming Strategies and Developing Options for U.S. Policy," Washington, DC: National Research Council, 2010.

34. Jack Goldsmith's blog provides some interesting comments on the Panetta remarks in his, "The Significance of Panetta's Cyber Speech and the Persistent Difficulty of Deterring Cyberattacks," available from *lawfareblog.com/significance-panettas-cyber-speech-and-persistent-difficulty-deterring-cyberattacks*.

35. Alexander (Endnote 8) has said we want to be able to respond at cyberspeed which seems in considerable tension with requiring presidential approval.

36. Compare the account in Ellen Nakashima, "In Cyberwarfare, Rules of Engagement Still Hard to Define," *The Washington Post*, March 10, 2013, available from *washingtonpost.com/world/national-security/in-cyberwarfare-rules-of-engagement-still-hard-to-define/2013/03/10/0442507c-88da-11e2-9d71-f0feafdd1394_story.html* with that in David E. Sanger and Thom Shanker, "Broad Powers Seen for Obama in Cyberstrikes," *The New York Times*, February 3, 2013, available from *nytimes.com/2013/02/04/us/broad-powers-seen-for-obama-in-cyberstrikes.html*. Also, see Endnote 44.

37. Consider the shifting public attributions by South Korean officials to a recent cyberattack on parts of that nation's banking system. Originally supposedly generated in China, that was changed in a few hours to a domestic origin. See Hoe Sang-Hun, "South Korea Says It Misidentified Source of Cyberattack," *The New York Times* March 22, 2013, available from *nytimes.com/2013/03/23/world/asia/south-korea-says-it-misidentified-source-of-cyberattack.html?_r=0*. South Korea is one of the more vigilant countries about cybersecurity especially with regard to prospects of attacks from North Korea and China. The dangers of misattribution or misinterpretation are particularly great when the parties have only tenuous direct communications and view each other as implacably and irrationally hostile.

38. Structurally, this would be like putting Curtis LeMay in charge of Strategic Air Command and strategic and tactical nuclear intelligence collection and analysis during the early years of the Cold War. Recent concerns with the two-hatted current arrangement may stem more from bureaucratic rivalry between and within the Department of Defense and the intelligence agencies than the concern expressed here.

39. To quote Alexander, "This defend-the-nation team is not a defensive team. . . . This is an offensive team that the Defense Department would use to defend the nation if it were attacked in cyberspace." See Mark Mazzetti and David E. Sanger, "Security Leader Says U.S. Would Retaliate Against Cyberattacks," *The New York Times*, March 12, 2013, available from *nytimes.com/2013/03/13/us/intelligence-official-warns-congress-that-cyberattacks-pose-threat-to-us.html*.

40. David E. Sanger, John Markoff, and Thom Shanker, "U.S. Steps Up Effort on Digital Defenses," *The New York Times*, April 27, 2009, available from *nytimes.com/2009/04/28/us/28cyber.html*; Christopher Drew and John Markoff, "Contractors Vie for Plum Work, Hacking for U.S.," *The New York Times*, May 30, 2009, available from *nytimes.com/2009/05/31/us/31cyber.html*; John Markoff and Thom Shanker, "Halted '03 Iraq Plan Illustrates U.S. Fear of Cyberwar Risk," *The New York Times*, August 1, 2009, available from *nytimes.com/2009/08/02/us/politics/02cyber.html*; Corey Kilgannon and Noam Cohen, "Cadets Trade the Trenches for Firewalls," *The New York Times*, May 10, 2009, available from *nytimes.com/2009/05/11/technology/11cybergames.html*; Committee on Offensive Information Warfare, National Research Council, William A. Owens, Kenneth W. Dam, and Herbert S. Lin, eds., *Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities*, Washington, DC: National Academy of Sciences, 2009.

41. Karen DeYoung, "Brennan Reshaped Anti-Terror Strategy," *The Washington Post*, October 25, 2012, available from *pulitzer.org/files/finalists/2013/washpostnational2013/washpostnational03.pdf*.

42. The analogy is, of course, to Stuxnet/Olympic Games, Iran, and cyberattacks on the Saudi Arabian Oil Company (ARAMCO), and U.S. banks. See Andrea Shalal-Esa, "Iran Strengthened Cyber Capabilities After Stuxnet: U.S. general," Reuters,

available from *reuters.com/article/2013/01/18/us-iran-usa-cyber-idUSBRE90G1C420130118*; Nicole Perlroth and Quentin Hardy, "Bank Hacking Was the Work of Iranians, Officials Say," *The New York Times*, January 8, 2013, available from *nytimes.com/2013/01/09/technology/online-banking-attacks-were-work-of-iran-us-officials-say.html*; Nicole Perlroth, "In Cyberattack on Saudi Firm, U.S. Sees Iran Firing Back," *The New York Times*, October 23, 2012, available from *nytimes.com/2012/10/24/business/global/cyberattack-on-saudi-oil-firm-disquiets-us.html*.

43. For an analysis of the factors other than U.S. strategy pushing in that direction, see Nazli Choucri, *CyberPolitics in International Relations*, Cambridge, MA: MIT Press, 2012.

44. A summary of the February 2012 *Sigint Strategy 2012-2016* appears in James Risen and Laura Poitras, "N.S.A. Report Outlined Goals for More Power," *The New York Times,* November 22, 2013, available from *nytimes.com/2013/11/23/us/politics/nsa-report-outlined-goals-for-more-power.html*. The quotes are from the NSA document itself.

45. "Broad Agency Announcement: Foundational Cyberwarfare (Plan X)," DARPA-BAA-13-02, Washington, DC: Defense Advanced Research Projects Agency, November 20, 2012. The document disclaims interest in cyberweapons related technologies while calling for American military superiority in cyberwar.

CHAPTER 14

IDENTIFYING THE REAL AND ABSOLUTE ENEMY

Rob van Kranenburg

> But I could imagine, the logical consequence of the Internet of Things is not just a new philosophy of how we can control our production and logistics. It completely changes the paradigms of sequences of operations. . . . The future is not predictable! But we try to predict our future every day. . . . The future will be self-controlled and service-oriented, in other word: the Internet of Things and Services.[1]

TO PREDICT

In his "Wired Opinion, The Internet of Things Has Arrived—And So Have Massive Security Issues," Andrew Rose falls into his own blind spot. It is not an obvious one. In fact, he seems to agree that we cannot predict how things will turn out. He says:

> I am hard-pressed to find a catastrophic scenario associated with the refrigerator—other than the refrigerator spending your entire month's pay on milk or becoming self-aware like Skynet—but the fact remains we can't predict how things will look. That makes regulation and legislation difficult.[2]

This is indeed the thing we humans tend to do: we either underestimate or overestimate. Over a century ago, John Elfreth Watkins, Jr., published "What May Happen in the Next Hundred Years" in *The Ladies Home Journal,* December 1900. His Prediction #4 is not one of his best guesses:

> Prediction #4: There Will Be No Street Cars in Our Large Cities. All hurry traffic will be below or high above ground when brought within city limits. In most cities it will be confined to broad subways or tunnels, well lighted and well ventilated, or to high trestles with "moving-sidewalk" stairways leading to the top. These underground or overhead streets will teem with capacious automobile passenger coaches and freight with cushioned wheels. Subways or trestles will be reserved for express trains. Cities, therefore, will be free from all noises.[3]

Watkins extrapolated from the vision of mobility of trams, trains, and subways, and as a result, could not envision the massive number of cars that would come to congest most cities. Closer to home, in 2001, when interviewed by Charlie Schmidt, then vice president of technology at Automatic Identification and Mobility (AIM), a trade association for manufacturers of tagging radio-frequency identification (RFID) technology, Steve Halliday claimed: "If I talk to companies and ask them if they want to replace the bar code with these tags, the answer can't be anything but yes. It's like giving them the opportunity to rule the world."[4]

All of these thinkers are able to accept massive change at one level while keeping others constant. Halliday is correct to assess the potentially disruptive character of RFID and, by extension Internet of Things (IoT), but could not or would not consider that the Internet, open source software, and open hardware is empowering not only companies he represented or envisaged, but also, a messy field of crowd-funded start-ups. In a similar vein, Andrew Rose stated:

> Given the wide-reaching impact of the IoT, formal legislation and government involvement is almost

> certain. Especially when we consider the safety risks of automated systems interacting in the physical world—governments won't be able to stand by silently if autonomous decisions endanger lives.[5]

In other words, Rose foresees all kinds of risks but insists that government as such will still be able to "ensure" anything. Yet, is this not as realistic as taking the opposite view by arguing that in different ages different agencies over resources defined power, and IoT might represent such a change? If that is the case, there is no longer any government, as we know it.

The discrepancy between what will change and what will remain constant thus seems to be only partly due to discerning data from noise, as it is a recurring issue in all predictions of the future.

BIOLOGICAL AND EVOLUTIONARY CONSTRAINTS TO CHANGE

"DNA ties us all together; we share ancestry with barracuda and bacteria and mushrooms, if you go far enough back."[6] Spencer Wells shows in his Genographic Project through our shared DNA how we are—in all our diversity—truly connected.[7] He argues that it was 10,000 generations or 50,000 years ago (relatively recent in evolutionary terms) that language and non-domain related expression (arts) kick-started toolsets that led to the cultural, social and artistic intricacies that we have today.[8] Before that, the cognitive tools and material toolsets appear to be quite constant over a long period. The difference was made by language acting as a tool for cooperation and negotiating. Both the explosion of variety in practices and tools and many of the crises we confront today have their roots, and he argues, in the dawn of the Neolithic:

> We spent an enormous amount of time as hominids and as primates living as hunter-gatherers. That is the natural way for us to live, and we're suddenly living in this profoundly unnatural way, and we're still in the process of adapting to it and working out how to live with it. . . . We were once used to living in groups of no more than about 150 individuals. Now we live in cities of millions and the cultural cacophony creates a feeling of unease and we are seeing evidence of that with the rise of mental illness.[9]

Wells believes there is hope—what he calls "Pandora's seed." "When Pandora opened the box, she at least had to slap it shut fast enough to contain hope. . . . The hope is that humans are innately innovative and that we can innovate very rapidly when we're forced to." [10]

REAL AND ABSOLUTE ENEMIES

Carl Schmitt distinguishes between *der Wirkliche Feind* and the *Absolute Feind* (the real enemy and the absolute enemy). The latter is "*die eigene Frage als gestalt*" (His own question as shaped). The absolute enemy is the inability to change convictions, alliances, and opinions. The absolute friend is always very near to you, consisting of everyday routine skills; it is your blind spot. The real enemy can differ from time to time and period to period. Each historical situation demands the capabilities to define as those real enemies the ones that can redefine all that you hold normal, dear, and take for granted. It is clear that only rarely do these threats to ontologies, (what you "are," what you hold yourself to "be," what you believe to be "normal," "just," and "fair") lead to classical or asymmetric warfare. One cannot fight depression, weather,

climate change, or religious beliefs, because there is no clear definition of what a victory would mean—other than having things **not** happen. Nor can temporary success be clearly defined. Most important, however, these situations offer no context or markers—openings—to make an informed choice about the kind of weapons that could either be used for defense or offense.

ENERGY

War is about energy, not necessarily about people. In the days of the battle of Culloden Moor, Scotland, arms smashing other arms got tired and gave way. Richard Overy shows in *Countdown to War* (2009) that the decision to go to war in 1939 was made on both sides in a state of "growing irrationality."[11] Protagonists on either side were dead tired. The decision to go to war came as a **relief** to them. By then, the technologies of war had advanced to such an extent that battles could be prolonged potentially indefinitely. Armor tires in a much slower way. Robots do not get weary at all and need no sleep. According to Ronald Arkin, a roboticist at the Georgia Institute of Technology, who is developing ethics software for armed robots by crunching data from drone sensors and military databases, it might be possible to predict, for example, that a strike from a missile could damage a nearby religious building. Clever software might be used to call off attacks as well as initiate them.[12] Still, as long as the machines cannot pay for themselves, it is people who make decisions on who does what kind of fighting and where. Human beings still decide on the nature of war, the definition of a threat, an asset, a risk, and the vital necessities and resources that are

deemed necessary to live. Yet, it is clear that the kind of intelligence that is most apt to make these decisions differs from the times of Culloden; Stalingrad, Russia; and Operation EAGLE CLAW in Iran.

In the age of the battles of men, all was analogue. What you saw is what you got and smelled as you heard the murmurs and sighs of men bleeding to death, with feet, arms, or legs chopped off. There was innovation in tactics, in choosing terrain, in the choice of weapons, but in this space where men were still seeing other men kill or be killed, innovation in the face of unknown outcomes has always followed certain rules and procedures.

When tanks became decisive in World War II, each bloc innovated along its own strengths and weaknesses (German Tiger, Soviet T-34, and Allied Sherman). None of the three blocs invented something significantly different or another mode of fighting. Indeed, all three stayed within conventional thinking and innovation within their own particular sensibilities and cultural schemata under certain specifications and requirements, to be validated in action, immediately enabling rapid feedback and improvement cycles, clear goals and objectives, and a clear win or lose scenario. Unsurprisingly, this situation has become the natural habitat of innovation: companies grow big and compete with each other on details building corporate branding, innovate under specific requirements, validate in real time, immediately enabling rapid feedback and improvement cycles, and demand clear goals and objectives and win or lose scenarios.

After World War II, the entire field of operations was taken to a different level where analogue contexts no longer defined the course of action, policy, and the direction of future investments. The RAND Corpora-

tion took the battlefield to space, thereby introducing and eventually rendering the axiomatic drivers to the digital age of computers and coding.

It was the clear insight of the military commanders and political leadership that the new operational fields would require a new kind of intelligence to lead and co-direct alongside traditional military expertise: the speculative and creative engineer-researcher who was able to define his very own new territory where there was none before. In this context, it was RAND that saw space as a way to harness and direct operational resources anywhere on the planet. RAND was able to embody and direct at the same time a cultural, social, and political shift toward a beginning of evidence-based policy and research and development (R&D), building up datasets that were to be used as input for policymakers. In order to do this, it literally created its own axiomatic borders and playing ground. It therefore built a new ontology alongside the old one of traditional and analogue warfare. This new ontology posed new questions, created new definitions of threat, risk, assets, security, and even the very nature of war. RAND was able to do this because of a balance of disciplines and funding, choice of use cases, and building of new methodologies:

First, was the profound understanding by the military and political leadership of the deep nature of the change that was needed to face the consequences of a reality that had been shaped by the tools of the day. As Commanding General of the Army Air Force, H. H. "Hap" Arnold wrote in a report to the Secretary of War:

> During this war the Army, Army Air Forces, and the Navy have made unprecedented use of scientific and

> industrial resources. The conclusion is inescapable that we have not yet established the balance necessary to insure the continuance of teamwork among the military, other government agencies, industry, and the universities. Scientific planning must be years in advance of the actual research and development work.[13]

Second, was understanding the importance of choosing the right use case, that, in its successful design, showed more than the mastering of certain skills and techniques. In this connection, the emphasis on space was prescient. As the special memoranda abstract summarizing Project RAND working papers and follow on reports noted:

> . . . the most riveting observation, one that deserves an honored place in the Central Premonitions Registry, was made by one of the contributors, Jimmy Lipp, head of Project RAND's Missile Division, in a follow-on paper 9 months later: 'Since mastery of the elements is a reliable index of material progress, the nation which first makes significant achievements in space travel will be acknowledged as the world leader in both military and scientific techniques. To visualize the impact on the world, one can imagine the consternation and admiration that would be felt here if the United States were to discover suddenly that some other nation had already put up a successful satellite.'[14]

Third was a recognition of the need for new methodologies. This was evident in the introduction of the first report of Project RAND, *Preliminary Design of an Experimental World-Circling Spaceship*, released May 2, 1946, from the key passage found on page 4:

> It cannot be emphasized too strongly that the primary contributions of this report are in methods, and not in the specific figures in this design study. One point

> in particular should be highlighted: - the design gross weight, which is of the greatest importance in estimating cost or in comparing any two proposals in this field is the least definitely ascertained single feature in the whole process. . .The most important thing is that a satellite vehicle can be made at all in the present state of the art.[15]

The successful combination of A, B, and C—balance of disciplines and funding, choice of use cases, and building of new methodologies—is rare. When it succeeds, however, it means a period of hegemonic and infrastructural domination, as we have witnessed in the leadership of America until now. Unless the United States is able to repeat this process, it will lose this leadership.

In an American context, it was RAND that managed the transition from Culloden, Antietam, and Stalingrad to space. The transition to robotic warfare, however, has to be negotiated by a network of varied and widely diverging skillsets that allow for conflict **inside** the network.

THE INTERNET AND THE INTERNET OF THINGS

In a future world of super-senses, as Martin Rantzer of Ericsson Foresight has argued, "new communication senses will be needed . . . to enable people to absorb the enormous mass of information with which they are confronted."[16] He also claimed that the user interfaces we use today to transmit information to our brains threaten to create a real bottleneck for new broadband services. Implementing digital connectivity in an analogue environment without a design for all the senses leads to information overload.

In a ubiquitous computing (ubicomp) environment, the new intelligence is extelligence, "knowledge and tools that are outside people's heads."[17]

Against this background, we are currently on the verge of witnessing the emergence of a:

> mega-market, where markets such as home and building automation, electricity generation and distribution, logistics, automotive as well as telecommunication and information technology will steadily converge. We do not know the consequences of connecting all these smart objects (smart meter, e-vehicle, cargo container, fridge etc.) to the Internet.[18]

Professor Michael ten Hompel, Managing Director of the Geschäftsführender Institutsleiter, Fraunhofer-Institut Materialfluss und Logistik (Fraunhofer Institute for Material Flows and Logistics), described the consequences this has for something as "solid" as logistics:

> The logical consequence of the Internet of Things is not just a new philosophy of how we can control our production and logistics. It completely changes the paradigms of conventional supply chain management. Within the Internet of Things the supply chain will be created in real time: *Entities*, consisting of objects and a piece of (agent based) software, generate the resulting supply chain on the move. Therefore the sequences of operations are not predicted. This leads to a new understanding of how to handle our logistic management which won't be a supply chain (!) anymore.[19]

Ten Hompel is not a Science Fiction writer; nor is he is projecting a vision. He is simply describing an emergent reality that, to a large extent, is already here.

It is important to understand that the Internet and the IoT combined change the very nature of power.

Psychologists specialized in the behavior of larger groups of people explain:

> . . . the relative ease with which one is able to exert influence over masses by assuming a causal force which bears on every member of an aggregate, and also for each individual there is a large number of idiosyncratic causes. Now let us suppose that the idiosyncratic forces that we do not understand are four times as large as the systematic forces that we do understand. . . . As the size of the population increases from 1 to 100, the influence of the unknown individual idiosyncratic behaviour decreases from four times as large as the known part to four tenths as large as the known part. As we go to an aggregate of a million, even if we understand only the systematic one-fifth individual behaviour as assumed in the table, the part we do not understand of the aggregate behaviour decreases to less than 1 percent (0.004).[20]

This shows how top-down power works and why **scaling** has become such an important indicator in such a system of "success." Imagine you want to start a project or do something with your friends or neighbors, say five people. This means that you have to take into account before you do anything—state a goal, negotiate deliverables, or even a first date on which to meet for a kick-off—that all five people relate to huge idiosyncrasies and generic forces that have to be aligned or overcome before you can even say hello. This shows how difficult it is to start something. It also explains why you are always urged to get bigger and why you need to grow. It is only then and through the process of getting bigger itself that the management tools can operate, lying in wait for you to discover them. To be decisive, make a difference, to set about a course for change is in no need of growth. Under-

standing the nature of these social relations in these terms shows how difficult it is to script moments of fundamental change, as hierarchical systems by the very fact that they are top down can concentrate on managing systematic forces relatively effortlessly.

With the Internet, however, these idiosyncrasies have been able to organize and raise their weight in the ratio, and the IoT will allow these even further, bringing the sensor network data sets to individuals who can handle them on their devices. This acceleration of weak signals into clusters, organized networks, and flukes cannot be managed anymore by formats that are informed by and that inform systematic forces as the **nature of these forces** have changed.

Thus, it is always difficult for policy to deal with systemic change. It is extremely natural for it to see the above operation as an **attack** on its system and not as a **new iteration** caused by the hegemonic forces it has allowed to operate: education, freedom of speech, consumerism, and the Internet. In nearly all instances, we see revolutions break down in such constellations. It is also understandable that **super-empowered individuals** identified by state and intelligence actors are a major threat to the system (democratic capitalism) as a whole.[21] In the light of the above discussion about the new environment, however, this is not a threat, but an **opportunity**.

In our current architectures, we are used to dealing with three groups of actors: citizens/end users; industry/subject matter experts; and those involved in governance/legal matters. These all are characterized by certain qualities. In our current models and architectures, we build from and with these actors as entities in mind. The data flow of IoT will engender new entities consisting of different qualities taken from the former three groups diminishing the power of the tra-

ditional entities. The IoT will break them. It will force a divorce. This divorce can be brutal or friendly.

If we want to define power to its core, we can say that it is the self-assigned agency of states to assign numbers to people (legal-illegal), and the self-assigned agency of companies to isolate data in Internet Protocol and copyright and patents (legal-illegal). They are wed together. Without the former, the latter has no capability to enforce any laws. Without the second, the first has no capacity to ensure that citizens do not start to question why they should keep paying taxes, as some level of convenience is provided.

The Internet brought this wedding into question as the only possibility to posit as a foundation for everyday life and praxis. It revealed how much legacy is actually still in this combination built on violence, isolation of data, and (preferably phrased as "healthy") competition. A quick look at the top 100 companies before and after the Internet shows how disruptive the Internet is.

IoT means full traceability, and not one thing is unmonitored or out of sight. All and everyone are in full light. There will be no more users who need to secure privacy, as the concept of privacy has to be distributed over the qualities of the new actors. There will be cookies on the table you put your cup on, and, no, you do not want to be notified how long this table will store the information that you had an espresso there.

It enables new forms of work, redefining what a "job" is:

> By 2020, more than 40% of the U.S. workforce will be so-called contingent workers, according to a study conducted by software company Intuit in 2010. That is more than 60 million people. We are quickly becoming a nation of permanent freelancers and temps.[22]

Strangely:

> the Americans in their 20s and 30s who will be most affected by it remain decidedly upbeat. They are much more hopeful than older generations, polls show, that the country's future will be better than its past. Based on what younger adults have been through, that resilience is impressive. It's probably necessary, too. The jobs slump will not end without a large dose of optimism.[23]

All this is possible because of the monitoring capabilities that are embedded in these practices that enable business-to-business (B2B) and customer-to-customer (C2C) without third party costs on liability or accountability.

Another kind of service could consist of offering real-time threat analyses, showing that the threat of a terrorist attack for individuals is 0.0001 percent and, for the sake of argument, slipping and falling in the bathroom is 0.3 percent.[24] At an airport where people use Layar, Google Glasses, Twitter, and LinkedIn—and where nobody wants to be blown up—the worst thing that can happen is that erroneous information about fellow passengers is obtained from the accessible databases. In such an environment, more and more fatal misunderstandings can occur. Umar Farouk Abdulmutallab slipped through the net of the regular security dashboards. If we were to feel once again responsible for our own actions and safety, perhaps we would have intercepted him earlier.

In this new **conceptual** space, we have to build new notions of privacy, security, assets, risks, and threats tailored to a reality of today, not a reality of yesterday or further back in time. So our main question now is to

stare reality in the face and tell civil society and competing military doctrines to stop fighting lost causes from intrinsically untenable and un-fortifiable positions. To start a methodology that allows us to identify a number of real enemies and the absolute enemy that the U.S. military, and by definition, the United States (as the military takes about half of every tax dollar of citizens) is facing. It comes down to deciding when it is time to act out of a deep knowledge that the current situation is untenable. Unfortunately, the analysis of the situation leaves different stakeholders with different timeframes. Nevertheless, there are ways forward.

In his seminal text, *The Social Order of a Frontier Community*, Don Harrison Doyle wrote, "social conflict was normal, it was inevitable, and it was a format for community decision making."[25] Sociologist Lewis Coser also advised that, instead of viewing conflict as a disruptive event signifying disorganization:

> We should appreciate it as a positive process by which members of a community ally with one another, identify common values and interests, and organize to contest power with competing groups.[26]

The new environment of the IoT will resemble these "frontier communities" because of their seeming disorganization where conflict will be the norm.

We are in need of a new iteration of a successful combination of A, B, and C, a balance of disciplines and funding, choice of use cases, and building of new methodologies. It is difficult, but whoever succeeds will enter a new period of hegemonic and infrastructural domination. A means negotiating real and absolute enemies with new stakeholders such as the open source community, the WikiLeaks Crew, and Anonymous Hackers, Bradley Manning, the activists of Open

Hardware, Software, Innovation, and Data. For B, the use cases must be novel, real, and testify to the creation of new kinds of knowledge of material processes. When Steve Jobs returned to Apple in 1997, one of the first things he did was close down the Advanced Research Group, saying research needs to be done in the crucible of development. Low hanging fruit for us in 2015 are, sewage systems, bridges, roads, and inner city development, in short taking the space metaphor back to Earth in a **smart**, **hybrid** way. C is about creating spaces for new definitions about what is data and what is noise that underpins new temporary forms of reading and outputting new combinations of sensor, visual, and text data.

Stated more baldly, it is clear as Global Futures Partnership noted:

> The increasing globalization of R&D, real-time diffusion of technical knowledge through international networks, and the convergence of advancing technologies are creating new challenges for global security. Innovations in such diverse areas as ICT, biological sciences, neuroscience, material sciences, nanotechnology, and robotics could provide hostile actors increasingly cheap access to a wide range of technologies. Destructive application potential of rapidly advancing innovations is compounded when the technological convergence is considered. Emerging and commercially available technologies can be used in novel and undesirable ways to achieve political, military, or monetary goals.

To meet this challenge, we just need a commanding general like Arnold to stare reality in the face and tell civil society and competing military doctrines to stop fighting lost causes from intrinsically untenable and unsustainable positions. To develop and implement

a methodology that facilitates the identification of a number of real enemies as well as the absolute enemy that the U.S. military and by definition the United States (as the military takes about half of every tax dollar of citizens) is facing. It is important to move ahead rapidly and decisively.

ENDNOTES - CHAPTER 14

1. Personal mail to the author by Professor Dr. Michael ten Hompel, who holds the Chair of Materials Handling and Warehousing at TU Dortmund University and is managing director at Fraunhofer-Institute of Material Flow and Logistics (IML).

2. Andrew Rose, "The Internet of Things Has Arrived—And So Have Massive Security Issues," Wired, January, 11, 2013, available from *wired.com/2013/01/securing-the-internet-of-things/*.

3. John Elfreth Watkins, Jr., "What May Happen in the Next Hundred Years," *The Ladies Home Journal*, December 1900, available from *yorktownhistory.org/wp-content/archives/homepages/1900_predictions.htm*.

4. Charlie Schmidt, "Beyond the Bar Code," *MIT Technology Review*, March 1, 2001, available from *technologyreview.com/featuredstory/400913/beyond-the-bar-code/*.

5. Rose.

6. Spencer Wells, "A family tree for humanity," TEDGlobal 2007, June 2007, available from *ted.com/talks/spencer_wells_is_building_a_family_tree_for_all_humanity*.

7. Spencer Wells, *The Journey of Man: A Genetic Odyssey*, Princeton, NJ: Princeton University Press, 2002; and New York: Random House, 2004, p. 75.

8. Wells, "A family tree for humanity."

9. *Ibid*.

10. Spencer Wells, *Pandora's Seed: The Unforeseen Cost of Civilization*, New York: Random House, 2010.

11. Richard Overy, *1939: Countdown to War*, New York: Viking, 2009.

12. "March of the Robots," *The Economist*, Technology Quarterly, 2nd Quarter Ed., June 2, 2012, available from *economist.com/node/21556103*.

13. *A brief history of RAND*, Santa Monica, CA: RAND, available from *rand.org/about/history/a-brief-history-of-rand.html*.

14. RAND, Special Memoranda, website abstract for the reports pertaining to Project RAND, available from *rand.org/pubs/special_memoranda/SM11827.html.*

15. *Preliminary Design of an Experimental World-Circling Spaceship,* Santa Monica, CA: RAND Corporation, 1946, available from *rand.org/content/dam/rand/pubs/special_memoranda/2006/SM11827part1.pdf,* p. 4.

16. Martin Rantzer, *Foresight Paper – All Senses Communication*, No. ERA/SVZ/R-01:029 Uen, Ericsson, 2001.

17. Ian Stewart and Jack Cohen, *Figments of Reality*, Cambridge, UK: Cambridge University Press, 1997.

18. Jens Strüker (*strueker@iig.uni-freiburg.de*) *et al*., on the LinkedIn Group, "Internet of Things," 2011.

19. Personal mail to the author by Professor Dr. Michael ten Hompel.

20. Arthur L. Stinchcombe, *Constructing Social Theories*, London, UK: The University of Chicago Press Books, 1968, pp. 67-68.

21. Rob van Kranenburg, "Transformational Technologies #4: Implications for an Expanding Threat Environment," presentation at workshop "Transformational Technologies: Implications for Global Security," Rome, Italy, September 17-18, 2012.

> This Global Futures Forum workshop is the fourth in a series titled 'Transformational Technologies: Implications for Global Security.' On behalf of the Global Futures Forum community, and in partnership with the Italian Intelligence Community, it is our honor to host this GFF workshop at Palazzo Salviati, Headquarters of Centro Alti Studi Difesa. All remarks will be unclassified, off the record, and not for attribution.

"If the pace of technology continues at this rate, greater technological change will occur in the next 20 years than has occurred in the whole of the 20th century. . . ." The Lipmann Report Eds., "Cyberterrorism: The Invisible Threat Stealth Cyber Predators in a Climate of Escalating Risk," *Foreign Affairs Magazine*, The Lippmann Report, November/December 2010.

22. Jeremy, Neuner, "40% of America's workforce will be freelancers by 2020," *Quarz*, March 20, 2013, available from *qz.com/65279/40-of-americas-workforce-will-be-freelancers-by-2020/*.

23. David Leonhardt, "The Idled Young Americans," *The New York Times*, May 3 2013, available from *nytimes.com/2013/05/05/sunday-review/the-idled-young-americans.html*.

24. *Preliminary Design of an Experimental World-Circling Spaceship,* p. 4. "It cannot be emphasized too strongly that the primary contributions of this report are in methods, and not in the specific figures in this design study."

25. Don Harrison Doyle, *The Social Order of a Frontier Community: Jacksonville, Illinois, 1825-70*, Urbana, IL: The University of Illinois Press, 1983.

26. Lewis A. Coser, "Social Conflict and the Theory of Social Change," *The British Journal of Sociology*, Vol. 8, No. 3, September 1957, pp. 197-207, available from *jstor.org/stable/586859*.

CHAPTER 15

COULD THE UNITED STATES BENEFIT FROM CYBER-ARMS-CONTROL AGREEMENTS?

Benoît Morel

PROLEGOMENON: CYBER-ARMS-CONTROL HAS BEEN DISCUSSED AND DISMISSED (BY MOST) LONG AGO.

WHY REVISE THE ISSUE NOW?

The apparently relentless cyberespionage originating in China did not exist to the same extent years ago and has become a bone of contention between the Chinese and U.S. governments. The U.S. Government has not developed efficient ways to defeat those cyberintrusions, let alone provide protection against cyberattacks on the rest of the country. That problem has no simple solution, as there is no known technological fix against attacks using spear phishing or exploiting one or more of the countless vulnerabilities buried in the software in use everywhere. The U.S. Government can hardly hope to accomplish much by taking a more offensive posture. Not only are U.S. offensive capabilities seriously limited at the moment (that could change), but also the United States—because of its level of dependence on technology—is far more vulnerable to cyberattacks than any of its present or potential foes. That situation will not improve soon, so something else should happen, because computers are absolutely central to the life of the U.S. Government and military.

Cybersecurity raises a new situation for the U.S. military and government, accustomed to basing the national security posture on significant technological superiority. Neither the U.S. Government nor its military establishment can claim to be leaders in cybersecurity. Critical expertise in cybersecurity resides safely outside government spheres of influence. Once in a while, Congress or the presidential administration comes out with some (much needed) potential legislation or executive orders. However, what the government produces tends to be useless or irrelevant and is sometimes even worse than doing nothing. The different branches of the government behave as if they have not yet adjusted to the "culture" of cybersecurity.

For good reasons (which have a lot to do with the fact that the government does not understand the problem well and does not know what to do about it) the U.S. Government is alarmed and refers to the cyberthreat as the most serious threat to U.S. security today. Against this background, it is important to consider once again whether international agreements can mitigate some of those concerns.

INTRODUCTION

Claims that the cyberthreat against the United States is out of control have become little more than platitudes—and this itself is very telling. As alluded to in the prolegomenon, the cyberstrategic posture of the United States is so bad that it has to devise a strategy from a position of inferiority. In its eagerness to correct that situation, if Congress comes out with ill-conceived legislation, this is neither by malice nor the result of partisan bickering. Most congressmen are genuinely preoccupied with other issues, but they are

also outsmarted and have serious difficulties in familiarizing themselves with the cybersecurity culture.

The cyberthreats of today take a variety of forms, cyberespionage being perhaps the most prominent. Protesting against the excessive aggressiveness of cyberespionage the way the U.S. Government often does is an unintended acknowledgment of helplessness. Espionage is the international relations equivalent of the oldest profession. It has always been an important component of international relations. The United States is not foreign to espionage; it invests more in intelligence than any other nation. During the Cold War, the Americans developed sophisticated technologies that they are now proud to showcase in a museum in Washington, DC. When it comes to that modern form of espionage called cyberespionage, however, the United States finds itself in an unfamiliar situation: it is at a disadvantage, in fact, at a serious disadvantage. The U.S. Government finds itself in the position of asking the Chinese to do something that no responsible government would do voluntarily; refrain from accessing valuable information.

All this is taking place at a time when the Internet is basically unregulated. Cybercriminality is a growing concern worldwide, and this lawlessness provides an excuse for those who advocate increased regulation. Can one imagine a regulatory framework (a form of "cyber-arms-control" agreement) that would be acceptable to all nations and could comprise an international cyberorder? What might this so-called cyber-arms-control look like? To be enforceable, it would need to be verifiable, desirable from the point of view of powerful nations like the United States, and acceptable to all others.

One immediate concern with introducing laws and regulations is the real possibility of unintended negative consequences. The anarchic nature of cyberspace has not yet acted as a hindrance for the ever-increasing reach and success of the Internet. Another problem is the political context in which multilateral discussions on regulating the Internet would take place. The infamous international conference that took place in Dubai, United Arab Emirates, in December 2012, showed that there were deep disagreements among key nations on some fundamentals.[1] In particular, there is a critical mass of nations interested in introducing regulations that target aspects of Internet life they find disruptive or subversive to their society, regime, or culture. This might take the form of the free movement of ideas or the content of some material posted online.

The United States and, in different ways, the rest of the world, have growing security concerns stemming from the Internet. A cyber-arms-control agreement should aim at alleviating those concerns. However, if there is a consensus on the fact that the Internet raises international security concerns, there is not, at least at this moment, international agreement on what those concerns are.

CYBER AGREEMENTS COULD TAKE DIFFERENT FORMS AND COVER A VARIETY OF THINGS

One effect of the unprecedented level of intrusive spying made possible by cybertechnology is that it redefines the security geography. The United States has far more to lose in the emerging technological environment than any other state. It has far more critical information, of both the military and nonmilitary

variety, accessible from the Internet. What the National Security Agency (NSA, the lone place for excellence in cybersecurity in the U.S. Government) can learn by penetrating as deeply as it does in the Chinese system is limited compared with what an average hacker based in China can learn from the United States by using relatively simple techniques. The reason for this is the United States has a lot more information that is difficult to protect in companies involved in national security and more technological secrets than any other country, especially China. Might international agreements lessen the impact of that asymmetric situation?

What kind of attacks could conceivably be covered by an international agreement? Cyberattacks can take many forms. Some are more "bellicose" in the sense that they target assets like critical infrastructures or attempt to do damage (cybersabotage), as opposed to the more common ones whose goal is to steal information (cyberespionage), not to mention those that qualify as cybercrime. The question of when a cyberattack constitutes an act of war is far from being solved. Moreover, the issue is further complicated by the question as to how this might be codified by a treaty. There is still an entire legal framework that must be developed before one can even discuss the subject cogently.

The first requirement of any good agreement is that it is verifiable, a vital prerequisite for being enforceable. This requirement undoubtedly would be difficult to meet fully today. Contrary to what is sometimes claimed, however, the problem of attribution is not completely intractable. Attackers use the protection of proxies, where the track disappears. Part of the reason is that some companies offer proxy servers as service, with impunity. Proxy servers (a major cause of the problem of attribution) do not need to be off-

limits to law enforcement of the country in which they are located. One possible solution might be to hold governments responsible for all malicious cyberactivities originating from their territories, even if these activities are carried out through proxy servers.

Even were such a concept to be accepted, the success of this approach would require the support of all nations. Otherwise, there would still remain shelters for international attacks, as cyberattackers have the ability to hijack computers in any country. Furthermore, an attack could have many legs; that is, it could originate in Toledo, Ohio, travel through Buenos Aires, Argentina; Seoul, South Korea; Novosibirsk, Russia; Nairobi, Kenya; and Lisbon, Portugal, before hitting its target in Cleveland, Ohio. In order for the attack to be traced back to its source, each of these countries should be willing and able to cooperate. This requires they all have the technological infrastructure to monitor their own traffic and the expertise to analyze it. Were it possible to engineer such a high level of international cooperation, cyberspace would be significantly more transparent, and the problem of attribution would be less of a concern. Unfortunately, today only selected countries (more exactly 45 countries) are either willing or able to participate in what is referred to as the "G-8 24/7 network." This is an informal network that provides "high tech expert contact points which permits sharing of information on on-going investigations against cyber crimes."[2] Moreover, considering the technology required, it will take some time before all nations are able (even if they are willing) to participate in such a network.

Whatever its merit from a security perspective, the implementation of such a system would generate a level of transparency in cyberspace that would run into serious opposition from a variety of corners. It would not, for example, be welcome by those who favor secrecy or privacy, like the users of The Onion Router (TOR). TOR, which was originally a U.S. Navy program, is a system of communication featuring several layers of encryption and involving several routers, configured in such a way that the intermediate routers (except the last) do not know the ultimate destination of the packets. It is difficult to imagine a system that "solves" the problem of attribution while simultaneously allowing systems like TOR to operate. Yet, TOR is only one example. Part of the reason for this is that many regard the current level of transparency of the Internet as excessive. While some of the critics of transparency are legitimately concerned about privacy protection and civil liberties, the difficulty with TOR and other similar technologies is that they are open to exploitation by nefarious actors. The dark web, which is where most of the underground economy is located, is made possible by these technologies.

Nevertheless, it appears that the problem of attribution can be exaggerated. This is exemplified by the fact that a U.S.-based cybersecurity company was able to establish, beyond a reasonable doubt,[3] that many of the attacks reaching the United States originate from a specific building in Shanghai where a well-known unit of the Chinese government operates.[4] The Chinese government has chosen to deny having anything to do with what they claim Chinese law considers a crime. There is nothing compelling the Chinese government to analyze its internal traffic and trace those attacks to computers in China, even if the United

States presented its evidence. In the eyes of the rest of the world, the Chinese are probably lying, but what they are accused of, espionage, is a legitimate part of the relations between nations. In April 2013, during a visit to China paid by the Chairman of the U.S. Joint Chiefs of Staff General Martin Dempsey, his Chinese counterpart, General Fang Fenghui, stated that cyberattacks could be "as serious as nuclear bombs."[5] He went on to say that China and the United States should cooperate on these issues. However, having also made the disingenuous comment that "none of those activities is tolerated in China," he cautioned "progress will not be swift." Compounding the problem, "the Chinese apparently did not give any answers to General Dempsey on whether they intended to stop these activities, as specifically requested by the [Barack] Obama administration."[6]

This lack of reassurance was particularly problematic because several examples of spying have been traced back to China. One of these was originally discovered because the Dalai Lama suspected that his network was compromised. Eventually a group from the University of Toronto, Canada, established that a piece of malware had been introduced in the network to spy on emails and people and send its information to servers scattered throughout the world—a scheme the group dubbed Ghostnet.[7] By monitoring the servers, the researchers discovered that many other networks (in particular embassies and companies) were compromised. The information was clearly of interest to the Chinese government, but the origin of the attack was in Cheng Du, suggesting that the Chinese government had outsourced the operation. In a subsequent report, Shadows in the Cloud, the University of Toronto researchers reported the same servers were

used to spy on the Indian Government.[8] Another espionage initiative discovered by Kaspersky and named the "Red October Campaign,"[9] suggests that many of the worst cyberspying attacks are done outside governments. The information is likely sold to whoever is interested—presumably, but not necessarily, governments. In such scenarios, governments have more than "plausible" deniability, as it is possible to trace the attack back, and it in no way leads to them. As such, an international agreement attempting to codify spying via outlawing cyberspying does not appear to be a workable proposition.

Might bilateral agreements then accomplish what multilateral agreements could not? The Chinese appear to be trying shamelessly to get their hands on absolutely any kind of information: military, governmental, but also, and potentially more important, technological and commercial. Stealing technical or commercial information has different implications from pilfering military secrets. That crucial difference could pave the way for limited agreements. Protecting military secrets through international agreements is probably neither realistic nor even desirable. The fact that the U.S. Government does not do a good job at protecting its secrets is its own problem. But making the theft of technical or commercial information an international crime is a different matter. Agreements limited to the protection of the technological/commercial information may accomplish more and be easier to achieve, as they rest on a stronger legal basis. This is admittedly in a context where the Chinese have a documented record of violating every single bit of legislation on intellectual property against a background of the globalization of the economy and the internationalization of trade and regulation through

the World Trade Organization process. Given the additional consideration that China is now the second economy in the world and expected to become the largest in a few decades, it is not ridiculous to expect Beijing to accept some new norms of commercial behavior. Not only would the United States enjoy the support of its European and other allies, but it also has some, but not unlimited, leverage with China when it comes to trade.

There is also the case of attacks (like the Aurora[10] attacks, among others, which targeted the Gmail accounts of Chinese dissidents), which are considered criminal in the United States. China can take the position that the Chinese government could not be a party to cyberactivities that are also criminal under Chinese laws. There is, however, no evidence of any prosecution in China over this incident, which can definitely be traced back to that country.[11] Who other than the Chinese government could be interested in the content of those Gmail accounts? Furthermore, Google was only one among many targets. The others were the email accounts of Chinese dissidents at Yahoo, secrets in chemical companies and companies that belong to the military industrial complex, and more. China would have been the party most interested in the information targeted. The U.S. Government could, in principle, consider as unacceptable that the Chinese conduct criminal activities in the United States to fight political dissidence in their own country. But, unfortunately, nothing is simple, as we do not know the full extent of what the United States does in foreign countries in the name of security. In short, there are all sorts of obstacles to meaningful agreements.

Another complication standing in the way of making any agreement, whether bilateral or multilateral, verifiable, is that many cyberattacks are never detected. Yet others, such as the "Red October campaign" which lasted several years, are detected very late.[12] By the time they are detected, a lot of damage has already been done. The fact that so much undetected malicious activity is happening is unsettling. The answer is not to ask the perpetrators to refrain from doing it, however. It is to either reduce the probability that an attack is successful, or that it stays undetected. This is partially what legislation about sharing information between the public and private sector tries to accomplish.

For numerous reasons, the sharing of information between the public and private sectors is often regarded as a potentially efficient way to improve resilience against attack. The idea is inspired by the observation that most of the critical infrastructure is owned by the private sector. In practice, what people expect is that the information shared will be about the latest malware and/or could contribute significantly to improving "situational awareness." That reasoning does not stand up to scrutiny. Attacks on the government are, in fact, significantly different from attacks on banks. The attacks differ in their goals and, as a result, in the ways they are performed. Banks are targets because, in the famous words of Willie Sutton, they "are where the money is."[13] In contrast, as then-President of Israel Shimon Peres said when interviewed at the World Economic Forum in Davos, "governments do not have money, they have budgets."[14] When it comes to governments, what interests attackers are the secrets they hold. This necessitates a very different kind of attack. Attacks aiming at crippling critical infrastruc-

tures are very different again. Moreover, there is little that these three communities have to tell to each other about cyberattacks. The cyber vulnerabilities of critical infrastructures are in the computers controlling them and in the supervisory control and data acquisition systems. Only private companies responsible for critical infrastructures have such systems. The rest of the private sector, i.e., most of the private sector, has completely different vulnerabilities, and therefore, has to worry about completely different attacks, most of which are irrelevant for the government.

In other words, presenting the sharing of information between the public and private sectors as a kind of panacea is inspired by the misconceptions that they face the same kind of attacks, which is at best very rare. The fact that the private sector is reluctant to engage in that kind of sharing of information does not mean that it is unconcerned about cybersecurity. The private sector knows that this is a sub-optimal approach in the first place and will not be particularly useful to either companies or the government. Considering the natural reluctance of the private sector to share confidential information with the public sector, this approach is, in fact, counterproductive, as it antagonizes the private sector. In other words, a necessary feature for legislation to be either useful or successful is that it is endorsed enthusiastically by the private sector.

THE CHALLENGE OF ADJUSTING TO THE "CULTURE OF CYBERSECURITY"

In an interview in Davos during the 2013 World Economic Forum,[15] Shimon Peres mulled over the impact of cybersecurity on national security. More precisely, he mused about the role of the military and

government in the protection of citizens against cyberattacks. One primary mission of the military is the protection of the borders and of the citizens against foreign attacks. However, cybersecurity has created a new situation. Borders are an artificial concept for the Internet, and the role that the military could play to protect them in cyberspace is unclear. There is no country today where the military officially has the mission to protect the citizenry against cyberattacks. Even if military forces had this mission, they would not be able to carry it out effectively

In cybersecurity, the U.S. Government does not have a very well-defined role and its leadership lacks credibility. When U.S. netizens have their computers infected or compromised, they turn to security professionals for help, not to the government. When in March 2008 Dan Kaminsky[16] established the exploitability of a critical vulnerability (in the Domain Name System) in a critical infrastructure (the Internet), a summit was urgently organized to find a fix. This eventually led to the deployment of Domain Name System Security Extension (DNSSEC).[17] Microsoft hosted the "summit" in Redmond, Washington. The Department of Homeland Security (DHS), whose official mission is the protection of critical infrastructures, was not a part of that summit when it should have been its role to lead the response. It did not occur to the "experts" to alert DHS. The Kaminsky attack, with its far-reaching consequences, was a bombshell in the life of the Internet. Curiously, the fact that the U.S. Government was absent during the whole drama was hardly noticed, as if it had no natural role to play. The government does not have much credibility because it does not seem to have the needed expertise.

The fact that the government and military lack the expertise they need in cybersecurity is not a secret. The Defense Advanced Research Projects Agency's (DARPA) tentative solution was to hire as program manager a well-known hacker who goes by the alias "Mudge."[18] The goal was to facilitate the penetration of cybersecurity culture throughout DARPA and by extension the Department of Defense (DoD). This was unsuccessful, and the automatic budget cuts, known as sequestration, became an excuse to end the experiment. That, in a sense, predictable failure proceeds from a misunderstanding due to a difference of cultures, between hackers and members of the DoD community, and ignorance about cybersecurity on the part of DARPA, which seems to have thought that the expertise of hackers could be translated smoothly into policy or technological initiatives. The initiative underestimated the importance of the difference of culture.

Hackers are an important component of the world of cybersecurity. However different they are from each other, hackers have in common the desire to make complicated hi-tech systems do something for which they were not designed. Hackers have demonstrated so much ingenuity that it is safe to say that each time a new technology appears, some hacker will find ways to abuse it. Even so, most hackers do not spend too much time mulling over the security implications of their exploits. Nevertheless, many cyberweapons result from their exploits. The cyberattackers are the people who are interested in using those exploits, in effect, "weaponizing" them. Because the technical dimension is where the military personnel are the weakest in cybersecurity, DARPA made the common mistake of thinking that cybersecurity could be reduced to

a mere technical problem . . . the very kind of technical problems hackers know best how to solve. Naturally what Mudge[19] tried to bring to DARPA is the technical expertise of the hackers. This is what DARPA thought it wanted. It actually needed technical experts with the mindset of the cyberattackers. There is more than a subtle difference between the two.

Hackers often speak at conferences (DefCon,[20] SchmooCon,[21] Chaos Computer Club,[22] or Black Hat[23] meetings, although some of these are intended primarily for corporate people who can afford high registration fees). At such conferences, hackers proudly present their new exploits to their peers. The exploits, then, become public domain. When exploits are used in cyberattacks, most of the time it is by cybercriminals who are not necessarily as good at hacking as those who develop the exploits. In fact, those hackers who want to use exploits they develop themselves, do not present them in public conferences. As for the conferences themselves, one cannot confuse them with those held by academics: there exists far more banter and beer than attempts at any form of sophistication. On the other hand, from a cybersecurity perspective, those meetings are far more informative than academic conferences. The hackers' community is the repository for far more knowledge about cybersecurity than academia. From the perspective of security, however, neither academia nor most hackers see the security implications of the exploits—which is the basis of the culture of cybersecurity.

The cybersecurity equivalent of the strategic thinking that the military has developed over the ages does not exist. Even more damaging is the doomed attempt to apply to cybersecurity strategic concepts, such as "deterrence" or cyberspace "dominance," inherited

from a completely different security domain. Attempting to organize the debate around inappropriate concepts hinders progress, as it leads to a distorted view of what cybersecurity entails and does not translate into operational solutions.

We are still (and probably will be for quite some time) in an unsettling phase of realizing that, although cyberattacks can potentially be sophisticated, even without sophistication, they can be simultaneously difficult to stop and devastating. We do not yet adequately understand how to bound the problem, and things seem to be getting worse. It is common knowledge that the modernization of infrastructures, such as the power grid, water distribution, telecommunication, air traffic, and transport, in general, are implemented in such a way that U.S. exposure to potentially devastating cyberattacks keeps increasing.[24] Everybody realizes this, and yet it still takes place. It seems that the technological push for more use of Information Communication Technology is irresistible, like a fatal attraction.

From a strategic standpoint, what cybersecurity requires is a fundamental rethink of the basis of security. New concepts should either be developed or incorporated into our intellectual arsenal. If we let our most critical infrastructures rely on technologies vulnerable to attacks that we do not know how to prevent or stop, we had better prepare strategically for the consequences of this situation. We should likewise be prepared for the possibility that, when we need them most, those infrastructures will not be fully operational. "Resilience" has become a popular buzzword in the debate on the security of critical infrastructure. How to ensure such resilience is not yet clear, as is whether resilience represents a long-term solution. There is the possibility that the innovation behind the resilience

could become a target itself. A potential improvement to resilience is a new concept, introduced by Nassim Taleb[25] in 2013—"antifragile."[26] An antifragile system gets stronger when it is attacked. The immune system is an example, as are human beings in the aggregate. The question, then, becomes, can we design critical infrastructures or other critical systems in such a way that they are antifragile? To make a system antifragile requires relying, more than is the case now, on artificial intelligence, as that implies some learning capability. One way or the other, artificial intelligence clearly has a large role to play in the future of cybersecurity, as cybersecurity would benefit from the introduction of intelligent tools.[27] This logic relies more on computers and processing capabilities.

The most important part of the culture of cybersecurity is the one that is the least well understood: figuring out what opportunities the hacking exploits confer to cyberattackers. The sophistication of the exploit is not correlated with the damage it can do. For example, attacks, where the penetration of a network is due to spear phishing, do not qualify for the moniker "sophisticated." However, governments, financial institutions, and the like have not yet found an efficient way to avoid having their network penetrated in that way. But penetration can be accomplished in many different ways, such as the exploitation of software vulnerabilities. In a typical cyberattack, the penetration is only the first phase. After that, in general, malware is introduced in a variety of ways (often downloaded). The malware can be very sophisticated and have devastating functionalities. The people who make (and sell) malware are not very well known. They do not demonstrate their malware in hackers' meetings, although they often are also hackers. When they advertise their malware, it is to make money.

HOW IS THE U.S. CONGRESS RESPONDING?

Most attempts at producing cybersecurity legislation become controversial and end up in failure. The need for more sharing of information between the private and public sectors is one of the most common themes heard in Congress and other corners of the U.S. Government. For reasons stated above, this concern should not be allowed to play such a prominent role. It antagonizes the private sector and would not accomplish nearly as much as its proponents seem to think. Too often, proposed legislation becomes controversial over concerns about privacy. One disruptive effect of the proliferation of the Internet is a redefinition of the concept of privacy. That Congress participates in that debate is desirable. This is a very important component of the kind of democracy the United States wants to be. But privacy and cybersecurity are by and large different subjects with a very small overlap. Not only does Congress seem not to make that distinction, but it also does not seem to grasp the importance of increasing the protection of privacy. Instead, as in the example of the "Cyber Intelligence Sharing and Protection Act" (CISPA), Congress is proposing legislation giving less protection to the privacy of U.S. citizens. The case for that kind of legislation (which is supposed to help situational awareness and law enforcement) is, in fact, weak.

Congressional debates on cybersecurity tend to treat the whole subject as an entangled mess of issues. Cybersecurity is not well-served by debates mixing up privacy, cybersabotage, cyberespionage and cybercrime. These are very different subjects calling for very different answers. Privacy should enter into that kind

of debate as a binding constraint. The combined facts that the personal information of individuals happens to have commercial value, and the propensity of law enforcement agencies to use any excuse to increase their reach, are creating a situation where privacy is becoming completely compromised. Congress should be more receptive to these growing concerns about privacy and refrain from proposing legislation like CISPA, which suggests exactly the opposite. The burden of proof that civil liberties are expendable when it comes to cybersecurity is not met. Good legislation is protecting a modern and open society from cyberattacks, and as far as possible, should not infringe on individual liberties and privacy.

What new legislation should accomplish is to strengthen the cybersecurity posture in this country. Take the example of banks. They are part of the private sector. They are not interested in sharing more information with the government than they already do. Still, they are privately concerned by the severity of some cyberattacks (like massive Distributed Denial of Service [DDOS] attacks in the fall of 2012) and would like to know what the government could or would do for them in case things became even worse. What could the government have done about the DDOS attacks in the fall of 2012? If, as alleged, the attacks came from Iran in retaliation for the sanctions, should those cyberattacks have been treated as part of the conflict with Iran? Or would it have been better for the government to help the banks have access to additional webspace? At high expense, Akamai offers unlimited webspace.[28] This would defeat the DDOS attacks, as to saturate Akamai, one has to clog the Internet. Whether this approach makes political sense or not, it shows that the government can be involved and helpful in

ways significantly less contentious than through a form of information sharing, which the private sector rejects. This problem falls also in the purview of Congress.

Congress should also concern itself with the fact that despite the Federal Information Security Management Act (FISMA), the cybersecurity protection of the government has ample room for improvement. Apart from the text of the act, which was produced in 2005, FISMA was basically a fiasco. There are important lessons for the present to be drawn from the experience with FISMA. Cybersecurity is a real challenge for governments. It requires an unprecedented cultural and technological adjustment. Unfortunately, FISMA degenerated into a paperwork exercise, hardly a good way to face the challenges of cybersecurity. The origin of the problem can be traced to the clash between the rigid bureaucratic culture of the government and the demands of the new disruptive culture of cybersecurity.

The National Institute for Standards and Technology (NIST) was in charge of implementing FISMA. Based on the obvious fact that some agencies or departments carry more sensitive information than others, NIST tried to produce "metrics" to measure both the level of cybersecurity and the needs of different agencies. Yearly grades were given to the agencies or departments to measure their relative performance and monitor their progress. To the delight of the media, DHS and DoD consistently navigated between D and F.[29] But those grades were at the same time uninformative, unfair, and useless. Uninformative, because the way information was extracted was through a questionnaire filled out by representatives of the agency. In other words, FISMA audits were basically

paperwork exercises, and the questions by nature could not properly probe important issues such as the technical expertise and competence of the people involved. This was unfair, because being in charge of the cybersecurity of DoD, for example, is tantamount to mission impossible. In the words of General Keith Alexander, "The DoD network is not defensible, per se."[30] The exercise was useless because it did not provide information about what the most critical problems were and what should be done. Not only is a replay of FISMA something to avoid, but it should be recognized for what it was—a failure in need of corrective actions. A necessary start is to acknowledge the origin of the problem, which is that crossing two cultures as different as cybersecurity and government bureaucracy does not work. The government has only one option: adjusting to the culture of cybersecurity, however disruptive that may be.

There are reasons to believe that Congress and the government have not yet reached the level of situational awareness that would make them realize that cybersecurity has a different culture from that to which they are accustomed. Evidence of this problem abounds. For example, a good exercise would be to figure out what difficulties are being encountered by the head of the NSA, General Alexander, one of a few members of the U.S. Government whose competence in cybersecurity is not in doubt. As he noted, in his mission to build cyber command, we are "stuck at the starting line."[31]

What Congress can certainly do is ask the military to do a better job. Considering the importance of cybersecurity in all aspects of the security of the United States, and considering the size of the U.S. military as an organization with a tradition of being a leader in

the technologies that matter for security, it is unfathomable that the U.S. military still uses the service of private consultants for some of its cybersecurity problems. The services should long ago have developed their own intrusion detection capability and should be by now super-leaders in cybersecurity. If one excepts NSA, the U.S. military is seriously behind, compared to where it should be in cybersecurity.

Having as a unique point of excellence in cybersecurity, an agency like NSA, however, also has downsides. It leads to a situation where the NSA plays a leading role in that field not only in DoD, but also elsewhere in the government.[32] That was the official reason for the resignation of Rod Beckstrom from his position as head of cybersecurity in DHS. Given its mission (intelligence and espionage), NSA is not the most obvious choice to be the coordinator of the cyberdefense of the country.

Cybersecurity is also a threat to U.S. citizens. If it were not for the existence of the security industry, they would be helplessly exposed. But the security industry is also a for-profit activity. Considering that the most precious assets of American people are potential targets, if Congress does not find a workable solution, it would be fair to say that, despite the official rhetoric, the government is letting down its citizens. There is a perceptible worsening of the situation, which has the potential to degenerate badly. That could be potentially avoided with some shrewd legislation. It is in principle the job of Congress to produce such legislation. In cybersecurity, its record may not be stellar, but this is the only legislative power the United States has.

THE U.S. MILITARY AND CYBERSECURITY

The record of the U.S. military in cybersecurity is far from satisfactory. Considering that, in all the other areas of high technology, the U.S. military has managed to become a leader, and considering the importance of cyber for the life of the U.S. military, the future needs to be better.

The Past.

In 1998, the U.S. military was kept on high alert for 3 weeks by what was perceived as a coordinated stream of cyberattacks, in an episode called Solar Sunrise. The question was whether the perpetrators of those attacks were terrorists, the Iraqi government, or some other sinister organization.[33] The answer was three teenagers, two living in California, and one in Israel. Postmortem critics of this humbling experience noticed that key lessons from "Eligible Receiver" (a cybersecurity exercise where NSA was playing the red team) had not been implemented.[34] For example, there had not been progress in intrusion detection capability.[35] This is far from the only lesson that should have been learned. That an organization of the size and stature of the U.S. military could be so vulnerable to attacks that amounted to pranks by teenagers was not only sobering, but should have triggered a serious rethink of U.S. strategic posture in cyberspace. It did not, at least not in ways which strengthened significantly the U.S. ability to withstand cyberattacks, as was documented again by the more recent episode of "Agent.btz."[36]

Agent.btz was a piece of malware that had been detected in the wild in June 2008 (it was also called

Autorun). To propagate, the malware uses a very old and well-known technique: infecting removable devices like USB keys. To do that, Agent.btz exploited a weakness of the Windows operating system's autorun system. The classified military network is physically separated ("airgapped") from the unclassified one, which is connected to the Internet. USB keys were used to transfer files between the two networks. Agent.btz was piggybacking on those transfers to find its way onto the classified network. When in the classified network, it would scan the databases and copy files containing certain keywords. It would then take advantage of another transfer through a USB key to make its way back to a computer connected to the Internet. Finally, it would transmit what it had found to a proxy somewhere in the world. Apparently the U.S. military identified the breach only in November 2008, and it was deemed serious enough to brief the President.[37] The response was to disable all the USB ports, as well as other removable devices, on all the computers belonging to the military.[38] Considering the importance of the computers in the design and execution of military operations, this is, to say the least, a nuisance. In fact, there is evidence that, as a result, some Afghanistan theater operations that could have saved the lives of some U.S. military personnel could not take place. In a blog written in 2008, one could read:

> You may have read the news that an 'agent.btz' virus has *crippled the military*. This one is truly a horrifying terror attack against our men and women in uniform. It's far worse than the devastating *Solar Sunrise computer attacks* that crippled the U.S. Air Force in the 1990s. The Air Force is now failing to launch dozens of "ATO" [Afghanistan Theater of Operations] missions

> every day because of 'agent.btz', and we're actually losing soldiers' lives as a result. You heard what I said, folks. Two soldiers DIED in Afghanistan because the Air Force couldn't launch all of its aircraft due to the 'agent.btz' virus. Our death toll is going to mount until we get a handle on this terrorist cyber-weapon.[39]

The story of Agent.btz is disturbing for several reasons. First, in the design of the protection of classified material, the military had not fully realized that removable devices were known vectors for the propagation of malware. This is problematic. The alternative is that they also had not realized the full security implications, which would be, in a sense, worse. Second, the breach was discovered in November 2008 and was due to malware that had been detected in the wild in June 2008, 5 months earlier. A known malware with serious security implications may have roamed freely for quite a while in classified networks before it was detected, which does not say anything good about the progress in intrusion detection capability that had been recommended a decade before. Third, the solution found (disabling all USB ports and the use of removable devices, depriving computers used by the U.S. military of one of their most useful functionalities) cannot be considered sophisticated.

The decision to resort to such a drastic solution to an existing problem projects the impression that the people in authority are outsmarted by the complexity of cybersecurity. This suggests that military units have yet to familiarize themselves with the culture of cybersecurity. Among other things, that means that to take full advantage of what cyber has to offer, military personnel should be computer savvy. They should be able to make full use of computers in hostile environments (the natural environment for military person-

nel) and have the ability to handle nontrivial cybersecurity situations. Otherwise, the U.S. military will have a handicap against potential adversaries who can make full use of their computers.

In its official rhetoric to Congress, the military never misses an opportunity to voice concerns about cybersecurity. However, apart from Cyber Command, there are hardly any large-scale cybersecurity initiatives taking place. Instead, there are myriads of small initiatives. According to its head, Alexander, Cyber Command has had difficulty getting off the ground. Culture seems to be a problem there, too. The traditional ways of thinking in the military do not work well when applied to cybersecurity.[40] A whole new mindset is needed. It is probably unfair to go this far, but it is tempting to suggest that the answer to Agent. btz, of banning the use of removable devices proceeds from a military logic or culture that the only really safe response is a simple response. To paraphrase Albert Einstein, in cybersecurity things should be made as simple as possible, but not simpler. Banning the use of removable devices belongs squarely to the simpler or simplistic.

The Present.

One of the main priorities of the U.S. Government and military should be, and officially is, to improve the posture of U.S. cybersecurity. This has been the case for many years. When DHS Secretary Janet Napolitano realized the extent of the problem, she secured the resources to hire 1,000 security experts.[41] This was an inappropriate response to a real problem. There were not worldwide, let alone in the United States, 1,000 persons with the right kind of expertise. In

cybersecurity, expertise is a rare and precious commodity. It involves a mix of technical depth, policy savvy, and sense of strategic thinking which is, at best, very rare. The strategic thinking appropriate to the task may be the most important in the context of the military, but also the most problematic, partially because the traditional approach to strategic thinking is inappropriate. The relation between weapon systems and their military significance can be complex. But, by and large, military planners have a reasonably good grasp of it. As a result, the design of military operations is the result of some form of pragmatic optimization, which works reasonably well. But there is not yet a similar grasp of the cyber equivalent problem, i.e., appreciation of the tactical and strategic significance of "cyberweapons." This is particularly true with regard to the defensive dimension.

DARPA, which represents the cutting edge of the military's preoccupations, is pushing aggressively for research in the area of cyberwar. Unfortunately, the design of the Broad Agency Announcements on that subject betrays the difficulty of even that part of the government to adjust to this new culture. The concept of cyberdominance, whatever it means, is not a useful organizing principle to improve U.S. cybersecurity posture. Cyberspace is not seen best as a battlefield, but rather as a conduit of interactions between actors scattered across the world. The goal should not be "controlling" cyberspace, itself not a very realistic and, therefore, useful or even desirable goal, but to overwhelm those who use cyberspace to attack us. This does not imply that cyberwar is the cyberspace equivalent of the Strategic Defense Initiative popularly known as Star Wars. The notion that cyberbattles are intense engagements involving many actors and

computers interacting against each other in real time bears little resemblance with what a cyberwar actually would entail. There may be many things happening, such as logic bombs (malware inserted in software that will have malicious consequences when the software is used), infrastructure suddenly defaulting, and more. The first imperative would be situational awareness. This would require the ability to process a lot of information in a hostile environment. The whole logic of the engagement would be vastly different from a Star Wars battle, where the battlefield would be much more visible; the targets, and the way to destroy them, clearer.

The Report of the National Defense Science Board.

In January 2013, the National Defense Science Board produced a report entitled *The Resilient Military Systems and the Advanced Cyberthreat*.[42] Following what has become a tradition, the report began by stating that the cyberthreat was comparable in its severity to the nuclear threat of the Cold War. It proceeds by recommending that DoD take the lead in making the critical systems using information technology (i.e., most of the critical systems) resilient.

"Resilient" has become a popular buzzword. Wanting to have systems, critical infrastructures, or other assets, resilient to cyberattacks is, at least, an acknowledgment, or the realistic assessment, that it is impossible to protect them completely. One criticism of the report is what proceeds from that flawed strategy consists of reacting to a threat, rather than the more important task of planning for a different future. As long as the cybersecurity posture of the U.S. Government is purely reactive, progress will continue to be

slow. However, to be able to implement an alternative strategy to be proactive instead of reactive, one should possess some concept as to how to do that.

The report is critical of what is happening today. Its criticism goes well with the gist of the present paper: "Current DoD actions, though numerous, are fragmented. Thus, DoD is not prepared to defend against this threat."[43] One alternative to this fragmentation would be a large-scale, coordinated, and well-planned effort to make the U.S. military the super-leader in cybersecurity. That does not seem in the cards yet, as one can also read in the same report: "It will take years for the Department to build an effective response to the cyber threat to include elements of deterrence, mission assurance, and offensive cyber capabilities."[44] This is a very depressing statement. The question is whether what is more depressing is the reference to concepts like "deterrence" and "mission assurance" borrowed from the mainstream military thinking, which applies poorly to cybersecurity, or the expectation that "it will take years . . ." for something DoD already had quite a few years to work on. Cybersecurity did not hit the United States after the rest of the world. If anything, it started in the United States. Why has it taken so long? The answer is that learning a new culture is a complicated process of familiarization and education, which takes time.

The Future.

There is only one acceptable future: a world where the U.S. military succeeds in extending its technological superiority to cyberspace. So far, the U.S. military did not suffer much as a result of its relative backwardness in that area because it was engaged in conflicts

against nations (Iraq and Afghanistan) not particularly advanced in that field. We should admit honestly that we would be less concerned by the possibilities of confrontation with China if the United States were significantly less vulnerable to cyberattacks. It seems safe to assume that China knows its way in U.S. cyberspace, probably better than anybody else does, even those in the United States. Clearly, this is not a comfortable situation.

There is an imperative for the U.S. Government and military to endeavor to become the super-leaders in that most critical component of the conflict spectrum: cybersecurity. This means among other things that we should take the success of Cyber Command very seriously, and Congress should provide as much useful support as possible.

CONCLUSIONS

So far, cybersecurity is not a success story for the U.S. Government and military. It is unprecedented in the history of the United States to see the official rhetoric and official declarations emanating from the highest level of the government referring to potentially lethal threats to the country and simultaneously being able to accomplish so little against them. The dangers are easier to identify than are ways to prevent or mitigate them. Cybersecurity is a challenge for all governments. However, the challenge is worse for the U.S. Government.

The adjustment to a new culture tends to be a slow and protracted process. If one compares the situation to what it was a few years ago, there has been progress. By way of analogy, it is a bit like the grass growing. Progress is not immediately visible; it takes place

only very slowly. This reflects the slow penetration of the culture of cybersecurity in the U.S. Government and military.

To the two questions, could international agreements, whatever form they may take, benefit the United States or should the United States push for some form of multilateral treaty-based international cyberorder, the answer is the same—a qualified no. There is no good framework for a multilateral negotiation dealing with cybersecurity issues. Bilateral agreements with countries like China are not necessarily much more attractive, as the United States would have to negotiate from a position of weakness. But the protection of commercial secrets may offer an opening to negotiations and is probably the best chance for some form of international agreements, as that intersects with trade, an area of overlapping interest.

ENDNOTES - CHAPTER 15

1. "Internet remains unregulated after UN treaty Blocked," *The Guardian*, December 14, 2012, available from *theguardian.com/technology/2012/dec/14/telecoms-treaty-internet-unregulated*.

2. See G8 24/7 High Tech Crime Network Overview available from *itlaw.wikia.com/wiki/G8_24/7_High_Tech_Crime_Network*.

3. The methodology of the investigation by Mandiant inspired more controversy than its conclusions. See *intelreport.mandiant.com/Mandiant_APT1_Report.pdf*.

4. Lee Ferran, "Report Fingers Chinese Military Unit in US Hacker Attacks," ABC News, February 19, 2013, available from *abcnews.go.com/Blotter/mandiant-report-fingers-chinese-military-us-hack-attacks/story?id=18537307*.

5. Andrew Browne, "China: Cyberattacks Are Like Nuclear Bombs," *The Wall Street Journal*, April 22, 2013, available from *wsj.com/articles/SB10001424127887323551004578438842382520654*.

6. Jane Perlez, U.S. General Sees Hope for Chinese Help on Korea, *The New York Times*, April 24, 2013, available from *nytimes.com/2013/04/25/world/asia/us-hopeful-after-talks-with-china.html*.

7. "Tracking GhostNet: Investigating a Cyber Espionage Network," *Information Warfare Monitor*, March 29, 2009, available from *f-secure.com/weblog/archives/ghostnet.pdf*.

8. "Shadows in the Cloud: Investigating Cyber Espionage 2.0," Joint Report of the Information Warfare Monitor, Toronto, Canada, and Shadowserver Foundation, April 6, 2010, available from *nartv.org/mirror/shadows-in-the-cloud.pdf*.

9. GReAT, "'Red October' Diplomatic Cyber Attacks Investigation," SecureList.com, January 14, 2013, available from *securelist.com/en/analysis/204792262/Red_October_Diplomatic_Cyber_Attacks_Investigation*.

10. Kim Zetter, "Google Hack Was Ultra Sophisticated, New Details Show," Wired, January 14, 2010, available from *wired.com/threatlevel/2010/01/operation-aurora/*.

11. Matthew J. Schwarz, "Google Aurora Hack Was Chinese Counterespionage Operation," *InformationWeek*, May 21, 2013, available from *darkreading.com/attacks-and-breaches/google-aurora-hack-was-chinese-counterespionage-operation/d/d-id/1110060?*.

12. Kaspersky, January 14, 2013, available from *kaspersky.com/about/news/virus/2013/Kaspersky_Lab_Identifies_Operation_Red_October_an_Advanced_Cyber_Espionage_Campaign_Targeting_Diplomatic_and_Government_Institutions_Worldwide*.

13. See *quoteinvestigator.com/2013/02/10/where-money-is/*.

14. World Economic Forum, Interview with Shimon Peres, "Davos 2013—A Conversation with Shimon Peres, President of Israel, February 12, 2013," available from *youtube.com/watch?v=dvhfbj2uhYQ*.

15. World Economic Forum, "A Conversation with Shimon Peres," Davos, 2013, available from *https://www.youtube.com/watch?v=dvhfbj2uhYQ*.

16. See *defcon.org/html/links/dc-archives/dc-16-archive.html#Kamnsky*.

17. DNS is the Domain Name System, the directory of the Internet. This is a critical component of the Internet. If it does not function well, users cannot reliably get to the sites of their choice. DNSSEC is the DNS security extension. The idea was to avoid the possibility that the user would be directed to malicious sites by adding a layer of security. See *icann.org/en/about/learning/factsheets/dnssec-qaa-09oct08-en.htm*.

18. His real name is Peter Zaitko.

19. Arik Hesseldahl, "Computer Security Legend Mudge Leaves DARPA for Google Job," AllThings.com, April 13, 2013, available from *allthingsd.com/20130413/computer-security-legend-mudge-leaves-darpa-for-google-job/*.

20. See *defcon.org/*.

21. See *shmoocon.org/*.

22. See *ccc.de/en/*.

23. See *blackhat.com/*.

24. See, for example, the comments of Leon Panetta, Remarks by Secretary Panetta on Cybersecurity to the Business Executives for National Security, New York City, October 11, 2012, available from *archive.defense.gov/transcripts/transcript.aspx?transcriptid=5136*.

25. See *fooledbyrandomness.com/*.

26. Michiko Kakutani, "You Are All Soft! Embrace Chaos! 'Antifragile,' by Niassim Nicholas Taleb," *The New York Times*, December 16, 2012, available from *nytimes.com/2012/12/17/books/antifragile-by-nassim-nicholas-taleb.html?_r=0*.

27. Carl Landwehr, "Cyber security and artificial intelligence: from fixing the plumbing to smart water," published in the *Proceedings of the 1st ACM workshop on Workshop on AISec*, 2008, available from *landwehr.org/2008-09-sp-landwehr-ai-and.pdf*.

28. Brian Prince, "DDoS Attacks Spiked in Q1 2015: Akamai," *SecurityWeek*, May 19, 2015, available from *securityweek.com/ddos-attacks-spiked-q1-2015-akamai*.

29. See *fismacompliance101.com/fisma-report-card.htm*.

30. Henry Kenyon, "Cyber Chief Issues Call For Action—Not More Talk; Alexander Outlines Who Does What," *Breaking Defense*, November 8, 2012, available from *defense.aol.com/2012/11/08/cyber-chief-issues-call-for-action-not-more-talk-alexander-o/*.

31. See Jared Serbu, "On cyber defense, U.S. 'stuck at the starting line'," Federal Drive, November 8, 2012, available from *http://federalnewsradio.com/federal-drive/2012/11/on-cyber-defense-us-stuck-at-the-starting-line/*.

32. See *online.wsj.com/public/resources/documents/BeckstromResignation.pdf*.

33. See *globalsecurity.org/military/ops/solar-sunrise.htm.*

34. The exercise Eligible Receiver is discussed in *globalsecurity.org/military/ops/eligible-receiver.htm*.

35. The need to work on Intrusion Detection was already emphasized in a Comprehensive Error Rate Testing report from 2000, "State of the Practice of Intrusion Detection Systems," available from *sei.cmu.edu/reports/99tr028.pdf*.

36. Ellen Nakashima, "Cyber-intruder sparks response, debate," *The Washington Post*, December 8, 2011, available from *washingtonpost.com/national/national-security/cyber-intruder-sparks-response-debate/2011/12/06/gIQAxLuFgO_story.html.*

37. Noah Shatman, "Insiders doubt that 2008 Pentagon Hack was Foreign Spy Attack," Washington, DC: The Brookings Institution, 2010, available from *brookings.edu/research/opinions/2010/08/25-pentagon-worm-shachtman*.

38. Noah Shachtman, "Under Worm Assault Pentagon ban Disks and USB drives," Wired, November 19, 2008, available from *wired.com/2008/11/army-bans-usb-d/*.

39. See *blog.afcyber.us/2008/11/20/jointchiefs.aspx#Comment.*

40. Attempts to map military concepts to cyber security are common but often misleading. See "The Library of Sparta," Black Hat Meeting, available from *esecurityplanet.com/network-security /using-military-strategy-to-fight-cyber-battles.html.*

41. Michael Cooney, "Homeland Security to hire 1,000 cybersecurity experts," Computerworld, October 1, 2009, available from *computerworld.com/article/2528471/security0/homeland-security-to-hire-1-000-cybersecurity-experts.html.*

42. "Resilient Military Systems and the Advanced Cyber-Threat" Washington, DC: Defense Science Board, January 2013, available from *www.acq.osd.mil/dsb/reports/ResilientMilitarySystems.CyberThreat.pdf.*

43. *Ibid.*, Executive Summary.

44. *Ibid.*

CHAPTER 16

TRANSNATIONAL ORGANIZED CRIME AND DIGILANTES IN THE CYBERCOMMONS

Kelsey Ida

Although there still exists debate on the general motives and organization of transnational organized crime, there is nonetheless broad consensus that such crime operates in relation to some kind of market function.[1] In this manner, the "digital age" has **revolutionized** transnational organized crime. The Internet and cyberspace have given criminal organizations a means of conducting profit-generating activities with greater efficiency and an extra-territorial capacity. Moreover, within the continuous, evolving electronic space,[2] because no single actor—individual, group, state, or organization—has a legitimate monopoly on violence, it is reasonable to believe that criminal horizons will ever expand.

Just how far those horizons will reach, however, is debatable. During the past 2 decades, transnational organized crime indeed has risen to unprecedented levels and acquired tremendous profits, with traditional law enforcement largely unable to keep up.[3] But perhaps the more intriguing question is, can and will actors in the private sphere—specifically "digilantes"—organize (bottom-up) to take independent action against transnational crime? Historically, when citizens have determined their criminal justice system to be inadequate, they have taken regulatory matters into their own hands.[4] Though past **vigilantism** against organized crime has met with little success, given the unique operational features of the Internet,

will digilantes and digilante groups have a role to play as regulators of transnational criminal justice?[5] There is already evidence of digilantes rallying to take on isolated cybercriminals (e.g., cyberpredator stings; China's "Human Flesh Search Engine"), and digilante groups have even taken some notable action against transnational criminal organizations (i.e., Anonymous vs. Los Zetas). Especially when we consider how "smart power"[6] and "anonymity" characterize agencies in cyberspace, the question arises, what is the role of the transnational public in curbing transnational crime?

This chapter proceeds in three parts. The first section briefly summarizes the breadth and depth of transnational organized crime and reviews the explanatory models offered for its explosive growth. The second section highlights the unique operative features of cyberspace and argues that bottom-up regulation by digilantes may not be as far-fetched a phenomenon as initially thought. After all, in the absence of an actor with a legitimate monopoly on the use of force, digilantes have a major power share in cyberspace (i.e., "smart power"), as well as protective anonymity, which begets **agency**. They have the capacity to influence the international regulatory system in an unprecedented way. The final section addresses the relevant question in criminology that asks, "Do criminals organize around opportunities for crime, or do criminal opportunities create new offenders?"[7] Even if they have proven agency, will digilantes actually exist as a force of communal good, or will these unaffiliated agents, inevitably and deterministically, be driven to partake in criminal enterprises themselves?

It should be emphasized that it is **not** the aim of this analysis to offer a formal argument on bottom-up

private sector regulation in a digital, globalizing age. The observations here have not yet been subjected to a rigorous testing or field research, and prior to making declarative and confident statements, corroborating studies are necessary. In essence, this is a preliminary "plausibility probe" into digilante agency in electronic space.[8] Ultimately, this is an area ripe for future investigation.

ELECTRONIC FORUMS AND FRONTIERS: EXPEDITING CRIMINAL MARKET EFFICIENCY

Criminal Organizations as (Vehement) Rent-Seeking Firms.

Since the late-1980s, organized crime has grown at an unprecedented rate and, in the context of globalization, has taken on an undeniably **transnational** character.[9] Criminal activities have expanded across more and more state boundaries. Moreover, while criminal activities include the traditional income-generating enterprises such as drug trafficking, firearms trafficking, and money laundering, new illicit markets have also emerged (e.g., organ trafficking and cybercrime).[10] The annual turnover of all transnational organized criminal activities is approximately U.S. $870 billion. Consequently, it is likely that profits are also in the billions.[11]

A number of theoretical models and frameworks have been offered to explain the tremendous growth of transnational organized crime. Political models, for example, have highlighted the criminal opportunities bequeathed to organized groups in the context of global political instability (e.g., weak states or transitioning states). Phil Williams and Roy Godson recount that

the end of the Cold War found many post-communist countries extremely vulnerable to organized crime.[12] Where previously there had been a "controlled equilibrium" of state authority and organized crime, the depression of a strict authoritarian structure enabled organized crime groups "to expand the scope of [their] activities in ways that were unprecedented."[13]

Social models, meanwhile, have emphasized the diaspora distribution and adaptation of cultural/social systems beyond national borders as accounting for the dramatic rise in transnational crime. Edward Kleemans points out that social relationships are critical for criminal cooperation in that they discourage cheating.[14] Because criminal organizations must think in terms of both the "shadow of the past" and the "shadow of the future," there is a high importance placed on **trust** within organized crime.[15] Kleemans elaborates:

> There are no stock exchanges or yellow pages, there are only people you know or do not know, and whom you either trust or mistrust. A fundamental aspect of criminal co-operation consists of searching for suitable co-offenders.[16]

With cultural-trustworthy social networks communicating and moving across borders, so too are criminal networks on the move. Williams and Godson point out the significance of diaspora communities in outsourcing organized crime to "trusted" co-conspirators that may not reside in the central criminal node.[17] As exemplified with Nigerian organized crime and Chinese triads, if diaspora populations are widely scattered across the globe, this gives organized crime a transnational network distribution that is simply unparalleled.

Ultimately, however, economic models have perhaps the most consensus in studies of transnational organized crime.[18] Some scholars express (rightful) concern about adopting a purely rational-choice economic model of crime,[19] but agreement on a general profit dimension remains. Even the official definition of "organized criminal group" offered by the United Nations Office on Drugs and Crime (UNODC) clearly identifies this financial element (i.e., organized criminal groups as aiming "to obtain, directly or indirectly, a financial or other material benefit").[20]

Williams and Godson note that there are two main economic theories applied to transnational crime, though the two theories are not entirely symmetrical. For instance, the "market model" understands criminal members, but not organizations themselves, as operating according to supply-and-demand dynamics.[21] "Enterprise models" meanwhile, look at criminal organizations as **businesses** engaged in (vehement) rent seeking.[22] To maximize profits, these criminal organizations will diversify their markets and adjust their strategies accordingly (i.e., entering markets from drug trafficking to endangered animal smuggling). Williams and Godson clarify:

> Not all criminal organizations engage in a formal planning process; nevertheless their thinking, intuitively or deliberately, will reflect standard business needs and take into account such factors as new product opportunities, product dominance, profit margin, market needs and opportunities, degree of competition, risk management, retirement strategy, and the like.[23]

It should be noted that, amidst the growing trend of organized crime engaging in licit ventures as well as illicit ones, this latter model seems to be particu-

larly compelling.[24] In their daily rhetoric, academics, law enforcement officials, and policymakers all commonly replace "organized crime" with the term "illegal enterprise."[25]

All Systems Operational—Criminal Upgrade 2.0.

An economic modeling of transnational organized crime would suggest that organized crime would ever expand as more income-generating opportunities present themselves (and offer a comparative advantage). Looking at the effects of "globalization," Williams and Godson warn:

> There will be a growing tendency for organized crime to become transnational in scope. Although purely domestic criminal organizations can be both successful and wealthy, the power and success of criminal enterprises could depend increasingly on their capacity to act transnationally. . . . The corollary is that existing criminal organizations that are already transnational in scope will expand their operations in the search for new markets.[26]

For some, this is not a cause for immediate alarm. Peter Andreas, for instance, acknowledges that globalization has created new market frontiers for transnational crime.[27] However, he considers this evolution of transnational crime as only the "latest chapter in an old story" of illicit activities.[28] Transnational crime is not a new phenomenon, and history supports the premise that where there is "globalization of crime," there is also a "globalization of crime control."[29]

What is troubling about Andreas' conclusion is that it does not appreciate fully one important element that has characterized 21st-century globaliza-

tion—technology, specifically digital technology.[30] Indeed, globalization—like organized crime—is an exceptionally complex and broad phenomenon, and perhaps should not be defined purely in terms of technological growth. However, one cannot speak of the phenomenon of increased interconnectedness without also speaking **to that technological context which has enabled it** (if not directly embodied it).[31] The development and maturity of information and communication technologies (ICTs) has been at the crux of an increasingly interconnected world. ICTs have transformed profit margins. In commercial terms, it may be said that ICTs, while enabling and expediting corporate decision-making across difficult geographic frontiers, have given producers the ability to do more.[32] The new technologies of the past 3 decades have allowed us to tap into previously inaccessible markets, and even venture into entirely new ones.

As naturally as commercial horizons have broadened through ICTs, so too have criminal horizons. Michael Levi describes how the digitalization of international business has also allowed criminals to communicate more efficiently and with less personal risk in their enterprise. The Internet, for instance, allows organized crime groups to distance themselves from their illegal goods and services and iterate crime in a way that they previously could not—especially in carrying out financial activities and fraud.[33] Burner phones and encrypted communication make it very difficult to trace organized crime, with significant consequences in smuggling operations (i.e., goods and people).[34] ICTs have even revolutionized the activity of counterfeiting by enabling:

> the skimming of magnetic-stripe credit card details by retailers and their staff, which can be sent by e-mail

> to colleagues in China, Italy, and Russia (theoretically, to any moderately skilled people anywhere in the world).[35]

While it is possible that the digitalization of international business has had organizational consequences for organized crime, such consequences have not necessarily been detrimental. For example, Brenner writes that amidst increasing usage of cyberspace, the traditional Mafia-style hierarchical organization of organized crime has declined.[36] This may be because, while the physical world has a fixed, empirical structure requiring a socially-organized hierarchical structure, cyberspace is "inconsistent with hierarchy."[37] However, even in the face of this potential command-structure change, organized crime has shown remarkable resourcefulness and adaptability to a network-level organization. For instance, in Colombia, as criminal bands (BACRIM) of younger crime lords have been forced to step into prime leadership roles, rather than immediately conforming to the hierarchical structure of their predecessors, they have taken measure of their criminal resources—contacts, reputation, capacity to negotiate, networks of corruption, firepower—and adapted.[38] Across Latin America, these groups are organizing at a more communicative and network level, increasing their profits, and perpetuating their longevity.[39]

Even more unsettling is that, despite Andreas's optimism, our regulative framework for transnational crime has not adapted to the digital environment. Daniel Alexander writes, "Law enforcement is presently 5 to 10 years behind the global crime curve in relation to technological capabilities."[40] In addition to the problems of actually tracking the digital footprint

of organized crime (especially with anonymity software such as the Onion Router), one major problem law enforcement does face is navigating through multiple jurisdictions. For instance, even though the United States may have expansive and rigorous laws that address cybercrime, if and when the criminal activity in question proceeds outside the national jurisdiction, it becomes very difficult to coordinate inter-jurisdictional enforcement.[41] States often have very different understandings of what organized crime actually is, and in many states, domestic police corruption hampers any attempts at criminal apprehension.[42] Recent decades have seen renewed efforts at communication and data exchange though the International Criminal Police Organization, but there is still continued reluctance by many law-enforcement agencies to share information and command joint taskforces across borders.[43] The UNODC summarizes:

> The process of globalization has far outpaced the growth of mechanisms for global governance and this deficiency has produced just the sort of regulation vacuum in which transnational organized crime can thrive. People and goods can move more cheaply than ever before, and criminals and contraband can only be interdicted by national governments. Human and commercial flows are too intense to easily distinguish the licit from the illicit. Silos of sovereignty provide sanctuary to those who, however harmful their activities, are of use to the authorities in one country or another. The open seas, which constitute three quarters of the earth's surface, remain essentially ungoverned.[44]

Amidst this reality—wherein organized crime is global, profit-based, and with few policing agents capable of standing up to its might—there is a valid reason for concern. The threat of harm to the trans-

national public certainly stands to intensify.[45] Moreover, organized crime is also likely to enter and professionalize further markets of **substantial** harm and victimization. For instance, organized crime has thus far had limited engagement with child pornography outside human trafficking. Instead, trafficking in child pornography has occurred more on a voluntary basis between amateur collectors through peer-to-peer networks.[46] Recent estimates, however, put the revenues of this market to be now $250 million annually.[47] What are the ramifications of this? The UNODC warns:

> If child pornography were to approach the profitability of adult pornography, this could attract the attention of organized crime groups, transforming what had been a furtive paper exchange into a professional operation and leading to greater levels of victimization.[48]

DIGILANTES FOR A DIGITAL AGE?

Smart Power and Anonymity as Empowering Functions in Cyberspace.

This example of trafficking in child pornography, however, also brings to the discourse a unique (and largely unexplored) analytical dimension—namely, that of online vigilantism, or digilantism.[49] In the past decade, there have been numerous examples of cybergroups mobilizing specifically to apprehend child molesters. In both the United Kingdom (UK) and the United States, for instance, private groups have utilized cyberspace to contact pedophiles and sexual predators before allocating some form of justice upon them, usually identity-naming and public shaming.[50] Some of these private groups have even been recog-

nized and "deputized" by local authorities for their auxiliary efforts. The chatlog evidence gathered by U.S.-based nongovernmental organization Perverted Justice has been admitted to court and led to 588 convictions against child predators.[51] The "confrontation videos" of the informal group, Letzgo Hunting, have also led to criminal arrests in the UK.[52]

Such instances of digilantism should certainly not be taken as **absolute** digilante success against criminal predators. There is no hard evidence that digilantism has deterred market demand for child pornography, or that it has curbed the overall trend of sexual predation. What is significant here, however, is that these instances indicate **the presence of a unique frontier for justice online**. If, and when, a crime has threatened the public enough, especially given their own proximity to the nonmediated space, nonstate actors—with or without the blessing of the state—**have taken it upon themselves to respond**.

The question then emerges: what are the prospects for digilantes in cyberspace to act as real (if subtle) policing agents against transnational organized crime? Note that this is a slightly different question than that which asks if there is a role for the private sector as a partner in the global fight against organized crime. Where individual companies provide the goods, software, and licit association that facilitate organized crime, there **is** likely a role for private-sector involvement in organized crime prevention.[53] The question at hand, however, begs attention to a more bottom-up civil society approach, rather than a top-down initiative. At the base level, there may be identified two unique conditions—smart power and anonymity—which empower select members of the transnational public to act with much greater agency in cyberspace than in traditional geopolitical settings.

Smart Power.

The first of these conditions is "smart power." In cyberspace, there is no single coercive actor with a Weberian "legitimate monopoly on the use of force." Susan Brenner remarks that cyberspace distinctively: (1) eliminates the constraints of the physical world, (2) vitiates identity, and (3) is situated in such a manner that perpetrators can cause harm on a scale that even surpasses what is possible in the real-world.[54] Virtual actors can flit across vast distances within mere seconds, and they can fluidly change identity—while also having a capacity for high violence. A state, even if it is well-equipped with traditional force mechanisms of the physical world, cannot so easily secure a monopoly on violence in cyberspace. It is perhaps equivalent to trying to capture a bacterial specimen with a butterfly net.

In the absence of a legitimate state to govern the virtual world, agency arguably flows to those individuals who can best manipulate the virtual environment. This amounts to those individuals with high cyberknowledge (i.e., encryptions skills, coding skills, hacking skills, programming skills, etc.), or what I call "smart power." In perhaps implicit recognition of the internal and external threats posed by this absent monopoly of violence, governments do recruit and co-opt those individuals with smart power.[55] Through this, they are able to reintroduce some semblance of hierarchy on the virtual world—e.g., illegalization and eventual shut down of the online contraband market Silk Road by the Federal Bureau of Investigation (FBI) in 2013.[56] However, it is notable that organized crime also recruits talented hackers and those individuals with smart power.[57] Armed with such human

resources, organized crime often stays two steps ahead of law enforcement. For instance, even when their activities are apprehended in cyberspace, criminal smart power empowers groups with the ability to shift quickly themselves—and their activities—into new, undetectable forms. Indeed, only a month following the government seizure of the Silk Road and the arrest of administrator Ross Ulbricht, the Silk Road 2.0 was launched, administered by a new "Dread Pirate Roberts" (Ulbricht's pseudonym on the Silk Road).[58]

With the government unable to retain a constant monopoly of smart power, law-abiding behavior cannot be fully enforced or coerced (at least by traditional means). What is key here, however, is that not all smart power actors are spoken for. Many are yet unaffiliated, and it is with them that regulatory power may lie.

Anonymity.

Before speaking more to this, however, it should be noted that, though smart power may be a necessary condition to a digilante agency, anonymity might be a necessary condition for smart power. Hinted at in her second distinction of "vitiated identity," Brenner has observed, "Cybercriminal and cyberterrorists can be anonymous or assume false identities with an efficacy that is impossible in the physical world."[59] When individuals/groups occupy fixed and empirical space, there are only so many identities they can assume before those with greater coercive power track them down for reprisals. It should be noted that public vigilantism against organized crime is relatively uncommon for this reason.[60] In strong states, vigilantism is likely to be subdued and deterred by the government,

while in weak states, vigilantes face retaliation by organized crime groups that have the monopoly on violence (e.g., the "political hijacking" of the Bakassi Boys).[61] Anonymity, however, allows continuous, fluid movement for digilantes to act outside the threat of coercion. With respect to cyberspace, anonymity begets smart power, and smart power begets agency for change.

Digilantes Rising?

One question that immediately arises is whether any transnational public group with adequate computer skills can have "digilante agency" and the potential to make a change. It would seem that an individual does not have to have extensive programming skills in order to have a power share (and anonymity) in the anarchical virtual world. Consider, for instance, the ease with which computer-literate individuals can access unauthorized video content, such as unlicensed versions of HBO© shows like *True Detective* or *Game of Thrones*. Can moderate cyberknowledge sufficiently empower anyone as an effective digilante against organized crime?

The "419 digilantes" and Nigerian organized crime may serve as a prospective case for this. Citing crime data, the lack of swift legal action, corruption in Nigeria, and select victim narratives, the 419 digilantes (stationed at 419eater.com) in the past decade have engaged in a vicious scambaiting campaign against Nigerian criminal organizations.[62] Broadly posing as potential targets to lure cybercriminals into revealing valuable information, the 419 digilantes then publically repost the scam—and all "trophies"[63] taken in the course of the scambaiting—both as retributive justice

and as a public service with the hopes that it impacts real crime.[64]

Unfortunately, there is not here enough evidence to determine what effect, if any, such digilante action actually has on Nigerian organized crime. Beyond the self-claims of the 419 digilantes, there is no way of measuring how many criminal activities are curtailed or how many criminal profits are lost due to these "public shaming" posts. Nigerian organized crime still generates large profits from advance-fee schemes.[65] Byrne also points out that many of the 419 digilantes' reposts and trophies are colored by strongly racist overtones, making the collective act more politically partisan, and less digilante, in character.[66]

This is not to deny that the 419 digilantes might have an impact on organized crime, but digilantism arguably requires a distinct caliber of smart power and a particular end-goal of criminal redress for regulatory success. A stronger example of digilante agency may be seen in the hacker-to-hacktivist group, Anonymous, and their fight against Los Zetas.

In the early-2000s, Anonymous existed as a loosely organized cybergroup, largely synonymous with trolling and sophisticated hacking pranks. Since 2008, however, it has shifted from being a curious hacker group to a politically active hacktivist group. Gabriella Coleman, one of the leading scholars on hacker culture and Anonymous, recently wrote:

> Anonymous signals the growing importance of what I call 'weapons of the geek,' a modality of politics exercised by a class of privileged and visible actors who are often at the center of economic life. Among geeks and hackers, political activities are rooted in concrete experiences of their craft.[67]

As with the case of the 419 digilantes, there is still an argument that Anonymous is not a socially concerned and frustrated digilante group, but a disorganized nuisance.[68] As Coleman points out, however, the group has maintained very stable activist nodes in the past 4 years.[69] During this time, Anonymous has demonstrated an increasing willingness to use its smart power to redress directly social injustices and even organized crime. For instance, in early-2011, Anonymous played a substantial role in the Arab Spring. The hacktivist group made sure communication forums were kept open for protesters in Egypt, Libya, Algeria, and Syria, and even went so far as to attack the Tunisian government website and disable the software the ruling regime was using to track the movements of its citizens.[70]

The most significant case for this chapter, however, lies in Mexico. Following its activist engagement in the Middle East, Anonymous singularly turned its "weapons of the geek" against organized crime itself, engaging the Mexican drug trafficking organization, Los Zetas, in a novel example of bottom-up digilantism. In October 2011, following the kidnapping of an Anonymous member residing in the state of Veracruz, Anonymous threatened to publicize online the personal information of Los Zetas and their associates unless Los Zetas freed the hostage by November 5.[71] Despite Los Zetas' attempts at "reverse hacking" and death threats sent to Anonymous members, the criminal organization did release the kidnapped member on November 4.[72] Admittedly, Los Zetas gave a warning to Anonymous that they would execute 10 people for every name that the digilantes might subsequently publicize.[73] What remains significant here, however, is that Los Zetas was the first party to "blink." It was not

a clear victory for the digilantes, **but it certainly was not a loss**.

Notable here too is that Anonymous (through a local branch in Acuña) has since re-engaged Los Zetas, publishing photos of known Zetas properties online, thus far with little retribution.[74] Scholars in the academic community, such as Paul Kan, have warned the group to take care with its activities. By choosing to "out" the various parts of the organizational infrastructure, Anonymous has once more struck at Los Zetas' criminal brand, and Los Zetas is likely to respond in kind.[75] However, here again, the digilantes—with notable public support—have engaged organized crime beyond state enforcement.[76] It is uncertain as to where this action stands in the grand scheme of things, but this evidence does leave us in a position to wonder if indeed digilantes—with their anonymity and smart power—may be a significant force for regulating organized crime in the future?

CRIMINAL VENTURE AS THE DETERMINISTIC "ENDGAME"?

This chapter, so far, has been relatively optimistic that unaffiliated members of the public (and unaffiliated groups such as Anonymous) can—and would—make decisions according to a more societal-based moral authority, rather than on individualistic and self-seeking motives. However, there is evidence to suggest that this may not be the case. Rational-choice theory broadly dictates that an agent, when faced with alternative choices, will act self-interestedly, choosing the course of action that is calculated to provide "the highest attainable point on his preference scale."[77] Jay Albanese points out that technology creates easy-

access criminal opportunities—i.e., opportunities that are not created by motivated offenders, but simply provide easy access to illicit funds.[78] There is little risk and high expected utility. For an unaffiliated smart power agent, given the opportunity to hack into a rich consumer database and reap substantial profits—i.e., an identity-theft scheme—why would she/he **not** opt to become a criminal, either in isolation or as a member of an organized group?[79]

This is a legitimate question. Why be a digilante when it is more profitable to be a criminal? Nir Kshetri observes that in Eastern Europe and the former Soviet Bloc—where licit economies have been "too small to absorb the existing computer talent" and where there is large-scale technological unemployment stemming from the 1998 Russian crash—technological talent has been almost naturally co-opted into organized crime.[80] For instance, in Romania, frustrated by the lack of competitive employment opportunities, "some of the world's most talented computer students are exploiting their talents online."[81] Indeed, across the entire region, where organized crime groups may pay up to 10 times as much as "legitimate [information technology] IT jobs," a substantial proportion of the unaffiliated youth are being rechristened as criminal affiliates.[82]

However, proximity to even easy-access criminal opportunities is not necessarily deterministic in predicting criminal activity. Beyond the prospect of a "digilante identity" that imbues digilantes with the desire to "fight the good fight" (which will be briefly explored in the concluding remarks of this chapter), where rational choice is concerned, Elinor Ostrom famously pointed out that **individuals undertake collective action to solve social dilemmas**—and thereby avoid the "tragedy of the commons" or the net irra-

tional outcomes that occur when all individuals act in their isolated self-interest.[83] As she argued, "face-to face communication so consistently enhances cooperation in social dilemmas."[84] Though cyberspace does not directly provide this face-to-face communication, it does arguably create an efficient forum in which stakeholders can learn, communicate, and debate social dilemmas (as well as solutions to those dilemmas). There is evidence from the virtual world—especially Massive Multiplayer Online Role-Playing Games (MMORPGs)—that, in the absence of an effective designated enforcer, "good" vigilante groups will band together to safeguard new players—and strangers—from exploitation by advanced players (i.e., "newbie farming.") This is for the purpose of creating a fair playing space.[85] It is not a far cry to think that this cooperative discourse translates further into cyberspace.

In the end, proximity to easy-access criminal opportunities may thus co-opt some smart power individuals, but it is by no means a guaranteed outcome (even if we think in purely rational terms). Digilantes—perhaps evolved from the early curiosity seeking hackers—are not necessarily prone to partake in organized criminal activities.[86] These technologically-savvy people have the ability to recognize the problems of the status quo rationally, and also perhaps, the power to redress the situation.

CONCLUSION

This chapter has endeavored to assess the breadth of transnational organized crime in the digital age, as well as the potential for digilantes to act as collaborative regulators. As noted above, this is not a comprehensive argument, but a very early plausibility probe

of the data at hand. Greater research on the direct relationship between digilantes and organized crime is necessary. Anonymous vs. Los Zetas is a natural starting point, but research into the relationship between, for instance, the Chinese Triads and the Human Flesh Search Engine may also prove fruitful in the course of this investigation.

Another major area ripe for further research is the digilante subculture and identity, and especially its relation to the state and international organizations. Indeed, understanding the "digilante identity" is critically important in understanding "digilante agency," and insights from psychology and anthropology may have much to contribute to this discourse. It might be said that while profits and markets give utility in terms of security, human relationships often give utility in terms of purpose. Tyrone Adams and Steven Smith have made the argument that e-communities—electronic tribes—are forming around ideas.[87] Saskia Sassen further points out that there are constitutive processes in cyberspace:

> Digital space is partly inscribed by the larger power dynamics and cultural forms of the institutional orders or larger societies within which it is embedded. But digital power is not simply a mirror image of that world. . . . These new types of networks and technologies are deeply imbricated [sic] with other dynamics; in some cases the new ITs are merely derivative—a mere instrumentality of these dynamics—and in other cases, they are constitutive.[88]

Profits—collective and independent—do matter. However, social frames and values are also significant. When imported and projected into e-communities, our real life social frames—such as the "vigilante

hero"—might be a source of digilante agency as well. Analyzing depiction of criminal justice in children's literature and popular media, Lisa Kort-Butler identifies those heroic social frames that we (perhaps unknowingly) invest in and give meaning to:

> First, the justice system is often depicted as ill equipped to handle serious crime. Second, story lines suggested that the justice system is relatively weak, plagued by corruption or ineffectiveness. Third, heroes are driven by their notions of justice, recognizing that only they can stop the worst criminals and are morally obligated to do so. Fourth heroes are willing to use force to capture offenders, but they also use brainpower. Finally, although heroes work largely outside the law, they are supportive of the efforts of honest justice system actors.[89]

Lacking any strong corroborating evidence, this chapter does not put forth any argument that vigilante hero frames implicitly drive digilante mobilization, but it is worth asking if these social messages and frames are more than coincidental in cyberspace governance (i.e., cyberspace even provides secret identities in the anonymity that characterizes cybercommunication). Could it be that we are not merely living in the digital age, but may actually be entering the "Golden Age of the E-Superheroes"?

ENDNOTES - CHAPTER 16

1. For examples of scholars that identify this profit-based relationship, one may look at Jay Albanese, *Organized Crime in Our Times*, Burlington, MA: Elsevier, 2010. See also Michael Levi and Mike Maguire, "Financial and Organized Crime in Europe: Converging Paradigms of Control?" in Mortsel, Belgium: *Universalis: Liber Amicorum Cyrille Fijnaut*, 2011, pp. 723-734. The UNODC further identifies this market function in its 2011 and 2010 reports, "Thematic Programme: Action Against Transnational Organized

Crime and Illicit Trafficking, Including Drug Trafficking 2011-2013," New York: UNODC, 2011; "The Globalization of Crime: A Transnational Organized Crime Threat Assessment," New York: UNODC, 2010. It should also be noted that this paper also differentiates criminal organizations from terrorist organizations. Though terrorist organizations share many of the same features of criminal organizations, the more determinate political goals that characterize terrorist organizations are neither a sufficient, nor a necessary condition for organized crime (though they do often exist).

2. The term is attributed to Saskia Sassen, specifically recognizing that "electronic space"—though imbued with some power dynamics and cultural orders from the "real world"—is not simply a mirror image of the real, physical world. It has its own novel properties, and as such, will operate by slightly different rules than the physical world. See Saskia Sassen, *Globalization and Its Discontents: Essays on the New Mobility of People and Money*, New York: New Press, 1998, p. 182. Also, see Sassen's interview, "Space and Power" by N. Gane in *The Future of Social Theory*, 2004, available from Sassen's personal website, *saskiasassen.com/pdfs /interviews/space-and-power.pdf*.

3. See Susan Brenner, "Organized Cybercrime-How Cyberspace May Affect the Structure of Criminal Relationships," *North Carolina Journal of Law & Technology*, Vol. 4, 2002/03, pp. 1-50; see also Nir Kshetri, *The Global Cybercrime Industry*, Berlin, Heidelberg, Germany: Springer, 2010.

4. In a recent study on public support for vigilantism, Haas *et al*. summarized, "Vigilantism is commonly said to occur when citizens, from whom authorities are supposed to derive their legitimacy, believe that the criminal justice system is inadequate." See Nicole Haas *et al*., "Public Support for Vigilantism: An Experimental Study," *Journal of Experimental Criminology,* Vol. 8, pp. 387-413.

5. Public vigilantism **against organized crime** is rarely successful, as vigilantes are highly vulnerable to identification and reprisals by the criminal agents. This will be elaborated on in section two of this chapter.

6. In 2007, Joseph Nye popularized a similar term of "smart power" to describe "the ability to combine hard and soft power into a successful [foreign policy] strategy." My meaning of "smart power" is distinct from this, and I will apply smart power instead to speak to an individual agent's power context as situated in the ICT global market. For more on Nye's foreign policy definition, see Joseph Nye, "Smart Power," *Huffington Post,* November 27, 2007, available from *huffingtonpost.com/joseph-nye/smart-power_b_74725.html.*

7. This question is attributed to Jay Albanese, "The Causes of Organized Crime: Do Criminals Organize Around Opportunities for Crime or Do Crimnal Opportunities Create New Offenders?" *Journal of Contemporary Criminal Justice*, Vol. 16, No. 4, 2000, pp. 409-423.

8. "Plausibility probe" respective in the research tradition of Alexander George and Andrew Bennett, *Case Studies and Theory Development in the Social Sciences*, Cambridge, MA: MIT Press, 2005.

9. "The Global Regime for Transnational Crime," Issue Brief, Washington, DC: Council on Foreign Relations, June 25, 2013, available from *cfr.org/transnational-crime/global-regime-transnational-crime/p28656?cid=rss-economics-the_global_regime_for_transnat-070212*; See also Mats Berdal and Monica Serrano, *Transnational Organized Crime and International Security*, Boulder, CO: Lynne-Rienner, 2002.

10. UNODC, "Thematic Programme," UNODC, "Globalization."

11. "New UN campaign highlights financial and social costs of transnational organized crime," New York: United Nations, July 16, 2012, available from *un.org/apps/news/story.asp/story.asp?NewsID=42480&Cr=Drugs&Cr1=#.U1Lez158lBV*.

12. Phil Williams and Roy Godson, "Anticipating Organized and Transnational Crime," *Crime, Law & Social Change*, Vol. 37, 2002, pp. 311-355.

13. *Ibid*., pp. 317. Also on this model, see Mitchel Roth, *Global Organized Crime: A Reference Handbook*, Santa Barbara, CA: Abc-Clio Inc., 2010.

14. Edward Kleemans, "Organized Crime and the Visible Hand: A Theoretical Critique on the Economic Analysis of Organized Crime," *Criminology and Criminal Justice*, Vol. 13, No. 5, 2012, pp. 615–629. An important distinction of social models from economic models is that for social models, even before profits are calculated, emphasis is placed on human relations. In order for operations to be carried out effectively, there must be some degree of **social trust** within the network. This may have ramifications. See Klaus Von Lampe and Per Old Johansen, "Organized Crime and Trust: On the Conceptualization and Empirical Relevance of Trust in the Context of Criminal Networks," *Global Crime,* Vol. 6, No. 2, 2004, pp. 159–184; see also Jeffrey Mcillwain," Organized Crime: A Social Network Approach," *Crime, Law & Social Change,* Vol. 32, 1999, pp. 301–323.

15. Kleemans, p. 619.

16. *Ibid*., p. 620.

17. Williams and Godson, pp. 328-334.

18. See Brenner, "Organized Cybercrime"; Albanese, *Organized Crime*; Albanese, "The Causes,"; Levi & Maguire; UNODC, "Thematic Programme"; UNODC, "Globalization"; also see Steven Mallory, *Understanding Organized Crime*, Burlington, MA: Jones & Bartlett Publishers, 2011.

19. For instance, Kleemans warns again a purely economic explanation as he points out the critical juncture between "social embeddedness" and effective transnational criminal operations. Kleemans, p. 618.

20. UNODC "Thematic Programme"; UNODC, "Globalization."

21. Williams and Godson, p. 328.

22. *Ibid*., p. 328.

23. *Ibid*., p. 328.

24. Roth, p. 41; Albanese p. 237; Also see Jack Blum *et al*., "Financial Havens, Banking Secrecy, and Money Laundering," *UNODC Crime Prevention and Criminal Justice Newsletter,* Vol. 34/35, Prod. UNODC, 1998, available from *imolin.org/imolin/finhaeng.html*.

25. Mallory, p. 7.

26. Williams and Godson, p. 342.

27. See Peter Andreas, "Transnational Crime and Economic Globalization," in Mats Berdal and Monica Serrano eds., *Transnational Organized Crime and International Security*, Boulder, CO: Lynne Rienner, 2002, p. 39. Andreas notes that the economic liberalization of the past half-century has undoubtedly expanded transnational criminal horizons. Smuggling, for instance, has been transformed. While smuggling has existed as an illicit activity since the advent of cross-border economics, with globalization:

> what has changed are the commodities smuggled, the speed and method of transport, the size, structure, and location of the smuggling organizations, the content of state laws and the intensity and form of their enforcement, and the nature and level of consumer demand.

28. Peter Andreas, "Illicit Globalization: Myths, Misconceptions, and Historical Lessons," *Political Science Quarterly*, Vol. 126, No. 3, 2011, pp. 403-425.

29. *Ibid*., p. 416.

30. Andreas does acknowledge "new and enabling technologies" as contributing to transnational criminal growth. However, he seems to treat digital technologies as an equally accessible medium for both criminal enterprises and law enforcement, and has high optimism that law enforcement will harness these technologies to halt the burgeoning criminal activities. For more on this, see Andreas, "Illicit," pp. 415-6. I am not convinced this is the case, especially because cyberspace has those unique operative features which disturb the state's traditional monopoly of force.

31. For this purpose, I will adopt the definition of globalization echoed by Daniela Archibugi and Simona Iammarino, which recognizes globalization as the "intensification of world-wide social relations which link distant localities," but specifically emphasizes the innovative prospects and frontiers (i.e., "the increased international integration of economic activities and the raising importance of knowledge in economic processes"). See Daniela Archibugi and Simona Iammarino, "The Globalization of Technological Innovation: Definition and Evidence," *Review of International Political Economy*, Vol. 9, No. 1, 2002, p. 98.

32. Michael Levi, "Liberalization and Transnational Financial Crime," in Berdal and Serrano eds., *Transnational Organized Crime and International Security*. Also see Martha Roldan, "From 'Information' to 'Knowledge' Societies? Argentina in the Context of Engendered Regional Globalization," in Cecilia Ng and Swasti Mitter, eds., *Gender and the Digital Economy: Perspectives from the Developing World*, New Delhi, India: Sage, 2005.

33. *Ibid*., p. 64.

34. *Ibid*.

35. *Ibid*.

36. Brenner, "Organized Cybercrime."

37. *Ibid*.

38. Since the early-2010s, the large majority of elder criminal band (BACRIM) leaders have been "neutralized" by the Colombian government and internal conflicts. See Juan Carlos Garzón *et al*., *The Criminal Diaspora: The Spread of Transnational Organized Crime and How to Contain Its Expansion,* Washington DC: Woodrow Wilson International Center for Scholars, 2013, e-book available from *wilsoncenter.org/sites/default/files/CRIMINAL_DIASPORA%20(Eng%20Summary)_0.pdf*.

39. Garzón *et al*., pp. 8-9.

40. Daniel Alexander "Policing and the Global Paradox," *FBI Law Enforcement Bulletin,* Vol. 71, No. 6, 2002. Also quoted by Kshetri, p. 25.

41. Yvonne Jewkes and Majid Yar, *Handbook of Internet Crime*, New York: Routledge, 2013, p. 393. Also see Susan Brenner, "Cyber-Threats and the Limits of Bureaucratic Control," *Minnesota Journal of Law, Science, and Technology*, Vol 14. No. 1, 2013.

42. Kshetri, p. 44.

43. *Ibid*.

44. UNODC, "Globalization," p. 29.

45. It should be noted that the annual cost of organized crime estimated earlier by the UNODC does not speak to the "social cost," or to the number of human lives detrimentally impacted, as a result of organized crime. The UN writes, "Each year, countless lives are lost to drug-related health problems and violence and firearm deaths, among other causes. In addition, some 2.4 million people are victims of human trafficking." The Council on Foreign Relations points out that drug trafficking in Mexico has contributed to over 50,000 deaths alone in the past 6 years. These numbers are not tallied in total net losses, but the real, human victims of organized crime should not be forgotten.

46. UNODC, "Globalization," p. vi.

47. UNODC, "Thematic Programme," p. 20. Though according to the UNODC's earlier 2010 report, some estimates put this number as high as U.S. $1 billion annually. See UNODC "Globalization," p. 13.

48. UNODC, "Globalization," p. 13.

49. As a newly-emergent phenomena distinct from "vigilantism," I will here loosely draw from the loose operational term offered by Dara Byrne, but suggest the following definition of digilantism: "The manipulation of network technologies to promote a political agenda that *reconciles some absence of government*, and which may unfold across local, national, and international lines." For Byrne's original definition, see Dara Byrne, "419 Digilantes and the Fronteir of Radical Justice Online," *Radical History Review*, Issue 117, Fall 2013, p. 72.

50. Christopher Winters, "Cultivating a Relationship That Works: Cyber-Vigilantism and the Public versus Private Inquiry of Cyber-Predator Stings," *University of Kansas Law Review,* Vol. 57, 2008/9, pp. 427-460. Also see "Suspected Paedophiles Arrested After Vigilante Parents Pose as Underage Girls Online," *The Independent*, April 22, 2013, available from *independent.co.uk/news/uk/crime/suspected-paedophiles-arrested-after-vigilante-parents-pose-as-underage-girls-online-8583252.html*.

51. As of December 2014. See Perverted Justice's personal website, *perverted-justice.com*.

52. "Suspected Paedophiles."

53. For instance, the refusal to provide those goods and services that facilitate organized crime. Levi and Maguire have previously said:

> It is worth emphasizing that the organization of crimes results from . . . a dynamic process that evolves as offenders adapt (or fail to adapt) to their changing environment, including facilities offered by the legal commercial environment, such as container trucks and ships, car repair firms, payment card issuers and merchants, and financial institutions.

Levi and Maguire, p. 4. The private sector may need to consider making a conscious effort to avoid this.

54. Brenner, "Cyber-Threats," pp. 148-9.

55. "UK Cyber Defense Unit 'May Include Convicted Hackers'," BBC, October 22, 2002, available from *bbc.com/news/technology-24613376*; Andy Greenberg, "Pentagon Seeks High School Hackers," *Forbes*, May 21, 2009, available from *forbes.com/2009/05/21/cybersecurity-students-hackers-technology-security-cybersecurity.html*; See also Gerry Smith, "Feds Turn to Hackers to defend Nation in Cyberspace," *Huffington Post,* August 8, 2011, available from *huffingtonpost.com/2011/08/08/government-recruits-hackers-cyber-shortage_n_920795.html.*

56. Andy Greenberg, "'Silk Road 2.0' Launches, Promising a Resurrected Black Market for the Dark Web," *Forbes*, November

9, 2013 available from *forbes.com/sites/andygreenberg/2013/11/06/silk-road-2-0-launches-promising-a-resurrected-black-market-for-the-dark-web/*.

57. See Marc Goodman, "What Businesses Can Learn from Organized Crime," *Harvard Business Review*, November 2011, available from *hbr.org/2011/11/what-business-can-learn-from-organized-crime/ar/1*; also see Kshreti.

58. Greenberg, "Silk Road 2.0."

59. Brenner, "Cyber-Threats," p. 148.

60. One remarkable outlier to this may be Mexico's Michoacán vigilantes, who still remain in fair isolation from the national government despite a January 2014 agreement to merge into a joint "Rural Defense Corps." For more on this, see Tracy Wilkinson and Cecilia Sanchez, "Vigilantes to Disarm in Mexico's Michoacán State," *The Los Angeles Times,* April 15, 2014, available from *latimes.com/world/worldnow/la-fg-wn-mexico-michoacan-vigilantes-20140415,0,3543571.story#axzz2zw3W97EV*; Tristan Reed, "Mexico's Drug War: Substantial Changes Seen in Michoacán," *Forbes*, April 17, 2014, available from *forbes.com/sites/stratfor/2014/04/17/mexicos-drug-war-substantial-changes-seen-in-michoacan/*.

61. Kate Meagher, "Hijacking Civil Society: The Inside Story of the Bakassi Boys Vigilante Group of South-eastern Nigeria," *Journal of Modern African Studies*, Vol. 45, No. 1, 2007, pp. 89-115.

62. Byrne.

63. "Trophies" such as embarrassing and/or humiliating photos requested by a 419 scambaiter, and delivered by the scammer, as pretext for establishing trust. See Byrne's appendix for illustrations.

64. Byrne, pp. 71-2.

65. See "African Criminal Enterprises," Washington, DC: FBI, available from *fbi.gov/about-us/investigate/organizedcrime/african*.

66. Byrne, pp. 75-78.

67. Gabriella Coleman, "Anonymous in Context: The Politics and Power Behind the Mask," *CIGI Internet Governance Papers,* Waterloo, Ontario, Canada: Centre for International Governance Innovation, 2013, p. 2.

68. David Goldman, "Hacker Group Anonymous is a Nuisance, not a Threat," CNN (Money Section), January 20, 2012, available from *money.cnn.com/2012/01/20/technology/anonymous_hack/*.

69. Coleman, p. 3.

70. Coleman, p. 7.

71. Paul Kan, "Cyberwar in the Underworld: Anonymous vs. Los Zetas in Mexico," *Yale Journal of International Affairs*, Winter 2013, available from *yalejournal.org/article_post/cyberwar-in-the-underworld-anonymous-versus-los-zetas-in-mexico/*.

72. *Ibid*.

73. *Ibid*.

74. Paul Kan, "Anonymous vs. Los Zetas: The Revenge of the Hacktivists," *Small Wars Journal,* June 27, 2013, available from *smallwarsjournal.com/jrnl/art/anonymous-vs-los-zetas-the-revenge-of-the-hacktivists*.

75. *Ibid*.

76. A spokesperson of the local branch, Anonymous Free-Acuña, reported that the organization is collecting "hundreds of pieces of information" from sources across the area, implying a broad public support. Kan, "Cyberwar."

77. Herbert Simon, "A Behavioral Model of Rational Choice," *The Quarterly Journal of Economics,* Vol. 69, No. 1, 1955, p. 99.

78. Albanese, "Causes," p. 414.

79. Even when we recognize that decision-makers exist in a dynamic environment where they cannot make decisions based

on static utilities, but must account for the behavior of other actors, this is still likely to lead us to the conclusion that agents will still opt into "easy-access" crimes. After all, if agents remain protected under cover of a near-untraceable identity (i.e., small risk of retaliation), why would they **not** engage in criminal activities or hack-for-profit?

80. Kshetri, pp. 38-9.

81. *Ibid*., p. 38.

82. *Ibid*.

83. Elinor Ostrom, "A Behavioral Approach to the Rational Choice Theory of Collective Action," *American Political Science Review,* Vol. 92, No. 1, pp. 1-22; Also, Schelling early on pointed out that the rational system is not necessarily bound to produce "collectively satisfactory results." Thomas Schelling, *Micromotives and Macrobehavior*, New York, W. W. Norton & Co, 1978, p. 25.

84. Ostrom, p. 1.

85. Benjamin Duranske, *Virtual Law: Navigating the Legal Landscape of Virtual Worlds,* Chicago, IL: American Bar Association, 2008, pp. 66-68.

86. For more on this, see "The Conscience of a Hacker," an early declaration of hacker motives, published in 1986. A transcript of this document—also referred to as "The Hacker Manifesto"—can be found in the Phrack archives available from *phrack.org/archives/issues/7/3.txt*.

87. Tyrone Adams and Steven Smith, *Electronic Tribes: The Virtual Worlds of Geeks, Gamers, Shamans, and Scammers*, Austin, TX: University of Texas Press, 2008.

88. Sassen, "Space and Power."

89. Lisa Kort-Butler, "Justice League? Depictions of Justice in Children's Superhero Cartoons," *Criminal Justice Review,* Vol. 38, No. 1, 2013, p. 50.

CHAPTER 17

FROM CYBERCRIME TO CYBERWAR: INDICATORS AND WARNINGS

Timothy J. Shimeall

INTRODUCTION

Infrastructure and organization defenders categorize malicious actors in several ways, one of which may be the level of damage the actors seek to inflict and the motivation they have in inflicting this damage. John Howard and Thomas Longstaff, for example, categorized these actors (termed "attackers") into six groups based on damage and motivation.[1] These categories are summarized in Figure 17-1 below. Since Howard and Longstaff developed this categorization, other groups of attackers have emerged, including those we term "activists" and "warriors." Activists attack computers either to push information for advocacy or to use their online activity to influence decisions related to their specific issue.[2] Warriors attack computers to support real-world conflicts by interfering with information flows critical to some of the contending parties.[3] Other categories may need to be revisited to reflect the emergence of ideological as an addition to political motivations for online activity, particularly in the "spy" and "terrorist" categories. Howard and Longstaff's purpose was describing computer security incidents, and they did not include shifts of intruder behavior that might signal actors who should be categorized differently. This chapter describes possible indicators of such shifts, specifically from professional criminals or activists to spies, warriors or terrorists or

states, acting directly or through proxies. This chapter does not discuss initial categorization of actors but rather is focused on shifting categorization.

hackers — attackers who attack computers for challenge, status or the thrill of obtaining access.

spies — attackers who attack computers for information to be used for political gain.

terrorists — attackers who attack computers to cause fear for political gain.

corporate raiders — employees (attackers) who attack competitor's computers for financial gain.

professional criminals — attackers who attack computers for personal financial gain.

vandals — attackers who attack computers to cause damage.

Figure 17-1. Malicious Actors from Howard and Longstaff.[4]

The consideration of actors, and the level of damage they might inflict guides a wide range of organizations in dealing with malicious activity. The American National Standards Institute (ANSI) and the Internet Security Alliance, for example, sponsored a series of workshops on managing cyber-risk, which included an examination of the threats that various actors pose and the damage that they may inflict.[5] Actors that strike with particular persistence and levels of preparation are of most concern, especially if their impacts are intended for larger effects on society and its leaders. When a set of malevolent actors shifts from more casual to more premeditated methods, the rapid recognition of this shift motivates more prioritized and thorough defensive action.

Anonymous is a loosely-knit group of hackers that evolved over several stages from people communicating over the "4chan" open communication forum around 2008.[6] The initial group was primarily motivated by status and amusement. Although always unstructured and nonhierarchical, the group evolved,

becoming more exclusive and separatist in nature, focusing on website defacement for activist advocacy and for low-level disruption. Their initial campaign was against Scientology. In this campaign, they found that unstructured anonymity and collective action could be effective against even well-resourced opponents. The group also became strident in its opposition to government intervention in information distribution (filtering pornography, copyright protection, etc.). This stridency resulted in an increasingly sophisticated series of online attacks (although with a loosely-knit group, there is a considerable range in the attack sophistication). Starting with denial-of-service attacks, the attackers advanced into information theft and extortion. Over time, these attacks became less focused on generic or commercial organizations and more directly focused on governmental organizations. In particular, the group participated in support of movements in North Africa during the Arab Spring uprisings, attacking and undermining governmental monitoring efforts. Subsequently, the group attacked Israel (in response to a military operation in Gaza), portions of the U.S. Government (in response to hacker prosecutions), and Muslim extremist groups (in response to attacks on journalists and to restrictions on public expression). Effectively, the group had become more supportive of anarchic or anti-governmental aims, supporting such aims militantly, or responsive to attacks on either its members or against parties perceived as innocent.

In August 2008, a conflict between regions inside the nation of Georgia escalated into an armed incursion by Russian forces into Georgia,[7] with a significant (and subsequently very thoroughly analyzed) cyberattack surrounding this incursion.[8] The cyberattackers

were recruited through a variety of Russian and Russian-oriented websites, some associated with the Russian mafia. The attack consisted of flooding for denial of service and traffic manipulation leading to website defacement. Some of the flooding assets were used for cybercriminal actions before and during the timeframe of the cyberattack. Following the attack, numerous statements alleged participation by the Russian government in these attacks, but none was fully substantiated. Later events and publications have shown that this attack is in line with Russian military theory and doctrine, and several further examples have been noted, including cyberactivity in support of their incursion into Crimea.[9] Over time, these events have shown cyberwar activity aligning more closely with attacks to modify public opinion and to denigrate possible opposition, as well as continuing to hamper efforts by opponents, both defensive and offensive.

These cases appear to be representative of a larger trend: Online criminals may act, over time, and given sufficient motivation, in a manner that asserts the interests of one nation-state against another nation-state. This chapter discusses the transition of such groups from largely financially-motivated targets and private interests (cybercrime) to politically or ideologically-motivated targets and national interests (cyberwar). More formally, this chapter adopts an accepted definition of the term "cyberwar" as "any virtual conflict initiated as a politically motivated attack on an enemy's computer and information systems."[10] The distinction between cyberwar and cyberactivism lies both in the degree of potential damage (coercion rather than persuasion) and in the association with or opposition to national interests (nation-associated goals rather than ideology-associated goals). While this chapter will

focus on cyberwar, it will occasionally include discussion of the more extreme forms of cyberactivism.

The discussion provides some insight into indicators of such transitions and of the degree of activity associated with such transitions. The Anonymous and Georgia incursion cases will be used as running examples, but these are not the only such examples; several others have been cited in the literature and are also discussed here.[11]

The next section provides an overview of the transition from cybercrime to cyberwar, identifying the changes which may provide a basis for assessing this transition. The second section steps through an attack process and outlines potential indicators for the transition from cybercrime attacks to cyberwar attacks at various steps along the way. The chapter closes with a discussion of some limitations of the methodology.

FROM CYBERCRIME TO CYBERWAR

An indicator is a known or theoretical step which the adversary should or may take in preparation for hostilities.[12] Indicators are grouped into lists for monitoring purposes and interpreted to provide assessments of adversaries. This chapter focuses on one aspect of the monitoring and interpretation process, and particularly of one application of that aspect. A "shift," as used here, is a change in hostilities that may be detected or inferred from available data. While changes might occur that are invisible to defenders (in attacker's understanding, for example), these do not factor into defensive decisions and are not considered in this section. Network usage is inherently dynamic, as technologies, missions, and data are always changing. This is no less true for malevolent actors than for

other network users. From this dynamic usage, certain events are designated for monitoring as indicators (often related to attack models such as the cyber-kill-chain).[13] The indicators serve as input to the process of assessing shifts. Interpreting these shifts provides a basis for defensive decision-making.

The specific shifts of concern relate to malicious actors going from cybercrime to cyberwar activities. These shifts include those of motivation, aggression, methods, and impact. In aggregate, these provide for more actors moving to affect the political process, not just focusing on financial or status gains.

A shift in motivation is detectable via new targets, statements from the actors, or coordination between physical events and network activity. The actors display a shift in motivation via new targets when those targets both involve opportunities for politically-oriented gain (activity to influence either individual political leaders or the general climate of opinion of the populace) and impact on an industry or infrastructure sector different from those targeted in prior activity. For example, the Anonymous group's increased emphasis on revealing secrets that denigrate or discredit organizations that they target, as opposed to extortion or fraud, serve as indicators of more serious motivations leading toward cyberwar. Statements from the actors suggesting a shift in motivation may appear on the actors' websites, defaced websites, in online discussions, or in public releases such as press statements or online videos. Continuing the Anonymous example, a series of statements by the group showed their intent and motivation to fight restriction of information and decrease privacy of organizations that they target, based on their philosophy of anarchy. These statements appeared initially as online videos,

but as their activity attracted more attention, more appeared as direct press releases. Discerning a shift in motivation via coordination to physical events engenders more uncertainty. While the close proximity to an apparent physical event may make it appear to be a stimulus for the network event, presuming causality tends to lead to errors in analysis. As such, contemporaneous timing is best left as a supplemental or confidence-raising indicator. However, the very close timing between cyberactivity and the border incursion in the Georgian example, coupled with the choice of targets, shows the usefulness of such a supplemental indicator. Well after the attack, there were statements by Russian officials linking the attack to the overall Russian strategy.[14]

Detection of shifts indicative of motivation depends on either open-source or restricted-access monitoring of the affected networks, on the results of that monitoring being available for analysis, and on those results lending insight on the motivation of the actors. Open-source monitoring includes both the limited amount of network data that is published openly (principally samples of network attacks, statistical traffic summaries, and copies of defaced websites) and also news accounts or other openly distributed information. This data is generally accessible for analysis. Restricted-access monitoring tends to provide more detailed and comprehensive traffic data. Restricted-access includes both proprietary monitoring and monitoring performed by network service providers, content distribution networks, and network security vendors. As its name implies, data from this monitoring is generally controlled by access agreements or nondisclosure agreements. The analysis results lend insight on the motivation when they match with one of the criteria listed above.

Shifts in aggression apply principally to the rate of activity of malevolent actors. One characterization of this activity follows the classic "cyber-kill-chain" model, involving the establishment of preparatory sites, compromise of computers on targeted networks, exploitation of the compromised computer, or impact on military or political interests using the results of the exploitation.[15] In the Anonymous case, this rapid increase in aggression was observed during the 2010-11 timeframe, as the group differentiated itself from related organizations such as 4chan and AnonOps. The group rapidly deployed a broad-scale tool for denial of service and increased the rate at which it defaced and compromised networks. It shifted rapidly from a loosely-knit group of anarchists annoying specific organizations to a more targeted group taking on governments, large corporations, and well-resourced organizations.

Detection of shifts in the level of aggression is somewhat problematic. First, events need to be associated with the malicious actors, and attribution of actions (even when claims of responsibility are present) are problematic in cyberspace. Second, the significance of these events must be established, along with associations between events for cumulative effects, and this frequently involves making a number of assumptions about the victim organizations. Frequently, these victims are not willing to indicate the level of impact, and may either inflate (perhaps to support criminal prosecution) or minimize (perhaps to preserve organization reputation) the impact of these events. Third, the events need to be de-interleaved, since one or more events may start before previous events have completed. Finally, the rate of aggression (level of impacts per unit time, average interval between events, or other

measures) may be computed. As these measures trend over time, shifts may become apparent.

Shifts in methods indicate several possible changes, including that different malicious actors, have taken control over the computers used, that the same actors have changed tactics, or that different means of accomplishing the same tactics are being employed. On the other hand, in non-malicious and malicious networks, dynamic addressing may be employed, and a given address may be used by several different computers, or, less commonly, networks may shift address spaces.[16] This dynamic addressing may produce observations similar to the indicators of shifts in methods. These less malicious explanations serve as alternative hypotheses to be dealt with in analysis. Methods may be reflected in overall traffic levels involving the malicious actors (or experienced at the targeted network), in the mix of network ports involved, in the sizing and timing of network traffic, or in the specific targets selected. One example of shifting methods is in the Georgian attack, where the malevolent actors moved from methods that largely dealt with financial fraud and extortion against financial institutions to methods that largely focused on critical infrastructure. The speed in this shift of methods reflected the degree of preparation and the level of urgency in supporting the physical aggression by actions on the part of the Russian-controlled computers.

Detection of shifts in methods involves using the network monitors on the target network to profile the range of behaviors exhibited by the malicious actors. A range of methods for profiling these behaviors exist, including broad scale techniques to monitor chains of network data (packets) and specific techniques to explore the content of individual packets.[17] By con-

necting a profile (which applications, how frequently used, against which targets, from which sources) with a malicious actor or group of actors, deviations or evolution in that profile over time become detectable.

Over time, shifts in methods and aggression tend to produce shifts in the impacts experienced by target networks. The modified impacts have already been alluded to in the preceding discussion on shifts of methods. Cybercrime-focused groups tend to be very opportunistic, with very destructive impacts only observed when this impact is readily monetized (e.g., for extortion) or a component of a monetized attack (e.g., blocking a vendor by a denial of service attack so that the malicious actors can impersonate that vendor and implant software to provide unauthorized access). Cyberwar efforts historically have been more interested in destructive impacts (e.g., sending commands that damage connected devices, flooding networks, destroying data on hosts) than on impacts that readily yield monetary rewards. The change in balance between these two forms reflects the shift of impact. Cybercrime groups tend to be motivated externally: money, position, or reputation. Cyberwar groups tend to be motivated internally: accomplishment of mission, morale, and lending prestige to their cause or nation. A shift tilting impact toward cyberwar will be one that moves from annoyance-level monetary reward and ego-driven statements and toward more subtle results that affect the critical infrastructure. The Georgian example shows this shift, as the network that had previously been used for financial fraud and dissemination of unwanted email shifted to targeted compromises of government and military sites in Georgia, along with flooding against their networks. While there still was some (opportunistic) fraudulent

activity present, the bulk of the impact shifted to support the malicious actors.

The shift of impact may be detectible by looking at the cumulative effect of actions against the target network. One change will be which computers are targeted by the malevolent actors. Examining newly targeted computers in light of the missions assigned to those computers, and also the type of effects the malicious actors are seeking on those computers, will provide some indicators of the shift of impact. Noting any change in the pacing of aggressive activity against the target network, or relationship of that timing with real-world events, serve as further indicators of this shift.

In combination, multiple shifts serve to improve confidence in the assessment that a group is shifting its pattern of activity. A single detected change is likely not definitive. Cybercriminals often modify the pacing of their attacks. Actors have also been observed to vary the methods of attack, particularly when a new vulnerability or style of attack has become public. By combining results of assessing multiple shifts, however, an analyst may more robustly assess the malicious actor's intent behind its activity. This assessment should be undertaken with caution. While there exist well-publicized examples (as cited in this chapter), malevolent actors shifting from cybercrime to cyberwar is (fortunately) a rare event and the analysis methods need to be calibrated as such. Therefore, it is probably more common for cybercriminals to shift to less malicious behavior. There are numerous examples of such criminals converting to "gray hat," mixing authorized and unauthorized activity, or "white hat," shifting to purely authorized activity. In preparation for such a conversion, several shifts in behavior might

be expected. It is also common for cybercrime groups to split or cease operation. These groups tend to have a lot of internal distrust, and this lack of trust encourages divisions over goals and targets for the group.[18] As the members mature, they might also drop out of the group although this tendency has become less pronounced in recent years due to the monetization of cybercrime behavior. As shifts are identified, a division of the group might form an alternative hypothesis to be explored in the analysis.

Indicators.

The indicators available to computer network defenders can be categorized in several ways. One categorization is by the source of the indicators, whether they are collected internally to the defended network or externally to it. Another categorization is by the type of data used in the indicator, further subcategorized by host, service, or network data. Table 17-1 shows the interaction of both categorizations, illustrated by examples of network behaviors that might be indicated by the source and data involved. In this table, the source-based categories have been subdivided by the form of information from which the indicators are derived. A report is a descriptive document covering the behaviors. A rule is a specific set of conditions to support automated suppression of the behaviors. An observation is an alert, set of data, or artifact that displays the behaviors. The data from categorization is further divided into log and content subcategories for each type. The body of the table provides examples of the possibly malicious behaviors that might be associated with the intersection of categories.

Source\Data	Host Logs	Service Logs	Service Content	Network Logs	Network Content
Internal Report	Illegal login	Service shutdown	Service compromise	Resource exhaustion	DNS cache poisoning
Internal Observation	File system compromise	Data exfiltration	Web defacement	Flooding	Illicit email
External Report	Vulnerability reports	Vulnerability reports	Vulnerability reports	Address watchlist	Incident reports
External Rule	Antivirus	Host firewall rules	Spam signatures	Address blackout	Firewall rules
External Observation	File or registry changes	Domain watchlist	Web defacement	Incident signatures	Attack indicators

Table 17-1. Type of Behavior Categorized by Indicator Source and Data.

Historically, a primary indicator of malicious actors shifting from cybercrime to cyberwar has been statements from the actors themselves. In the case of Anonymous, these statements took the form of postings on the actors' website, or statements left in discussion groups.[19] In some attacks, press releases or other public statements were made. These releases are somewhat unreliable since the malicious actors may be unwilling to discuss all of their actions, current or planned, to maintain strategic surprise against targeted organizations. In the Georgian example, no contemporaneous announcement was made by the malicious actors.[20]

Third party assessments of activity by the malicious actors may be more robust. There are several organizations, such as iSight Partners,[21] Mandiant,[22] or Renesys,[23] that analyze various forms of network activity and generate specific reports either for client organizations or summarizing effects in a given infrastructure of a geographic region. The Computer Emergency Readiness Team (CERT) and other broad-

scale security groups also disseminate assessments of cyberactivity that may be useful in analyzing the intent of malicious actors.[24]

There are also more technologically-focused indicators distributed either by user groups or vendors of specific network technologies (routers, antivirus, firewalls, email, web, file sharing, intrusion detection, or prevention systems, etc.). These indicators are often configurations or rules for the specific technologies to use in addressing specific malicious activity. Sometimes these are associated with reports that link the malicious activity with larger technical threats (e.g., the annual Symantec Threat Report).[25] Some of these indicators are lists of addresses and domains for use in access control lists or in web proxies to block users from accessing malicious sites. When implemented to filter network activity, the rules and control lists cause the filtering tools to produce alerts that might indicate network threats. These alerts often describe specific (most proximate) sources, the target against which the activity is directed, the time of the activity, and the specific nature of the activity. All of these provide insight into the behavior of actors and on shifts in that behavior. However, because they are focused tightly on specific technologies, these lists and rules might have ephemeral effectiveness, particularly for actors that wish their activities to go unnoticed. Linking these indicators together for a more complete profile of activity could also prove difficult. Different vendors and technologies report quite differently, both in format and content of their reports. There are often not conventional labels that link alerts across technologies. Some security event management systems consume streams of alerts and link them by pre-established information as to where the alerts are generated and how to infer associations between alerts.

Another information source is reported activity from personnel who work within the defended organization. This information is often symptomatic—files with changed content, information lost, computers behaving unexpectedly or shutting down, lost contacts. However, these users may provide an insight indicative of a larger problem, and with context, identify a more serious attack emerging.

This section uses these categories to discuss how indicators may reflect shifts in motivation toward cyberwar. The discussion associates indicators with the phases of a cyberattack. In some cases, indicators from one phase may be useful in assessing later phases.

Indicators of Preparation.

The preparation phase of a cyberattack is where the malevolent actors are assessing potential targets, placing resources to use in the attack, and doing other advance work before initiating an attack. The principal difficulty in gathering indicators of preparation is that most of this activity will occur outside the scope of observation from the target of the subsequent attacks. For this reason, third-party analysis and reports might be the primary source of data for the indicators suggesting shifts in preparation.

Prior to an attack, there might be a change of alliances on the part of the malicious actors. Disagreements between actors are common, particularly when new causes, levels of activity, or targets are involved.[26] Statements on blogs or discussion groups might be indicators of these changing alliances, and third party information clearinghouses could well report on such statements. Technical indicators, including correlated activity (probing ports, protocols, or applications) on

a similar timeframe but from additional network locations might also indicate these changing alliances.

Beyond simple scanning, evidence of actors basing their attacks from new network locations (termed "hop points") may serve as indicators for shifts in preparation for a significant network attack. There is evidence that hop points used in cybercrime are quite persistent.[27] Criminals tend to keep the same locations since changing them is unproductive time, and they tend to use all of their locations (although not all against the same target), for an efficiency of operation. Surprise is a lesser concern in cybercrime than in cyberwarfare. In warfare, the hop points are often considered far more ephemeral, largely to defend against counterattacks and to help assure strategic surprise. Therefore, a noticeable change in network locations might serve as an indicator of preparation for a cyberattack.

During the preparation phase, any attack traffic generated will be intended for connectivity and access validation, rather than for deeper malicious effects. As such, they tend to be lower volume, more transient, and less followed-up on than in cybercrime. A noticeable shift in these characteristics from previously-used sources may serve as an indicator of preparation.

Some malevolent actors, seeking maximum strategic surprise, will validate hop points (typically very briefly and very cautiously) and then wait until attack initiation to further exploit these hop points. The risk to this strategy is that the utility of the hop points might be reduced (by chance or by defensive action) without the actors' awareness. This can threaten the planned attacks. An alternative strategy is to maintain a slow stream of traffic from the hop points, progressively moving to increasing activity so long as no defensive action or other limiting effects are observed.

Both strategies are quite different from the cybercrime strategies. In cybercrime, malevolent actors are using well-established methods, at a calibrated level against a broad population of targets; effectiveness against a given target is of lesser concern, so cybercrime tends to be stable, shifting only when outside factors act against the criminal infrastructures, such as a change in the ability to monetize the criminal attacks.[28]

By the nature of the activity, the preparation for cyberwar is difficult to assess. Many of the limiting factors discussed later in this chapter apply strongly to such assessment. Often, the preparation phase indicators will be significant only retrospectively. However, even given these cautionary notes, the retrospective recognition of preparation may serve as confirmation for the assessment of later phases of cyberwar attacks.

Indicators of Initiation.

The initiation phase indicates the malicious actors are performing an increasing number of attacks, even while perhaps continuing preparations for yet further attacks. The indicators for this shift are more visible than for previous shifts since attacks are visible as damage or attempted damage to the victim organizations. A variety of technologies exists for observing this damage or attempted damage including network traffic analysis.[29] Unfortunately, malicious actors are quite aware of these technologies, and, while some attackers are not concerned about detection, others fashion attacks that are less visible to detection technologies. Since network attacks are generated by software, modifying the characteristics of attacks is a matter of modifying that software. Methods that attackers have demonstrated in decreasing the visibility of their attacks include:

- Hiding attacks as benign network activity (e.g., by waiting for the target to contact a compromised third party, then embed the exploit activity within benign activity);
- Masking by modifying key characteristics of attacks (e.g., the apparent source of attack) that defenders use to alert or track attacks (masked by attackers using a distributed network of sources in combination), or by use of encryption (e.g., by installing a decrypting downloader, then encrypting all further traffic for conducting or directing the network attack);
- Blocking collection of network activity by either disabling or flooding the sensors for such activity; this has the added benefit (from the attacker's point of view) of distracting the network defenders toward protecting the sensor and away from protecting the true target of the attack.

To deal with malicious actors attempting to hide their attacks, defenders need to use a variety of approaches to identify attacks. This section is too brief for a full survey; the literature of network intrusion (a form of attack) detection is too large to do more than point to example indicators of initiating attacks.

Some of the indicators of attack initiation may be in the form of alerts for attempted (or successful) exploitation against supported network services. While there are a large number of possibly malicious contacts on supported network services, only a minority are followed up for attempted exploitation.[30] Of this minority, a portion (although possibly a large portion) may be detected by network defenses (gateways, firewalls, or network intrusion detection systems). The

difficulty with using alerts from network defenses as indicators of cyberwar-related attacks is two-fold: First, the inherent dynamism of Internet activity, which will be discussed further in a later section. Second, these network defenses often work based on signatures, which are established recognition sequences for known activity. If the activity is not known (either because it is individual or very new), then no signature will be available, and no alert will flag it as possibly malicious. These difficulties suggest that alerts be looked at in aggregate as indicators of shifts in behavior, rather than individually.

OTHER ATTACK PHASES

Attack execution involves the continuation and adaption of malicious activities originating in attack initiation. As such, the indicators for the execution phase will derive from the indicators of attack initiation. Any shifts on the part of the malicious actors will precede the execution of the attack as, during execution, cyberwar will have commenced.

Attack termination is the transition away from attack activities. In network activity, indicators for this transition are often in the form of a lack of observed behavior or, at least, a decrease in the frequency of such behavior. Rarely, a malicious actor will formally state a termination of attack, but such announcements should not be expected (and possibly not believed). In some cases, other malicious actors will adopt the behaviors of the erstwhile attackers, making an assessment of this termination even more difficult. Attacks may also be organized in waves or cycles, so apparent termination may only be temporary.

Limitations of Shifts as a Basis for Analysis.

There are several well-known limitations in network data serving as indicators of shifts for assessment of malicious actors. This section briefly summarizes these limitations as a cautionary note related to the application of the interpretation discussed in this chapter. The section concludes with some methods of dealing with these limitations.

Network data relating to attacks, whether cybercrime or cyberwar, are inherently partial. The partial nature derives from motivation on the part of both the attacker and the defender. The attacker desires that the data be partial so that the efforts of the defender will be incomplete or misdirected, leaving opportunities for further attack. The defender desires that the data be partial for more complex reasons. Defenders may have concerns related to the potential volume of data, which may impact both network bandwidth available for mission-related usage and the workload of the defenders themselves. Defenders may be concerned that more complete monitoring might be exploitable by the attacker to further refine and guide their attacks. Defenders may also lack the authority to install sufficient instrumentation for more complete collection, perhaps due to privacy rights on the part of parties using the network.

Even the data that is collected may be difficult to convert to indicators since the underlying applications of the network, and the user population may be very dynamic. Currently, computer networks are undergoing rapid changes in behavior with the adoption of outsourcing or cloud computing environments. These changes place mission-critical or mission-relevant activity outside the organization network,

concurrent with the rise of "bring your own device" policies, which transfers mission-relevant activity to computing environments owned by the organization's employees as private individuals, rather than as corporate assets. Coupled together, these changes are modifying the long-established client-server view of network behavior into something much less homogenous and much more difficult to directly assess. In the time of such dynamism, it is challenging to find even relatively constant indicators for malicious behavior that can trend to reveal shifts in that behavior.

The classic contrast of correlation versus causation also limits the interpretation of network behavior. So much is changing that even changes that are closely related in time and magnitude may not support causative relations. Correlated activities are much more common, to the point where analysts need to provide clear arguments for why the assumption of mere correlation must be rejected so that causation may be considered.

CONCLUSIONS

To deal with these limitations, multiple strategies need to be applied. First, analysts should exercise caution in the kinds of conclusions that they make attributing shifts in the malicious actors. While certainty (sometimes referred to as "ground truth") is rarely an achievable standard when analyzing network behavior, analysts need to assure that their conclusions are both derived from data and defensible in their assumptions. Second, analysts should consider courses of action to deal with trends that initially point toward one conclusion but rapidly swing away from that conclusion in later observations. Such swings might occur

when the observations were not driven by the types of shifts that the analysts assumed, but also when the malicious actors become aware of action by the defenders (or awareness on the defenders part) and change their tactics or strategies accordingly. Analysts may need to revisit the chain of logic that led to their initial assessments and consider alternatives that are made viable by such swings, or perhaps act preemptively and state their conclusions with alternatives that may be indicated by anticipated swings.

While these limitations make the task of the analyst more complex, that task is not intractable. Practicing analysts look at network behavior and produce actionable indicators on a frequent basis. Some of these indicators have later proven to point to transitions toward increasing depth and scope of hostilities. It is expected that as the methods and practice of cyberwar become more commonplace, the need for assessments of this sort will become increasingly urgent.

ENDNOTES - CHAPTER 17

1. John Howard and Thomas Longstaff, "A Common Language for Computer Security Incidents," Technical Report SAND98-8667, Washington, DC: Sandia National Laboratories, October 1998.

2. Gunter Ollmann, "Cyber Protesting Innovation," presentation at the Computer Security Institute (CSI) 2009 annual conference, National Harbor, MD, October 28, 2009, available from *damballa.com/downloads/r_pubs/CSI2009_CyberProtesting.pdf*.

3. Kamal Jabbour, "Cyber Vision and Cyber Force Development," *Strategic Studies Quarterly*, Spring 2010, pp. 63-73.

4. Howard and Longstaff.

5. American National Standards Institute (ANSI) and Internet Security Alliance, *The Financial Management of Cyber Risk*, 2010, available from *webstore.ansi.org/cybersecurity.aspx*.

6. Gabriella Coleman, "Anonymous in Context: The Politics and Power behind the Mask," Internet Governance Paper No. 3, Waterloo, Ontario, Canada: Center for Internet Governance Innovation, September 2013, available from *cigionline.org/sites /default/files/no3_8.pdf*.

7. U.S. Cyber Consequences Unit, "Overview by the US-CCU of the Cyber Campaign Against Georgia in August of 2008," August 2009, available from *registan.net/wp-content/uploads/2009/08/US-CCU-Georgia-Cyber-Campaign-Overview.pdf*.

8. Paulo Shakarian, "The 2008 Russian Cyber Campaign against Georgia," *Military Review*, November/December 2011, pp. 63-68, available from *academia.edu/1110559/The_2008_Russian_Cyber_Campaign_Against_Georgia*.

9. Ulrik Franke, *Warfare by Non-Military Means: Understanding Russian Information Warfare*, Report FOI-R--4065--SE, Stockholm, Sweden: Swedish Defense Information Agency (FOI), March 2015, available from *foi.se/Global/Press%20och%20nyheter/War%20by%20non-military%20means.pdf*.

10. Technopaedia, "Cyberwarfare," available from *techopedia.com/definition/13600/cyberwarfare*.

11. Jann K. Kleffner and Heather A. Harrison Dinnis, "Keeping the Cyber Peace: International Law Aspects of Cyber Activities in Peace Operations," *International Law Studies*, Report FOI-R--4065--SE, Newport, RI: U.S. Naval War College, Vol. 89, 2013, pp. 512-535, available from *usnwc.edu/getattachment/992607f1-9dbd-4762-b93c-079809f3b9d6/Keeping-the-Cyber-Peace--International-Legal-Aspec.aspx*.

12. Cynthia Grabo, *Anticipating Surprise: Analysis for Strategic Warning*, Washington, DC: Joint Military Intelligence College, December 2002.

13. Eric M. Hutchins, Michael J. Coppert, and M. A. Rohan, "Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains," 6th Annual International Conference on Information Warfare and Security, Washington, DC, 2011, available from *lockheedmartin.com /content/dam/lockheed/data/corporate/documents/LM-White-Paper-Intel-Driven-Defense.pdf*.

14. Shakarian.

15. Hutchins, Coppert, and Rohan.

16. R. Droms, "Dynamic Host Configuration Protocol," Internet Engineering Task Force, Request for Comments 2131, March 1997, available from *ietf.org/rfc/rfc2131.txt*.

17. Andrew W. Moore and Konstantina Papagiannaki, "Toward the Accurate Identification of Network Applications," PAM'05 Proceedings of the 6th International Conference on Passive and Active Network Measurement, Berlin, Germany: Sprinter-Verlag, 2005, pp. 41-54; and Muthuprasanna Alicherry and V. Kumar, "High speed pattern matching for network IPS/IDS," Proceedings of the 2006 Institute of Electrical and Electronics Engineers (IEEE) International Conference on Network Protocols (ICNP'06), Washington, DC: IEEE Computer Society, 2006, pp. 187-196.

18. Tim Jordan and Paul Taylor, "A sociology of hackers," *The Sociological Review*, Vol. 46, No. 4, November 1998, pp. 757-780, available from *yorku.ca/kitzmann/hackers.pdf*.

19. Coleman.

20. U.S. Cyber Consequences Unit.

21. iSight Partners, available from *isightpartners.com/*.

22. Mandiant Corporation, available from *mandiant.com/*.

23. Renesys Corporation, available from *b2b.renesys.com/about /index.shtml*.

24. Software Engineering Institute, CERT program, available from *cert.org/*.

25. "2014 Internet Security Threat Report, Volume 19," Mountain View, CA: Symantec Corporation, available from *symantec.com/security_response/*.

26. Jordan and Taylor.

27. J. Janies, M. Collins, T. Shimeall, S. Faber, R. Weaver, M. DeShon, and J. Kadane, "Using Uncleanliness to Predict Future Botnet Addresses," IMC '07: Proceedings of the 7th ACM SIGCOMM Conference of Internet Measurements, San Diego, CA, October 2, 2007.

28. D. McCoy, A. Pitsillidis, G. Jordan, N. Weaver, C. Kreibich, B. Krebs, G. Voelker, S. Savage, and K. Levchenko, "PharmaLeaks: Understanding the Business of Online Pharmaceutical Affiliate Programs," Proceedings of the 21st USENIX Security Symposium, Bellevue, WA, August 8-10, 2012, available from *usenix.org/conference/usenixsecurity12/technical-sessions/presentation/mccoy*.

29. Rick Hofstede, Pavel Čeleda, Brian Trammell, Idilio Drago, Ramin Sadre, Anna Sperotto, and Aiko Pras, "Flow Monitoring Explained: From Packet Capture to Data Analysis With NetFlow and IPFIX," *IEEE Communication Surveys and Tutorials*, Vol. 16, No. 4, Fourth Quarter 2014, pp. 2037-2063.

30. L. Andersson, E. Davies, and L. Zhang, "Report from the IAB workshop on Unwanted Traffic, March 9-10, 2006," RFC 4948, Internet Engineering Task Force, available from *rfc-editor.org/rfc/rfc4948.txt*.

CHAPTER 18

CRISIS MANAGEMENT IN CYBERSPACE AND IN A "CYBERED" WORLD

Phil Williams

INTRODUCTION

A little over a century after the mismanaged and catastrophic crisis that began in Sarajevo, Bosnia-Herzegovina, and ended with the outbreak of World War I, it is important once again to think about the prospects for crisis management. Attention to crisis management is all the more necessary and urgent, as, during the last several decades, it has been treated as largely irrelevant to the challenges of national and international security. Indeed, in the post-Cold War world, the very notion of crisis management seemed to fall into abeyance and disrepair. Without the prospect of a great power confrontation, crisis management appeared to be little more than a Cold War anachronism with little relevance to contemporary or future events. In recent years, however, this has changed, with several events and developments compelling more serious thinking about crisis management.

The first has been the recognition that, while transnational threats, such as terrorism and organized crime, have increased in salience and importance, geopolitical rivalry has not gone away. The most obvious example is the crisis over Ukraine, a crisis in which European Union efforts to draw Ukraine into the Western camp, at least economically, were trumped by Russia's use of military force to annex Crimea and its subsequent support for the rebels in eastern Ukraine. Notions that Europe had become an extended zone of

peace had been dented during the 1990s by the ethnic conflicts in the Balkans; they were destroyed by the actions of Vladimir Putin. Indeed, Putin's actions were a brutal but important reminder that geographic security concerns were as important for Russia as they had ever been; that military power remained an important and often decisive instrument of national security; and that power politics was not some 19th-century anachronism but an important feature of the 21st-century world—even in Europe. Although the U.S. response focused on economic sanctions and nonlethal aid, the Russian-American relationship increasingly was characterized by discord and suspicion rather than the kind of cooperation and trust envisaged at the end of the Cold War.

A second driver has been growing concern about the changing power structure in the global system resulting from the rise of China and the relative, and some would even argue absolute, decline in the power of the United States. Avery Goldstein added an important twist to this debate, noting that concern with the prospects of a long-term rivalry between the United States and China has obscured the possibility of a near-term crisis with associated instabilities between two nuclear-armed adversaries.[1] As he observed:

> In contrast with the diminished prospect for a showdown over Taiwan, the possibility that the United States and China could find themselves in a crisis triggered by sovereignty disputes in the South China Sea or the East China Sea has increased. Since 2005, a period of relatively low tension over claims to maritime territories and seas in East Asia has given way to growing concern about the willingness and ability of China and its neighbors to settle their differences peacefully.[2]

A third factor—and one that gives added weight to the first two developments—is is that revelations about the Cuban Missile Crisis have suggested that, even during the Cold War, crisis management was far from perfect and depended to a large degree on what Dean Acheson termed "plain dumb luck."[3] The Cuban Missile Crisis, which although highly dangerous, appeared at the time to be very skillfully managed, but actually came very close to catastrophic escalation. U.S. decision-makers were aware neither of the extent to which short-range nuclear weapons were integrated into the Soviet force structure nor of the fact that Soviet military forces in Cuba had been pre-delegated with the authority to use them. Nor were they aware that the Soviet submarines being compelled to surface by U.S. destroyers, each carried a nuclear torpedo, or "special weapon" as it was termed.[4] In the event, one of the submarine commanders, believing he was under attack, came very close to launching the torpedo, and it was only the veto of the flotilla commander, Vasili Arkhipov, that prevented an action that would have crossed the brink into nuclear war.[5] What makes this particularly salutary is that the Cuban missile crisis was relatively simple and straightforward, and took place in a world where there were clearly demarcated spheres of influence and mutual if tacit—although in retrospect incomplete—agreement on codes of conduct.

A fourth factor is that 2014 marked the 100th anniversary of the outbreak of World War I and inevitably was marked by a rash of new analyses trying to explain how a Balkan crisis rapidly escalated into a major European and ultimately a world war. Invariably, there were many echoes of the earlier debate along with a few new revelations and interpretations.

A significant portion of the earlier debate had focused on the issue of German culpability. In a very famous study, Fritz Fischer noted that Germany had deliberately gone to war in 1914 because of its aspirations for European hegemony.[6] A more benign assessment that replaced ambition with insecurity suggested that it was concerns about growing Russian military power that forced Germany to resort to a preventive war in the summer of 1914. Among the more recent studies, this theme was echoed by David Fromkin, with his conclusion that "Germany deliberately started a European war to keep from being overtaken by Russia."[7] In the final analysis, however, for both Fisher and Fromkin, the crisis precipitated by the assassination of the Archduke Franz Ferdinand in Sarajevo was an opportunity for Germany, an opportunity that was grasped decisively, if not eagerly, and that left little room for the peaceful resolution of the crisis. For others, though, the events highlighted the more general failure of great power crisis management to stop events in Sarajevo from escalating into a major conflagration: offensive military strategies and doctrines, the demands of railway timetables during military mobilization, the rigidity of German war planning, and the failures of civilian leaders to understand the implications of military plans and their strategic implementation, combined to take the crisis out of control and on an inexorable course toward war. Indeed, the cumulative effect of such factors was underlined in one widely acclaimed recent study, suggesting that:

> . . . the complexity of the 1914 crisis arose not from the diffusion of powers and responsibilities across a single politico-financial framework, but from rapid-fire interactions among heavily armed autonomous power-centers confronting different and swiftly changing

threats and operating under conditions of high risk and low trust and transparency.[8]

Whether war resulted from a toxic mix of German ambition and insecurity or a more general loss of control and a failure of crisis management, the anniversary was a reminder that stability cannot be taken for granted, that periods of peace can be far more fragile than they appear, and that order and stability can end abruptly. The 100th anniversary of the outbreak of the "Great War" was a salutary reminder, therefore, that in international politics peace and stability cannot simply be taken for granted. This was a reminder that resonated all the more because of the Ukraine crisis and a new Chinese assertiveness over disputed islands in the Pacific.

If it is essential to think once again about the need for—and demands of—crisis management in the 21st century, it is also important to keep in mind the new environment in which crises might occur. In this connection, there is an important distinction between crises that begin in cyberspace with a major cyberattack and those that are precipitated by events in the real world but are played out in a world in which cyberspace is an additional and important strategic domain. This domain offers new strategic options but also creates a new set of vulnerabilities, poses a new set of challenges, and adds a variety of potential complications. Drawing on the analysis of Chris Demchak about "cybered conflict," the argument here suggests that as well as having to manage crises in cyberspace, policymakers will also have to confront and manage cybered crises.[9] These can be understood as geopolitical confrontations between states that start outside cyberspace, but invariably have to be managed within

a context that includes cyberspace and a high level of strategic dependence by the participants on cyber systems for civilian and military activities.

Indeed, in both cyber crises and cybered crises, there is the possibility of cross-domain escalation, from cyberspace to the real world and from the real world to cyberspace. Against this background, this analysis initially examines the notions of crisis and crisis management. It then looks at some of the ways in which crises might occur in cyberspace and the accompanying pressures and requirements for crisis management. This is followed by a brief analysis of the way in which the management of real world crises might also be complicated by the fact that these crises are occurring in a cybered world.[10] The final section of the chapter identifies several ways in which the capacity for crisis management both in cyberspace and in a cybered environment might be enhanced.

CRISIS AND CRISIS MANAGEMENT

During the Cold War with its backdrop of nuclear weapons, the concept of crisis and the nature of crisis management were fully and explicitly articulated. Coral Bell illuminated the notion of crisis with her argument:

> the essence of true crisis in any given relationship is that the conflicts within it rise to a level which threatens to transform the nature of the relationship. . . . The concept is of normal strain rising to the level of breaking strain.[11]

This was usefully broad and could be applied to relationships among allies and those between adversaries. It is the latter that are of most interest here, of course,

and in this context, the following definition provides a useful starting point:

> An international crisis is a confrontation between two or more states usually occupying a short time period, in which important interests are at stake, and in which the possibility of an outbreak of war between the participants is perceived to increase significantly.[12]

This definition highlights the dual requirements of crisis management: It is necessary to take steps to protect national interests and—where war is perceived as highly undesirable—combine these with efforts to maintain the peace. As Glenn Snyder and Paul Diesing noted, in Cold War crises the dual approach was a mixed strategy of coercion and accommodation, but it was necessary to "coerce prudently" and "accommodate cheaply."[13] This clearly articulated the notion that in the nuclear age, it was necessary to protect interests but to do so while avoiding or containing escalation dynamics that could cross the threshold between coercion and violence. Once that threshold was crossed, it was not clear where the stopping points would be or even if there would be any.

Other scholars observed that crises typically were defined in terms of an increase in threat to interests, often accompanied by an element of surprise and a short time in which to respond. These characteristics meant that decisions were taken with a sense of urgency and under conditions of enormous uncertainty about the reaction of the adversary or the ability to maintain control over events. Consequently, policymakers were subject to considerable stress, and, although this could enhance capacity for sound and sensible decision-making in the short term if the stress were both high and sustained, it was likely to have a

debilitating effect on decision-making. This was not the only danger that decision-makers had to confront in crises. Crises invariably required strong action, and there was always a possibility that the actions taken would not be fully thought through and would intensify rather than moderate the crisis. Closely linked to this was the distinct possibility of miscalculation, of misunderstanding the adversary's resolve, and provoking rather than coercing. Another danger was that decision-makers would lose control over events and that the crisis would take on its own dynamic—rather as the Sarajevo crisis did. Where allies were also involved, they were potential wild cards, capable of disrupting carefully crafted strategic moves put into place by the major protagonists.

The dangers were very real and meant that confidence in crisis management was limited rather than unbounded. Indeed, some critics decried the notion, arguing that those who lived by crisis management were destined to die by crisis management.[14] This was a fatalistic and facile critique: The difficulty was, and is, that in the event of a crisis, there was really, and is, no alternative to prudent crisis management. For all its limits and shortcomings, crisis management was better than an unmanaged or mismanaged crisis. The same is true today—although as Herbert Lin has compellingly argued, managing the issues that have long been a challenge for crisis management "may well be more difficult for cyber conflict than for other kinds of conflict."[15] If crisis management was problematic during the Cold War, it is likely to be even more problematic during a cybercrisis or during a great power crisis that takes place in a cybered world.

CRISIS MANAGEMENT AND CYBERSPACE: THE CHALLENGES

As suggested earlier, crisis management has never been easy. There are several characteristics of a crisis in cyberspace, however, that could pose enormous difficulties. Some of these are a direct result of the distinctive environment of cyberspace. As Deighton Fiddner pointed out in an earlier chapter in this volume, cyberspace is both a domain in its own right and something that subsumes the other domains. It has also been characterized as a "fierce domain," a description that is particularly apt, given the ways in which cyberspace has become an extension of political competition among states. It has become a fertile ground for the activities of traditional and virtual criminal organizations, and a venue in which terrorists recruit, raise money, communicate with one another, amplify their attraction to vulnerable populations, and acquire information about potential targets.[16] Against this background, one of the problems when thinking about the outbreak of a crisis in cyberspace is that the noise level is already very high. Cyberattacks on the United States occur with remarkable frequency on a daily basis. Some involve simple hackers testing out their skills, but others are more malevolent and are linked to cybercrime or cyberespionage. Yet, others might be probing attacks by nation-states that are seeking to identify potential weak points that can be exploited or simply testing U.S. defenses and likely responses. Whatever the motive, as Herbert Lin points out, the "constant background of cyber-attack activity" has created a new baseline of competitive, hostile and even provocative activity, with probing, testing defenses and limited attacks the order of the day.[17]

Because they are in cyberspace, these attacks have had limited impact in terms of damage and have not been unequivocally strategic in nature. In fact, many attacks seem to have been motivated by criminality or espionage. Consequently, there has been a high level of tolerance and, in spite of a great deal of U.S. rhetoric about the cyberthreat being the most significant of all the current threats to the United States, none of the attacks has been sufficient to provoke a confrontation between the United States and either China or Russia.

In this connection, it is worth considering what a major cyberattack would look like. Even thinking in these terms, however, there is likely to be a significant gradation of seriousness and severity. Nevertheless, a major attack would likely stand out against this background of routine and frequent attacks. Such an attack is likely to be distinguished by some or all of the following characteristics: (1) wide scope with an extended target set that goes beyond specific institutions such as banks or particular corporations; (2) efforts to create considerable disruption to the functioning of the economy and society of the target state largely through targeting critical infrastructures; (3) possibly significant impact in terms of the availability of critical services such as power and communications; (4) possible loss of life as result of the physical consequences of a cyberattack; (5) a possibly extended period in which the target state has to cope without fully functioning critical infrastructure. In short, a major attack has far-reaching consequences in terms of the damage to critical infrastructure.

The difficulty at this point becomes one of attribution. In October 2012, then Secretary of Defense Leon Panetta claimed that the Department of Defense had made "significant advances identifying the origins of

an attack. . . . Potential aggressors should be aware that the United States has the capacity to locate them and hold them accountable."[18] The attack on Sony that was traced back to North Korea suggests that such claims have some credence.[19] Nevertheless, the possibility of denial and deception coupled with the high level of noise suggests that unequivocal identification of the perpetrators of a major attack might remain problematic. Indeed, even when certain locations, entities, and attack vectors are identified, it is still not clear if they are perpetrators or simply innocent victims who are being set up to take the fall. In cyberspace, as Joseph Nye has pointed out, "ambiguity is ubiquitous and reinforces the normal fog of war."[20] Even major cyberattacks, therefore, might be characterized by a lack of clarity and by enormous uncertainties about their origins, let alone the purpose or intent of the perpetrators.

The real challenge in such cases is to determine responsibility and to identify and then track down the perpetrator. One issue that often arises in murder investigations is the possibility that the suspect has an alibi. Whether this is genuine or is a bogus claim, it provides a degree of plausible deniability. The same issue arises in cyberspace where plausible deniability can make it extremely difficult unequivocally to assign responsibility for a cyberattack, let alone cyberwar initiation. As one expert noted:

> we have entered an age where anyone can participate in a cyber conflict from any point on earth, masking their location and their identity, yet causing serious disruption. Attacks can also be 'crowd sourced' by governments—as some suspect might have been the case in Estonia and Georgia—or arise from acts of spontaneous participation, or both.[21]

This complicates the task of assigning blame to a rival state and forming an appropriate response.

The danger is that plausible deniability increases the likelihood of risk taking. The issue for the responder, however, is the extent to which the shield of plausible deniability can be breached. There is both an issue of feasibility here and one of desirability. The issue of feasibility concerns the nature of the evidence that could expose the denials for what they are. The Soviet Union's first reaction to allegations that it had placed missiles in Cuba in 1962 was one of denial; the denials were rendered implausible by photographic evidence that was unveiled to the world at the United Nations. It seems unlikely there would be an equivalent public disclosure in cyberspace. At the very least, it would be far less dramatic and direct. In the event that there is sufficient and compelling evidence, however, and that the attacked state has a high level of confidence in this evidence, then some retaliatory action would be inevitable. In other words, attribution would almost certainly precipitate a major crisis in cyberspace. In that sense, better attribution increases the risk of crisis, unless a potential perpetrator is also aware of the possibility, in which case willingness to take risks and initiate a major cyberattack might be limited. The danger here is that the expectations of rival states might be asymmetric, leading in a sense to a miscalculation about the ability to initiate a cyberattack anonymously and without eliciting serious retaliation.

Another major problem is that cyberspace is lacking some characteristics that have facilitated crisis management in the past. One important example of this is thresholds between different levels of intensity of the crisis. As Forrest Morgan and his coauthors have compellingly argued, "The key to managing risks of

inadvertent escalation lies in clarifying thresholds—on all sides of a conflict."[22] Yet this is likely to be far more difficult in a cybercrisis than it was during Cold War crises. In the real world, there are obvious thresholds such as that between coercive or threatening actions and overt violence, the geographical stopping points that have what Thomas Schelling described as a high degree of salience and are generally easy to understand, or the distinction between the use of conventional and nuclear weapons.[23] In cyberspace, however, thresholds are harder to define and recognize, let alone mutually acknowledge, agree upon, and respect. In some ways, the very ubiquity and complexity of cyberspace make thresholds a much more problematic, if not wholly irrelevant concept.

Linked to this is also a potential repeat of a calculation that played a key part in the 1914 crisis—that states could have their wars and enjoy them. This was obviously not the view of all the policymakers, with the civilian leaders generally exhibiting greater qualms about going to war than their military counterparts. Indeed, it is clear some of the policymakers involved in the 1914 crisis were horrified at the likely costs of a war. British Foreign Secretary Sir Edward Grey is an obvious example. Yet, the more pervasive and immediate concern for most of the decision-makers was of losing a war—a concern that drowned out caution and fed the mobilization race. There is a similar danger that policymakers in one or more countries somehow come to regard cyberwar as a bloodless alternative to war in the real world and take actions that have such damaging consequences on an adversary that retaliation—so long as the capability remains intact—has to be at least equally damaging. Indeed, in the aftermath of a major cyberattack on the United States, concerns

over credibility would likely crowd out prudence and drive major efforts at retaliation. In an odd way, policymakers might be even less willing to lose face in cyberspace than in the real world because actions to regain face do not appear as dangerous as they would in the real world.

It is clear even from this very cursory survey of how cyber crises might differ from traditional crises—especially those that occurred during the Cold War—that they could prove potentially unmanageable. Different, but potentially closely connected problems arise in several key areas: decision-making, communications, crisis-bargaining, making sound intelligence assessments, and maintaining control over events.

Decision-making in crises has always involved high levels of uncertainty. Coupled with time-pressures and the stress that this can induce, there has always been a possibility that policymakers would close off certain options prematurely, would take high-risk actions because of concerns over credibility, or would insufficiently think through the implications of a favored option, and in particular, how it might appear to the adversary. These dangers would certainly exist in a crisis in cyberspace. So too would the possibilities of group think and even wishful thinking, leading the decision-makers to take risks that a more deliberative and adversarial process might have both highlighted and avoided.

Such difficulties in the decision-making process in the United States are likely to be exacerbated by the dominant approach to cyberwar, which treats it as predominantly a technical issue rather than a political and strategic challenge of the first order. This has two implications. First, there is likely to be a large gap of understanding between the technocrats, who are very

likely to be predominantly military officers, and civilian decision-makers. Civil-military relations are invariably tested during crises and a crisis in cyberspace is unlikely to be an exception to this. Second, and perhaps even more fundamental, the U.S. President will most likely find himself out of his depth, faced with limited and poorly understood policy options, in which the gap between intention and result could be large. In some respects, this is akin to the situation in 1914 when foreign ministers did not fully realize the ways in which military plans and preparations would foreclose diplomatic options.

When consideration turns from decision-making to communications between the governments, there might also be unexpected difficulties. There often seems to be an implicit assumption that in a world of rapid and immediate communication through multiple electronic channels, communications among adversaries in a crisis would be easy and straightforward. Such communications certainly hold out the promise of overcoming one of the major problems that surfaced in the Cuban Missile Crisis: Formal communications channels were slow and difficult, and even additional improvised and informal channels sometimes added to ambiguity and increased rather than reduced uncertainty. Yet, it is not clear that rapid and instantaneous communications would facilitate careful and considered decision-making. The pressure to act or respond quickly could prove detrimental to the development and consideration of multiple options and the careful choice of a sensible course of action. Ironically, the ease of communications in a cybercrisis could also vary significantly during the course of the crisis. Depending on the scope and nature of the initial attacks or retaliatory measures, the possibility

of communication disruptions is also very real. While the participants in a great power crisis in cyberspace would have a vested interest in maintaining open communications channels, it is possible that these could be inadvertently (or perhaps under certain circumstances even deliberately) disrupted. At the very least, it is dangerous to assume the communications process would invariably be smooth and easy. Moreover, closely related to problems in communications are the dangers in the bargaining process.

In this connection, it bears emphasis that, even if communications work in an electronic sense, they might not always be understood or accepted. Part of the problem during crises is that actions often speak louder than words and are themselves a crucial part of the communication process. Yet, these actions may be interpreted very differently from the way they were intended. Indeed, there is always the danger of miscalculation in crisis bargaining. This problem is likely to be accentuated in cyberspace not only because of the inherent uncertainties but also because of the potential for unintended consequences. The competitive bargaining process and brinkmanship in a crisis carry risks that might not be fully understood by decision-makers on either side. To go back to the Snyder formulation, efforts to coerce prudently might be less prudent than those engaging in coercive actions realize. One of the dangers is that decision-makers might not fully understand the nature and impact of their own offensive options. It is possible, for example, that, one of the participants seeks to send a message with a limited cyberattack that, for one reason or another, has far more extensive and damaging effects on the adversary than anticipated. Depending on when this occurs, it could be the attack that provokes the crisis in

the first place or the one that leads to escalation. Bargaining is likely to be far more difficult and dangerous where the stakes are unclear, options are not nearly as carefully delineated as policymakers think, and intelligence is highly problematic.

Many of the problems confronting intelligence in a crisis in cyberspace are likely to involve the intentions and capabilities, the ambitions and fears of an adversary. Problems could also arise, however, in efforts to assess the damage that an adversary has inflicted on one's own critical infrastructure. Indeed, the degradation of infrastructure could itself make damage assessment highly problematic, extremely limited, or even impossible. It is a distinct possibility that the tools for making the assessment of damage have been degraded or destroyed by the same attack that inflicted the damage in the first place. Indeed, it is possible that damage assessments will be all but impossible. In effect, intelligence that is crucial in determining the next step in the crisis might simply be unavailable. It is perhaps the great irony that in a crisis where intelligence assessments are massively important for decision-making, those assessments might be particularly limited and of low or uncertain quality. Closely linked to this, it is difficult to know how many attacks and counterattacks might occur and how these iterations would evolve.

In this connection, Herbert Lin has identified another distinct and very real possibility in which probes for better information are wrongly interpreted as a continuation of the conflict. As he argued:

> knowing what the adversary is doing and the scope and nature of its future intentions are very important to decision makers, and the need to collect such intel-

> ligence will almost certainly result in greater pressures to use the entire array of available intelligence-gathering techniques—including techniques of cyber exploitation. If the adversary is unable to distinguish between an offensive operation for exploitation and one for attack—an outcome that seems all too likely—a cyber exploitation may run the risk of being perceived as part of an imminent attack, even if this is not the intent of decision makers.[24]

In other words, a crisis in cyberspace could generate an intense variant of the security dilemma in which a simple quest for clarification is interpreted as something much more malevolent and threatening.

In turn, these intelligence problems feed into the difficulties of maintaining control over events. In thinking about this, Forrest Morgan's useful and important distinctions between deliberate, inadvertent, and accidental escalation are particularly pertinent. As he notes, however, these forms of escalation have very different dynamics. Yet, they could also interact in important and damaging ways. A very real danger in cyberspace, for example, is that inadvertent escalation would be regarded as deliberate, thereby provoking an escalatory response rather than a reversal of the spiral. In this sense, there is a very real possibility of escalation based not on strategic intent, but on a series of misunderstandings of what the enemy is doing and why. The assumption in a crisis that the adversary is acting in a very deliberate and calculated matter is sometimes the prudent course. Yet, in other cases, the assumption of centralized management and perfect control and coordination will be totally wrong—with potentially very dangerous consequences.

It is at this point that the bargaining process and the issue of control over events could intersect with

the possibility of catalytic escalation. Indeed, the difficulty of identifying an attacker creates enormous potential for mischief. As Herbert Lin once again has pointed out:

> catalytic escalation occurs when some third party succeeds in provoking two parties to engage in conflict. For example, Party C takes action against Party A that is not traced to Party C and appears to come from Party B. Party A reacts against Party B, which then believes it is the target of an unprovoked action by Party A. The inherent anonymity of cyber operations may make 'false-flag' operations easier to undertake in cyberspace than with kinetic operations.[25]

Yet, this danger is likely to be far greater when a cybercrisis is already underway. It is conceivable, for example, that as great powers seek to contain and manage a crisis in cyberspace by reaching a cyber-cease-fire or cessation of hostilities, a third party by taking independent actions could completely undermine opportunities to defuse to the crisis. Indeed, actions by a third party could be even more provocative, destabilizing, and escalatory after a crisis has started than before. At this stage, sensitivities are inflamed, political pressures are likely to be high, and trust between the governments involved is already damaged and highly tenuous. In such circumstances, a third party action could have a major impact in undermining the prospects for successful crisis management and reigniting an escalatory spiral.

Moreover, there are several possible perpetrators of this kind of ploy. It could be a third power that sees itself as likely to benefit from some kind of confrontation or even hostilities between the two major states involved. It is also possible that it could be a nonstate

actor such as a terrorist organization that sees an opportunity to weaken one or both of its major enemies. A third possibility, and one emphasized by Lin, is that action could be taken by "patriotic actors" in one of the states involved without the tacit approval, let alone the authorization of the political leaders in that state:[26]

> The actions of these patriotic hackers may greatly complicate escalation management. Such actions may be seen by an adversary as being performed under the direction, blessing, tacit concurrence, or tolerance of the state and therefore are likely to be factored into the adversary's assessment of the state's motives and intent. The state's efforts to suppress patriotic hackers may be seen as insincere and are likely to be at least partially unsuccessful as well.[27]

Once again, such actions easily could be seen as a deliberate provocation by the adversary. In the aftermath of some kind of truce or suspension of activities, they would be seen as a total breach of faith and trust. In these circumstances, the consequences could be severe, provoking another round of attacks and dispelling what little trust had been established. In these circumstances, the danger is that denying responsibility would be seen as proof of perfidy, rather than as a genuine disclaimer. Indeed, for those actors intent on provoking escalation, cyberattacks on both the major powers involved—or what Lin termed "a double-sided catalytic attack"— could have profound escalatory consequences.[28]

In other words, we are in an era when a great power confrontation would involve unprecedented uncertainties and imponderables. Another major imponderable and potential complication is that the interplay

between cyberspace and real word military preparations is untested and, therefore, barely understood. What are the prospects for cross-domain escalation? This is an area for which there are few if any, precedents or guides to behavior, and where the prospects for successful management depend on the impact of a series of unknown unknowns. If a cyberattack had a major impact in weakening or disrupting military preparations, it would create use-them-or-lose-them dilemmas, adding new and unpredictable dimensions to notions of preemptive instabilities. During the Cold War, the key assumption was that a strategic nuclear attack could be deterred if the adversary knew that the target state had the capacity to retaliate after absorbing such an attack. But what if a cyberattack could electronically disrupt the national command authority? Even the very possibility that command, control, communications, and computer (C4) systems could be weakened might once again lead to a renewed emphasis on preemptive strategies and doctrines not because they promised victory, but because the vulnerability of the C4 system would compromise the capacity for strategic nuclear retaliation. In a sense, even the possibility of a cyberattack that might affect the confidence and perceptions that underlay the strategy of mutual assured destruction during the Cold War, today, could be profoundly destabilizing. In the midst of a crisis, it could present policymakers with complex dilemmas and profoundly difficult choices.

TRADITIONAL CRISES IN A "CYBERED" WORLD

Thus far, the emphasis has been on the possibility of escalation from a crisis in cyberspace to the real world.[29] Yet, it is perhaps equally plausible that cross-domain escalation might go in the opposite direction in that a geopolitical crisis would escalate into cyberspace. There are several reasons for this. One is the importance of electronic communications for battle space management at the strategic, tactical, and operational levels. The idea of information dominance—either having it in the case of the United States, or preventing the United States from exercising it in the case of China or Russia—has become central to the modern battle space as conceived in the strategic doctrines and plans of the three great powers. Moreover, for China or Russia, the idea of neutralizing or, at least, eroding U.S. superiority in technology through cyberattacks is very attractive. It fits both the Russian and Chinese conceptions of integrating cyberspace and information operations into national strategy—something both countries appear far more comfortable with than does the United States.

There is also a possibility that, in a geopolitical crisis, policymakers, seeking to respond decisively and coerce the adversary while maintaining control over events, might decide that attacks on the adversary in cyberspace are much less dangerous escalatory options than the traditional use of military force. The problem is that such attacks would almost invariably be on cybertargets that are within the homeland of the adversary. As such, they are likely to blur the salience of the homeland as a sanctuary, subtly but effectively undermining the significance of territorial spaces that

traditionally have been regarded as off limits except for the most high-risk options. To allow something that was regarded as catastrophic in the Cold War to become a significant option in a contemporary crisis is to move into uncharted and very dangerous waters. Indeed, to the extent that the homeland provides a fundamentally important territorial, political, and psychological threshold that has hitherto had a de facto sanctuary status, such a move might be seen as a far more significant and dangerous escalation than, for example, crossing the line between coercion and violence in a military clash at sea or in a remote area. Although such a judgment—and an appropriately serious and perhaps similar response—is not preordained, launching a cyberattack on the territory of a major power in the belief that this is a relatively safe option could prove to be the height of folly and something that "tips" a crisis out of control.

Even if there is sensitivity to such risks, however, there might be preventive or preemptive incentives and concerns for carrying out such an attack. In a geopolitical crisis, policymakers might regard the effectiveness of their military forces as under threat from cyberattacks by the adversary. One way of neutralizing this potential threat might be to degrade the cyber-capabilities of an adversary—something that would likely involve a major, albeit "defensive" cyberattack on the adversary's homeland. Another, of course, is to use the military capabilities before they are subject to degradation as a result of a cyberattack. Either way, the results are likely to involve significant escalation and would certainly make it much more difficult to maintain control over events in the crisis. In other words, it does not matter whether the crisis has its origins in cyberspace or more traditional geopolitical conflict,

very traditional and familiar use-them-or-lose-them dilemmas and dynamics could easily come to the fore once again, with very dangerous consequences. In this sense, cyberspace, potentially, at least, adds an important escalatory dynamic to real-world tensions and conflicts.

CONCLUSION AND RECOMMENDATIONS

The obvious implication of all this, of course, is that crisis management could prove much more problematic in the globalized and cybered world of the 21st century than it did during the Cold War when cyberspace did not even exist. An equally important implication of the preceding analysis is that security and crises in cyberspace are not narrow technical challenges; rather they involve fundamental issues of politics and strategy, great power relations, bargaining, and escalation dynamics and control. The challenge for crisis management in the 21st century is formidable. Governments and scholars alike have to confront the task of conceptualizing not just security and safety of infrastructure, but the nature of security in a world that is simultaneously a nuclear world and a cyberworld. There are several obvious things that could be done to achieve this:

1. Develop scenarios and training exercises that are more comprehensive than those usually carried out, and place the emphasis on the integration of bargaining strategy and communications across separate domains or spaces. Some scenarios should begin in cyberspace; other crisis scenarios could focus more on potential origins in traditional geopolitical rivalries and military clashes. In both cases, however, special attention should be given to notions of domain link-

age and domain escalation—how strong the linkage is, how and why cross-domain escalation might occur, what the impact would be on efforts at crisis management, and how such escalation might be prevented.

2. Bring together technical specialists, military commanders, and civilian decision-makers to consider how crises could be managed across different domains depending on the origin of the crisis, the strategy and tactics of the adversary, and the intense security dilemmas that might arise. There is an important learning element in this, especially for the civilian leadership. It is clear that, in the Sarajevo crisis, many of the key civilian policymakers did not understand the implications of the military options the generals provided. To allow such a situation to arise in a cyber or cybered crisis in the 21st century would be—to quote the title of a book focusing largely on cybercrime—a "fatal system error" in its own right.[30] To believe that policymakers can be prepared for all contingencies would be illusory; but to ensure that policymakers have rehearsed the requirements of crisis management and especially the kinds of choices, dilemmas, and tradeoffs they will confront in either a cyber or a cybered crisis is a categorical imperative.

3. Emphasizing research and development on attack attribution and damage assessment requirements both through cyberspace and through a broader intelligence effort is essential. It is equally important to identify and exploit synergies between what might be termed cyberintelligence and traditional national security intelligence. Timothy Shimeall's pioneering chapter in this volume on distinguishing between cybercrime and cyberwar identifies some important indicators of the transition to cyberwar within cyberspace and has important implications for the cyberin-

telligence component. Yet, it is equally necessary to fuse indicators from within cyberspace with broader indicators that emanate from traditional military warning intelligence and strategic intelligence for a more comprehensive assessment. This fusion is not something that can be done successfully under the duress of crisis. Rather, it is something that has to be planned and implemented under normal conditions. Only then does it stand any chance of working well under crisis conditions and augmenting the capacity for successful crisis management.

4. During the Cold War, the brinkmanship of the Cuban Missile Crisis was followed by a growing emphasis on crisis prevention or crisis avoidance, as well as by mechanisms such as the hotline that could enhance crisis management. Against this background, it would be eminently sensible to consider the development of rules of the road or cyber-rules of engagement that would be in the collective interest of all major states with high levels of investment in critical cyberinfrastructure. While accords such as the U.S.-Soviet Preventing Incidents at Sea Agreement of 1972 are hard to replicate in cyberspace, they do provide some kind of precedent and guidelines for codes of conduct in cyberspace that could contribute to both crisis prevention and escalation control in the event of a crisis. Certainly, such an approach should be on the agenda for U.S. diplomatic initiatives toward both Russia and China. Given the potential complexities and imponderables likely to characterize either a crisis in cyberspace or a great power crisis in a cybered world, anything that can be done to enhance predictability and impose a degree of structured expectations for decision-making could prove invaluable.

5. Take steps to ensure that, even when infrastructure has been significantly degraded, communication between adversaries remains possible. In other words, it is vital to protect and insulate "hotlines" so that these forces are able to operate even after a major attack in cyberspace has occurred and created significant damage to national infrastructure. The case for this is as compelling now as was that for the original hotline to be established in the aftermath of the Cuban Missile Crisis. This is not to ignore the possibility that direct communications can be manipulated, exploited for deception and denial, and used as simply another channel for coercive bargaining. Nevertheless, the advantages of maintaining direct communications that can be used to minimize the prospects for miscalculation and mistakes, or provide important reassurances to dampen escalatory pressures, outweigh the potential downside. A hot line could be particularly important in the event of efforts by third parties to provoke catalytic escalation.

6. Develop contingency plans for military options that can be implemented with minimum dependence on a functioning infrastructure in cyberspace. Although it has not been the primary focus of this analysis, a recurring theme has been the possibility that the United States, or indeed its adversaries for that matter, might be faced with use-them-or-lose-them dilemmas in relation to military forces—not in the sense that the forces would be destroyed, but that they would be rendered inoperable because of the degradation of the information and communications systems on which they depend. The more they can be designed to ensure continued resilience and operational effectiveness even in the absence of these systems, the less acute these dilemmas would be.

7. The administration that comes to power in 2017 should create a national commission in the United States that would examine the relationship between strategy and security as traditionally defined, security as it has evolved in cyberspace, and strategy that integrates cyberspace and traditional space. It should also take a completely new look at organizational arrangements for both cybersecurity and offensive cyberoperations, recognizing that there is no end state in terms of organizational structure for infrastructure security arrangements, but that systems, people, and institutions need to be highly flexible and ultra-adaptive. Blue ribbon panels occasionally proved useful during the Cold War, and a high-level panel coordinating the efforts of a multi-disciplinary network of experts could provide both political impetus for enhanced crisis management capabilities and the analytic and scientific insights to ensure that these can be applied effectively in both crises in cyberspace and cybered crises.

None of these recommendations is a panacea. But unless thinking about the interplay of crisis management and escalation in a world that is both nuclear and cyber becomes more systematic, more comprehensive, and more imaginative, the prospects for managing and containing the security challenges, the cross-domain linkages, and escalation dynamics will be dismal at best.

ENDNOTES - CHAPTER 18

1. Avery Goldstein, "First Things First: The Pressing Danger of Crisis Instability in U.S.-China Relations," *International Security*, Vol. 37, No. 4, Spring 2013, p. 50.

2. *Ibid*., p. 54.

3. See Dean Acheson, "Homage to Plain Dumb Luck," *Esquire*, February 1969, pp. 44–46, 76–77.

4. "U.S. and Soviet Naval Encounters During the Cuban Missile Crisis," in William Burr and Thomas S. Blanton, eds., *National Security Archive Electronic Briefing Book No. 75,* October 31, 2002, available from *nsarchive.gwu.edu/NSAEBB/NSAEBB75/.*

5. Edward Wilson, "Thank you Vasili Arkhipov, the man who stopped nuclear war," *The Guardian*, October 27, 2012.

6. Fritz Fischer, *Germany's Aims in the First World War*, New York: Norton, 1968.

7. David Fromkin, *Europe's Last Summer: Who Started the Great War in 1914?* New York: Vintage, 2004, p. 273 or New York: Knopf Doubleday Publishing Group, 2004, Kindle Ed.

8. Christopher Clark*, The Sleepwalkers: How Europe Went to War in 1914*, Kindle Ed. New York: Harper Collins, 2013, pp. 556-557.

9. This is drawn from Chris Demchak's notion of cybered conflict. See Chris C. Demchak, *Wars of Disruption and Resilience: Cybered Conflict, Power, and National Security*, Athens, GA: University of Georgia Press, 2011. See also her Chapter 19 in this volume.

10. For an early discussion of this notion, see Vincent Manzo, *Deterrence and escalation in cross-domain operations: where do space and cyberspace fit?* Washington, DC: National Defense University, 2011.

11. Coral Bell, *The Conventions of Crisis,* London, UK: Oxford University Press, 1971, p. 9.

12. Oran R. Young, *The Politics of Force: Bargaining during Superpower Crises,* Princeton, NJ: Princeton University Press, 1968, p. 15.

13. Glenn H. Snyder and Paul Diesing, *Conflict among Nations: Bargaining, Decision Making, and System Structure in International Crises,* Princeton, NJ: Princeton University Press, 1977, p. 207.

14. For a useful critique of crisis management, see Ken Booth, *Strategy and Ethnocentrism*, New York: Holmes and Meier, 1979, pp. 59-60.

15. Herbert Lin, "Escalation Dynamics and Conflict Termination in Cyberspace," *Strategic Studies Quarterly*, Fall 2012, p. 57.

16. See Jason Healey, ed., *A Fierce Domain: Conflict in Cyberspace, 1986 to 2012*, Vienna, VA: Cyber Conflict Studies Association and the Atlantic Council, 2013.

17. Lin, p. 57.

18. Leon Panetta, "Remarks by Secretary Panetta on Cybersecurity to the Business Executives for National Security, New York City," October 11, 2012, available from *https://www.lawfareblog.com/secdef-panetta-speech-cybersecurity*.

19. See, for example, Kara Scannell, "FBI details North Korean attack on Sony," *Financial Times*, January 7, 2015, available from *ft.com/cms/s/0/287beee4-96a2-11e4-a83c-00144feabdc0.html#axzz3bYrZhYBv*.

20. Joseph S. Nye, Jr., "Cyber Power," Cambridge, MA: Massachusetts Institute of Technology, p. 5, available from *web.mit.edu/ecir/pdf/nye-cyberpower.pdf*.

21. Ronald Deibert, "Tracking the emerging arms race in cyberspace," *Bulletin of the Atomic Scientists,* Vol. 67, No. 1, January/February 2011, p. 18.

22. Forrest E. Morgan, Karl P. Mueller, Evan S. Medeiros, Kevin L. Pollpeter, and Roger Cliff, *Dangerous Thresholds: Managing Escalation in the 21st Century*, Santa Monica, CA: RAND, 2008, p. xiii.

23. Thomas Schelling, *The Strategy of Conflict*, Cambridge, MA: Harvard University Press, 1960.

24. Lin, p. 67.

25. *Ibid*., p. 53.

26. *Ibid*., p. 60.

27. *Ibid*., p. 61.

28. *Ibid*., p. 59.

29. This section develops certain ideas initially articulated in Phil Williams, "Strategy for Infrastructure Protection and Crisis Management in the Cyber Age: An Elusive Quest?" in Denis Caleta and Paul Shemella, eds., *Counterterrorism Challenges Regarding the Process of Critical Infrastructure Protection,* Ljubljana, Slovenia: Publishing Houses Institute for Cooperative Security Studies, and Monterey, CA: Center for Civil-Military Relations, September 2011.

30. See Joseph Menn, *Fatal System Error*, New York: Perseus, 2010.

CHAPTER 19

CYBERED WAYS OF WARFARE: THE EMERGENT SPECTRUM OF DEMOCRATIZED PREDATION AND THE FUTURE CYBER-WESTPHALIA INTERSTATE TOPOLOGY

Chris C. Demchak

Peace traditionally rests on the forms of governance among states or groups.[1] Governance of any system rests on institutions, but in cyberspace today, there is a vacuum. The institutions in cyberspace currently guide rather than govern, using weak norms, public exhortations, convenience, and nonstate centralized addressing protocols resting on contracts and unenforceable, informal arrangements. The vacuum has encouraged a disequilibrium of the system whose anarchy tends to encourage predatory behavior for resources, especially among strangers with no shared obligations or social controls.[2] When the conflict, be it mass criminality or organized cross-border insolence, rises to what are seen as existentially intolerable or highly disruptive levels, the functional state must react to defend its prerogatives, territory, and societal well-being. In the past, this situation has generally led to war or a close equivalent involving weapons, death, and destruction.

The virtual anarchy of the global web has led not to war as we have known it but to a form of conflict in the interstices between peace and war that involves not only states but also anyone with access, time, and basic equipment. It is no longer the peace and war of Raymond Aron or Ken Waltz with declared oppo-

nents, uniformed militaries, observable incursions, and physically evident military power. Rather, it is more like the continuing, more convoluted systemic struggles seen by Thomas Hobbes, Niccolo Machiavelli, and Sun Tsu,[3] in which nearly everything up to the kinetic exchanges involving death and destruction of traditional war has become fair game among multiple predatory and defending parties. Campaigns may take years to unfold largely cloaked in multilayers of preferably anonymous deception and the slow, deep, systemic enfeeblement of adversaries rather than any identifiable, attributable, direct, physical strikes. This not-quite-peace-but-clearly-not-traditional-war emergent form of struggle, "cybered conflict," changes warfare for the near and longer future as well.[4] Henceforth, whether or not kinetic means are involved, every major conflict among states will involve cyber means that seminally influence the outcome of the conflict.

Cybered conflict today offers to states and nonstate actors alike a broad spectrum of choices for engaging in and benefiting from hostilities without being obvious and crossing known red lines of international law into kinetic exchanges. With the menu of options for seeking leverage, returns, or compliance, it is largely unnecessary to move deliberately across the known red lines of international law into a war which links cyber means and kinetic exchanges among major adversaries known to each other as opponents. The topology of the global cyberspace allows an unprecedented broad swath of the world's populations and states to pick among a wide variety of predatory campaign options with minimal investment of resources, an easily employed long, deceptive and generally anonymous reach, and largely free returns on investments in knowledge acquisition, employment, and

refinement. Since any actor can reposition its efforts at any point along the spectrum at any time due to the opaqueness of the substrate, moving to the unusual conditions of cyberwar with known state-level opponents and linked kinetic-cybered exchanges is less likely as a deliberate campaign element than as a product of accidental escalation.[5] The term is then analytically best placed at the end of the spectrum of cybered conflict where adversaries, through miscalculations, frustration, arrogance, and even naiveté, fail to reposition their efforts to a better advantage back down the spectrum before the outbreak of more overt and systemically harmful expressions of conflict. Thus, cyber "war" is unlikely, but systemic cybered conflict is already here.

The focus of this chapter is to frame systemically how the current globally open, unfettered, ubiquitous, and opaque cyberspace is encouraging conflicts among communities that may harm their future well-being and is changing their interstate system profoundly without a shot being fired. Three arguments will be made: First, cyberspace has spread as a highly insecure, open "substrate" under the world's major communities, with systemic characteristics democratizing anonymous predation globally and overwhelming established state and societal controls. Second, with cybered conflict the result of this virtual anarchy, states, and organized groups are now engaged in a transition era to sort out where the new societal and interstate controls on predatory behavior will be placed and enforced in the slowly emerging future "Cyber-Westphalia" interstate system. Third, the institutions built throughout this transition will strongly influence which states are robust or weak cyberpowers when cyberspace's topology stabilizes.

Three currently emerging models of possible future topologies bear close observation over time to discern how the trends of the global system are moving toward or away from the end of the cybered conflict spectrum to cyberwar itself.

CONFLICT "SUBSTRATE"

When the substrate[6] changes on which societies depend, so do the societies and the way they resolve uncertainties internally and externally. The cyberspace substrate is entirely man-made, man-owned, contracted out, man-maintained, man-updated, man-monitored, man-defended, and man–disrupted. The cyberspace substrate is evolving from its early free-for-all frontier era into an era of conflict during which states will rise or fall as cyberpowers but eventually will collectively construct yet a third Cyber-Westphalian era of states with their own defined jurisdictions in cyberspace.

This evolution is driven by the complexity and opaqueness of the highly insecure technological base of cyberspace encouraging a democratization of predation globally. Cyberspace has not changed human-human predation, but the globally open, unfettered cyberspace substrate has eased three historically daunting systemic obstacles to predatory behavior, namely scale, proximity, and precision. Prior to this era, only actors with considerable resources could afford to organize armies for war, could cross long distances to conduct battles, and could repeatedly acquire knowledge or experience in order to prevail. Now would-be attackers with limited resources other than Internet access and time, can with near impunity choose the scale of their organization from five to 5,000

members, the proximity of their targets from five to 5,000 kilometers away, and the precision of their target group from five to 500,000-targeted systems.[7] The ease of relatively risk-free conflict with others on the web is so apparent that even botnet gangs of criminals managing secretly controlled computers of innocent citizens will fight among each other technologically, often seeking to destroy the other's malicious software while inserting one's own.[8]

The characteristics of the globally open, unfettered, opaque cyberspace have not only generated much wealth but have also democratized predation on strangers at will with little to no governance or social controls to curb appetites or success. No more need resources, reach, or repatriation of returns stand in the way of experimenting with predation on strangers. As a result, not only individuals but whole organizations have emerged to benefit personally from this distant, free predation, and unethical adversary states have not been far behind. Today there is abundant evidence of exploitation of the digitized underpinning of societally critical functions and the extensive debilitating losses in social knowledge investment meant to sustain national well-being over time.[9] The data is already accumulating about the enfeeblement and sudden demise of major corporations such as Canada's Nortel, which are increasingly linked to the hacking of their knowledge and markets before the corporations are able to recognize the losses and adapt.[10]

With the massive amounts of success becoming increasingly visible, victim states have begun to respond, and the cyberspace meant to be a cooperative, free spirit environment[11] is now a conflict-laden substrate shared globally across the critical systems of any connected society. States and victim enterprises

are imposing or adapting structures in and around cyberspace's man-made elements in order to control the threats to the resources, jurisdictions, and allocation of benefits which follow efforts to shore up the national defenses. Eventually, the state level reactions to cyber-insecurities cumulate to alter the overarching national and international systems. There is no cyberspace normal equilibrium to which it globally will return in a cybernetic or ecological fashion, like wind patterns or tides. Rather, war built the modern state, and the cyberspace substrate's tendency to encourage predation and cybered conflict is, in turn, altering both the state and the surrounding international system.

CYBERED CONFLICT AND FUTURE CYBER-WESTPHALIA[12]

Robert Gilpin observed the necessity of looking beyond diplomacy and militaries to take into account the systemic influences and effects on the interaction of states and communities in order to understand the propensity to conflict.[13] Today cybered conflict is emerging as the new normal in struggles between states and groups competing for the enormous wealth laid open for the taking or generated by the ungoverned global substrate.[14] A wide spectrum of possible conflict options are being developed as humans, and their communities rush to fight over resources, access, long-term leverage, and sometimes reputation benefits obtainable through cyberspace without resorting to overt war. Conflict between states moves erratically from the traditional definable kinetic conflict to an amorphous range of predatory and defensive disruption operations.

Now conflict is likely to be shifting, opaque, and deeply disruptive at will for underlying systems penetrated by the global substrate. With more to gain from avoiding kinetic exchanges, adversaries will maneuver across tools, targets, times, and distances at will to avoid interruption or prevention. Operations in offense, defense, and third-party opportunism will be longer in duration, deeply deceptive in execution, and riven with ambiguities over when it started, as well as why, where, and who is involved at any moment.[15] Receding is the clarity of kinetic exchanges between militaries or, at least, armed groups expressing their grievances in public ways with visible tools, self-evident destruction, and calculable periods of activity. A nation can be in a cybered conflict with many adversaries at once and yet be unaware of its own losses and attrition of effective options.

In cybered conflict, deception is key to efficient success. Analogies to war are often expressed as games, chief among these are checkers, chess, poker, and go.[16] The problem with applying these analogies to the full spectrum of cybered conflict is that games have rules. Cybered conflict does not, especially none about the use of deception throughout operations at any level. There are very few circumstances under which announcing one's cybered campaign's onset, its progress, plan of action, or expected rewards is efficient or effective. Much like the first barrage in a traditional kinetic war, once the exploit and its losses are realized, the exploit will be countered, and retribution will be taken for losses. The maximum return is gained in cybered conflict when the opponents do not realize who deeply penetrated and exploited the systems on which their well-being depends.

The self-evident clarity of a fully overt kinetic war is unlikely, though not impossible. In this era, classical war is only likely by accident, overwhelming emotional misperceptions across media and many leaders, or true ruthlessness by states and nonstate groups.[17] Even so, the attractiveness of gain over the long term will induce a longer, slower, intensification of conflict involving the extraction of knowledge critical for the ability of civil societies to maintain the free flow of goods needed for the open global system and their own societal well-being. With no overarching democratic civil society hegemon able to enforce rules of warfare on multiple adversaries in a globally cybered anarchy, no system in any state is untouchable by such conflict if cyberspace reaches into it.[18]

Cybered conflict across major adversaries increasingly resembles "whole of the system" struggles closer to traditional total war, but these systemic conflicts anticipated by Gilpin, Anthony Giddens, and even Alexander Wendt[19] can occur with no shots likely to be fired. Cybertechnology has altered what conquest might mean in terms of returns on investment by state level predators. First, cyberspace as a massive sociotechnical system has three main elements according to Dan Kuehl—connectivity, content, and cognition.[20] Of these, content and cognition are key information elements enabling the substrate to penetrate throughout the critical elements of society. Throughout history, information plays an enormous role when it is able to be manipulated in delivery, in narrative, or in effect on the audience.[21] Conquest of another land and its human inhabitants often involved a range of placating information tools to reduce the ability to organize and resist, thus costing the conquering predator more to maintain control. These include a delivery that

seems god-like, deceptively innocent, or overwhelming to targeted peoples, a foundation story that justifies all measures taken including genocide, and a reinforcing subsequent cognitive structure including renaming, linguistic replacements, and ubiquitous enforcement of repression of alternative explanations.[22] Furthermore, cyberspace has a unique technological advantage over the control challenges of prior eras: It enables knowing and doing to be compressed tightly. The time between when the information is obtained (as in spying) and when action is possible (as in using technology for harm) is now nearly simultaneous for any adversary.

This blend of knowing and acting (and altering what is known) makes the technological change embodied by the global substrate exceptionally powerful as a tool for conflict in overwhelming defense mechanisms designed for reflection before acting in response. Recasting conquest of land and peoples rather as attempted conquest of the cyberspace substrate, its technology, narrative explanations, and the control of critical elements of a dependent society by incursion at one's whim certainly should induce national responses and actions. States faced with this newer form of penetration and conquest will naturally resist and what they construct in either conflict or fear will also change the topology of the international system over time, just as prior technological changes and attempts at conquest changed the international system in history.

Today, rising perceptions of how pervasive the threat and vulnerabilities are, is already inducing structural changes and new arrangements across public and private systems of states. At varying tempos and intensities, national leaders today are preparing

institutionally for new kinds of whole system battles. Global cyberspace substrate now influences the distribution of authorities in digital civil societies themselves. The greater the perception of imminent loss, the more the defending societies will alter themselves, if necessary, to avoid losing, and the more global cyberspace substrate now influences the distribution of authorities in and across digital civil societies themselves.

Today the building blocks of a future Cyber-Westphalian system[23] are emerging from the reactions of states recognizing slowly the extent of cybered conflict and their national vulnerabilities. Slowly state leaders are trying to define what they will defend for the nation, at what point along the access points into the traditional territory, with what means, for what length of time, and to what acceptable effects at home or against the adversary. National cybersecurity strategies are being issued.[24] National level cybersecurity centers, cybercommands or their national equivalents, and governmental computer emergency or incident response teams increasingly are emerging.[25] Legislation, directives, orders, or policy changes are also emerging to allow governments to extend their signals intelligence capabilities into Wi-Fi, Internet cables, or mobile telephony used to access the Internet.[26]

These institutional, strategic, and legal changes build the jurisdiction of the national political system with respect to the global cyberspace substrate. They are also building the foundations for the future cyberpower of their nations. Decisions made and institutionalized across states during this cybered conflict transition period will influence the ability of states to protect their well-being when this emergent Cyber-Westphalia consolidates,[27] a process estimated to take about a generation to be fully evident.[28]

ROBUST CYBERPOWER

Charles Tilly noted in his seminal observations that ways in which the society reconciled its capital and coercion mechanisms strongly determined the structure of a "modern" state that underpins today's liberal democratic civil societies and their ability to maintain a liberal international system.[29] In the same way, decisions made and institutionalized across states will influence the well-being of states in the subsequent Cyber-Westphalia era by providing their relative portion of cyberpower. That is, these institutions, strategies, and resources embedded in the national response will affect how resilient the whole society is to the threats of the cyberspace substrate and how able the state is to forestall devastating penetrations by selectively targeted disruptions prior to an attack. Over time, as the deeply digitized interstate system becomes more structured in the current transition era and produces the next era of cybered Westphalian states, some states will adapt their public and private sectors to the full spectrum of cybered conflict more effectively than others. Those states will be better placed in relative cyberpower and skill in cybered conflict to defend their national systemic well-being in both the near and far term.[30]

Three forms of governmental or semi-public institutional response to cybered conflict exist today, sometimes all in the same state. The most common form of response is some form of intergovernmental or "pan-agency" cybersecurity coordination agency or office focused on resilience to attacks across the government first and privately held critical infrastructure secondarily. Generally, this office is located quite near the head of government such as the prime minister. A good example is the British cabinet level Office of

Cyber Security and Information Assurance, as is the French National Agency for Security of Information Systems (ANSSI).[31] A second institutional model is the cybercommand model in which a military or security unit is given the task to defend its agency but also to track adversaries for active defense. The latter mission is better understood in its effects as the targeted and tailored forward disruption of exceptionally skilled cybered conflict adversaries before they can strike or during an operation without escalating the conflict or revealing the successful techniques. Naturally, the new U.S. Cyber Command is the originating model, but there are others emerging with a closely similar mission and without the specific name.[32]

A final form is the later iteration of the originally private cyberalert organization, the Computer Emergency Readiness Team (CERT). Designed by university professors to help subscribing private firms share their experiences in attacks and thus be better able to resist future attacks, the CERT model has been copied globally. It has also, however, changed in the process from a purely private defensive form, CERT1, to a more robust and generally governmental form with broader obligations to more actively share and train defenders, national CERTs or Cyber Security Incident Response Teams (CSIRTs)[33] or CERT2. The third iteration is yet more muscular in terms of adding elements of forward disruption implied in vague statements about forestalling imminent attacks. The muscular CSIRT is not yet evolved into cyber commands as a rule, but for states with few to no governmental cyber security resources, this model has begun to develop traction as not only a source of national knowledge for resilience but also a repository for cybertalent for possible forward disruption.[34] It is, however, as yet not at

the scale to displace either of the other models save in these already cyber-handicapped states.

As of now, many states have elected to establish one or more of these models, but will need the capacities of both resilience (pan-agency guidance) and disruption (active defense in cybercommand equivalents) to have established credible cyberpower for the coming Westphalian system. The decisions made in the near future will strongly influence how far along in these capacities defending states are during the transition. It is reasonable to expect that lagging states or those with insufficient investments in both will find themselves disproportionately under assault as their neighbor nations develop their cyberjurisdictions and power and thus become more difficult to penetrate and exploit with impunity.

THE FUTURE AND NOT-QUITE-PAST IN NEW INTERNATIONAL SYSTEM TOPOLOGIES

At the end of the day, it is not clear now which states among the rising, status quo, or declining powers[35] will have the perspicacious leaders and institutions that grasp the systemic nature of cybered conflict more accurately, nor what kind of liberal or illiberal international system will result. Nothing in the current structure of cyberspace guarantees democratic civil societies as the future normal state, a liberal international system as the overarching meme of the international system, or the continuance of atomized nations fending for themselves in the complex opaque conflicts of a deeply digitized and dynamically surprising globe.

Three possibilities have more likelihood of occurring, each having implications for the others in terms

of how much the future resembles the recent or distant past in terms of human conflict, cooperation, and benign neglect. These are a system of fractious atomized states with varying degrees of cyberpower and responsible behaviors, a system dominated by the rise of a non-European derivative, illiberal superpower and the decline of liberal institutionalist globalization, and a system of many various balancing responses dominated by new or renewed technologically integrated regional alliances of like-minded, like-structured, or like-threatened nations. The trends indicate more, not less, uncertainty and turbulence, and the continuing presence of cybered conflict, although the spectrum may have fewer options for nonstate actors.

Systemically Blended Democratic Civil Societies.

War built the modern state, but only because of serendipity in the form of the Catholic Church needing individuals to counter the coercive power of the aristocracy and the capital wealth of merchant cities.[36] When all conflict is cybered and systemic, i.e., reaching deeply into adversary home systems, its events or the reactions to them change political systems inevitably. With no shot fired, the challenges are in one sense more profound than physical threats. The possibility of a systemic cascade affecting wide swaths of a society, when taken seriously, tends to force coordination efforts across traditionally separated sovereignties that disperse power across civil society democracies. National security strategies can no longer leave economics off the table as a tool of interstate conflict, not only because of the commonality of tools, networks, and criticality with what was called national security systems but also because the loss of control over the

knowledge investments of one will inevitably mean loss of the other as well.

Conflict along the substrate is altering not only concepts of warfare but also the presumptions of power distribution in democracies themselves. Neutralizing threats able to worm in through a fundamentally insecure and ubiquitous substrate of economic or governmental systems begins to force the blending of authorities across traditional military, police, internal infrastructure, and economic concerns nationally and institutionally in ways discussed during the heyday of the anti-terrorist early-2000s but never truly required as long as national borders could be monitored and reinforced without blending the military and the police. The technical fungibility of the cyberspace substrate makes this blend increasingly necessary to have the comprehensive oversight needed to discern emergent patterns of harmful behavior before time between initiation and effect shortens beyond intervention, dampening, or restorative mitigation.

A good example is the recent development of teams in the U.S. Cyber Command specifically designed to help the largely vulnerable and beleaguered major private companies recognize they have been harmed and defend themselves.[37] This example is all the more powerful when it occurs in a federal nation like the United States without the strong history of public-private cooperation more common in Europe. Only in World War II and the context of total war was Franklin Roosevelt able to force the synchronization of government and economic actions, and only until the end of the war. Data sharing itself has been difficult for privacy and past abuse reasons across democratic civil societies. Only in states beset with major internal deceptive actors destructive to civil legitimacy and well-being, such as a Mafia, have the mechanisms

of widespread sharing of knowledge about internal behaviors been deemed necessary.

Yet, today discerning the major extractions or penetrations requires sharing across all the systems in the chain of cyberexchanges before and beyond the probable targets. As the substrate has linked so many of the socio-technical systems of the democratic state without awareness of its insecurities, so will the police, the military, and the critical economic actors be seeking knowledge across systems that are similar or the same in order for each to complete its own mission defense or forestalling of harm. That data inevitably will be collected societally as big data by actors intermediating among these sectors, resulting in all three coming to the same data table more and more often, and sharing among themselves as necessary for systemic survival as well. The institutional accommodations of this knowledge sharing will vary across democratic civil societies, but it is inevitable if the society is to develop the requisite resilience for adequate cyberpower in the future.

This blending trend, however, is unlikely to be internationally replicated in a cooperative global system, at least in the short term, because states defend themselves first and foremost. The threats of a globally malicious cyberspace substrate, especially at the scale and persistence of today, already have encouraged the rise of the building blocks of national borders. These "edges" of a state's cyberjurisdiction, whether or not they are actually equipped to protect them, must rise to reassure the political leaders internally before they can be softened to allow special sharing or access by allies, let alone random trading partners. Indeed, the perception that it is the openness that has caused these losses is fueling the need to put up threat dampeners

by filters (e.g., Sweden), monitoring (e.g., the United States), technological sovereignty (e.g., Germany), centralized guidance for Telecoms technological systems (e.g., France), or even address controls now emerging in marginally democratic states of the former Soviet Union.[38]

Under this basic atomized topology of states defending their own cyberjurisdictions, it is unclear which of these more blended democratic civil societies are better able to develop their cyberpower and defend their well-being during the transition era. Much depends on the effectiveness and acceptance of the sharing of knowledge and action as institutionalized within each state. The more unitary states with a long history of close connections between public and private sectors may ironically create more effective, public-private collaborative and yet controlling institutions of resilience and disruption. If the recent past is any guide, however, this will be exceptionally problematic for large and/or federal states to achieve. Federal states tend to formalize separate sovereignties across the government and have less cooperative relations with private corporate partners competing with each other in general.[39] The lack of internal cooperative regulation and actions makes the whole of the system resilience less effective and encourages governmental reliance on forward disruption with more intensity despite the blowback and accidental escalation risks. It will be harder for such states to establish a resilient reputation and one would expect they would experience a disproportionate amount of attacks as a result. The latter may have much tougher challenges with the scale and spectrum of cybered conflict, relative cyberpower, and national well-being in a cybered world.

Rise of Illiberal Cybered Superpowers.

A second distinct possibility is the rise of an illiberal state changing the relative perceptions of power across the international system by its scale of influence and unrelenting pursuit of the gains of cybered conflict, albeit below the red lines of war. Of course, China is the most likely major actor able to manipulate the atomization among states of Europe and the Americas in order to achieve a cyberhegemon status due to its wealth and monopoly of technology production and standards across the globe. Already China has achieved remarkable progress in the process, having become the major source of technology production globally and soon to surpass the United States as the largest economy in the world.[40] Its reputed command of cybered conflict is increasingly unparalleled, even if indignantly and vigorously denied. The Chinese leadership has proven especially adept in long-run, low-visibility campaigns through the broad synchronization of the massive globally executed extractions of economically critical knowledge by large, well-skilled cybered military units and vaguely directed "patriotic" hacker communities, with rapidly rising multi-market manipulations over time using subsidized and relentless flagship corporate enterprises like Huawei.[41]

As long as China remains politically unified by one party focused on providing economic resources now and over time as its sole claim to legitimacy,[42] it is unlikely that any sanction not rising to the level of threatening China's leadership directly with massive failure on this goal will succeed in attenuating these broadly encouraged expropriations from other countries. So much of the dramatic rise of China rests on

this massive transfer of wealth that asking the state to curb its citizens is akin to asking a farmer rising from abject poverty with many mouths to feed to forego harvesting and go broke in the name of the wider community. Few states, liberal or not, would accept this option barring a *force majeure* indeed. Several authors have suggested the fantastic Chinese rise is a chimera based on currency speculation, inefficient internal markets, and a highly insecure internal Internet of its own.[43] Elements of these assertions are undoubtedly true, but the overarching trend rewards a large scale in population linked to widespread technological persistence and familiarity. China manifests both at levels not shared by, for example, India. As long as the current underlying substrate remains as insecurely constructed as it is and as directly linked to the heart of the knowledge investments of the wealthier states, this predation will profit China and enable its rise as a major actor in the transition cybered conflict era at least. By scale alone, China's actions will change the rules of the conflict and elements of the outcomes.

As things stand now, the grave difficulty for democratic civil societies in resisting the rise of an illiberal hegemon is that the opaque complexity and ubiquity of today's cyberspace encourages persistence and deception in ways not accommodated by the rules of trade today in civil societies that focus case by case. If a patent idea is stolen before the sclerotic U.S. or European patent offices can even rule on the idea and it is marketed via a Chinese corporate entity with nearly unlimited credit from its government before the original developer can produce anything, then the years of knowledge investment have been stolen and the future returns lost to the originating developer and state. As long as this theft is anonymous, there is no

mechanism for proof that motivates the owner's state to act. Even when patterns of theft across millions of incidents emerge, the rules of civil society require that each is adjudicated separately, leaving the persistent large-scale perpetrator able to benefit from desiccating whole industries in victim states long before any government can act for longer term self-defense. The opposite is not true in the illiberal state, of course.

Importantly, the rise of illiberal states to dominate global systems is not possible unless deception is widely enabled by the deeply opaque cyberspace substrate. The tide of economic enfeeblement present in cybered conflict today tends to run against the state unable to act to punish adversaries without incontrovertible proof in a legal sense, unless the state acts vigorously and possibly illegally in its own defense countering the deception. The 2013 "*L'Affaire Snowden*" (The Snowden Affair) suggests that major states already are attempting to meet deception and persistence with the forward use of surveillance and unearthing of patterns, at the very least.[44] Stuxnet also suggests significant experimentation with tools of conflict that are programmed to alter behaviors of an adversary without crossing red lines or engaging an inadvertent cascade.[45] Nonetheless, without other institutional, legal, and technological changes and with many caveats already suggested, one can argue that the globally open, unfettered, and nearly free cyberspace substrate is indeed stacked in favor of a large, technologically-aggressive illiberal state rising over the transition era to prominence in the coming Westphalian interstate system.

How would such a hegemon actually orchestrate its influence under this scenario? In 2002, a prescient Kuehl argued that cyberspace operates to affect its

using groups across its connectivity, content, and cognition capacities.[46] By and large, democratic civil societies are only interested to date in controlling connectivity enough to eliminate systemic threats traveling across the nets, and in filtering content only to the extent of removing malicious packets containing these threats. Philosophically and politically, they have no desire to control cognition at all and the other two (connectivity and filtering) only as much as it takes to secure the well-being of their citizens. In contrast, illiberal states across the globe have indicated interest in control across all three aspects of cyberspace. This concern was, for example, explicitly indicated in the proposal to control cyberspace tabled in the United Nations (UN) in 2011 by China and Russia, in which cognition control is included as a national concern for "information security" rather than cybersecurity.[47]

Control of the characteristics of the basic technology of cyberspace would be key to hegemonic domination. Accordingly, an illiberal hegemon would be interested in having global technological standards that enable a full range of state controls across all of the three aspects of cyberspace identified by Kuehl. For economic efficiency and political convenience, other lesser states would migrate to using this technology as well. As the standards and the production designs preferred by this hegemon spread to become standard in many states, the cyberspace substrate under an illiberal hegemon will not only be divided nationally in cyberjurisdictions but also in close technological controls on what is passed among states whether by land, air, sea, satellite, or undersea Internet cables. Especially if the hegemon remains the major producer of the global technological systems used by nearly all states, the international system fueled by cybered exchanges increasingly will be illiberal.

Under this possible topology, cybered conflict continues to be particularly turbulent because democratic civil societies are unlikely to accept quiescently this development for long. They have already signaled distaste for having the UN, via its information and communication technologies agency, impose global technological standards favoring control of cognition as well as content and connectivity. However, the spectrum of cybered conflict is wide and options varying. In many other manifestations, the rising illiberal states iteratively can maneuver to spread these technologies and standards so deeply into nondemocratic civil societies that those opposing states will be forced to accept many aspects of this control just to interact economically with much of the world. It is exactly the possibility of a *fait accompli* instantiation of such restrictions across a major continent that is engendering deep concern with Huawei building, operating, and maintaining the African 4G network. While it is provided gratis to these developing nations, the systemic effects on the liberality of the emerging system may be profound.[48] The response from democratic civil societies will be turbulent, if only because democracies need to motivate their citizens, often through hyperbole, to make major investments against opaque and long-term threats whose perpetrating originating states are vigorously denying the allegations.[49]

Countervailing Regional, Civil Society and Herd Alliances.

If trends continue as they are today, given the deception and deeply systemic nature of cybered conflict now, the coming international Cyber-Westphalian system is unlikely to remain as the liberal arena set

up by Britain and enforced by the United States over most of the past century. However, neither is the new structure likely to be that of completely independent, atomized states defending themselves against major illiberal cyberpowers. Riven by competing internal interests and buffeted by the redirecting blame campaigns of more illiberal cyberpowers, it will be politically difficult and financially exceptionally hard for civil society democracies to invest soon enough in sufficient national cyberpower (both resilience and disruption capacities systemically) to protect their national well-being alone.

More likely is the rise of like-minded mutual cybered protection alliances sharing sensors and response systems and generative adaptations, especially across regional neighbors and already allied civil societies. Being an "island cyber" nation is difficult in the current and coming era because the opaqueness of the substrate does not vanish with the rise of state controls at some jurisdictionally defined and physically enforced edges. Effective national control of a cyber-jurisdiction will require a certain externalization of preferences to lighten the load on home filters or other systems meant to keep the national systems sufficiently unpenetrated for future well-being. Eventually like-minded states realize the benefits of having multiple redundant sensor sets across nations, engaging the intellectual ability of larger populations across civil societies, and of presenting multiple targets and punitive responders to continuing aggressors. This resetting of the scale, proximity, and precision advantages in the context of enforceable civil society laws and oversight reduces the system threat of cybered conflict at least inside the collective front of each alliance.

The opaqueness of the current cyberspace substrate, however, will affect the composition of alliances because they are unlikely to survive long unless all participants are roughly equivalent in holding up their own part of the collective frontier. In a complexly interdependent system, the weakest state becomes the avenue by which malicious external forces flow their attacks into the alliance at large, and out again. Therefore, just as the substrate tends to force blending of authorities within victim states, it is likely to force deeper technological ties among states choosing to ally themselves for cybersecurity. One can imagine a form of technological sovereignty being encouraged across a North American and European alliance with other allies such as possibly Japan being given special access, data sharing, and shared protections via common new basic technological systems of exchange. One would expect these alliances if they are to endure, to be grown differentially and deeply across small numbers of states, with weaker states on the outside or at best in a secondary periphery of limited trust.

In addition to the regional or like-minded alliances, one can foresee the development of "herd" alliances where smaller, weak cyberpowers band together but not necessarily against a specific state actor. Rather, unlike the one or two very large states, or a small number of very wealthy states who will be able to afford their own technological sovereignty, many states will be on their own on and off again. Not every state will be in an alliance or stay in the same one over time if it proves inadequate. But as weaker states are likely to be victims or proxies, there is an incentive to join alliances to reduce the burden and the likelihood of threat success, or just to have access to some collective knowledge. Thus, this topology is likely to

remain that of basic state cybersovereignty but with a slowly shifting environment of alliances, at least in the mid-term.[50]

For those in functioning and effective long-term alliances, cybered conflict may be turbulent, but the overwhelming burden of self-defense is diffused across a small community possibly performing different niche functions or, at least, dispersing the costs of sensors, analysis, and disruption. Collectively, they have more robust cyberpower in ways each individually cannot achieve easily. For lesser cyberpowers outside the stronger alliances, the rising Westphalian system will often be an era of frustration and loss of key knowledge investments as they drift in and out of lesser alliances attempting to secure their own cyberjurisdiction and well-being against deception and relentless technological change.

THE WAY FORWARD. THE NEED FOR SYSTEMATIC SLACK AND SENSORS?

Whether atomized fractious states, several illiberal hegemons, or collective mutual cybersecurity alliances come to dominate the future Cyber-Westphalian system and its conflicts, some aspects of today's threat environment, in particular, are likely to change in their role or probability dramatically.

First, as the emergent Cyber-Westphalian topology solidifies, the nonstate independent actor is doomed to decline and irrelevance. The states, all together, will be imposing limits on the current mass of organized or unorganized malicious actors who operate in the shadows of cyberspace. While the rise of China may have been helpfully fueled by the masses of young hackers making a living for themselves or

their corporate bosses on the technological insecurities and neglect of the wealthier western states, this flood of predators will have more difficulty exploiting the proximity advantage of the current substrate as victim states become more resilient or able to trace and strike back. Their slow loss of success will also make it harder to organize transnationally at the scale needed. With enforced national cyberjurisdictions, extractions across national cyberedges will require more and more the benign neglect of local authorities who, themselves, may be held culpable if the pattern continues.

Even in illiberal states that once massively benefited from that nonstate cybercommunity, the unorganized hacker will be less and less tolerated, and free-for-all hacking with impunity will decline overall. As citizens in illiberal states grow wealthier, they will also become more inviting alternative targets if the foreign prey becomes harder. No state desires its own hackers to hack internally. Across any topology likely today, the socially enforced punitive responses to the floods of malicious behaviors are quite likely to rise throughout this period. These new controls will narrow but not eliminate the paths for nonstate actors or transnational organizations with few resources to continue extractions at the levels and scale that occur today.

Second, the spectrum of cybered conflict is likely, as a whole, to demonstrate greater exploitation of precision in order to defeat heavily encrypted or dynamic technologies. The positive news is that today's script kiddie being able just to buy a simple program to exploit a botnet nearly vanishes. The downside is that successes will be seen as massive exploits of weak states or major penetrations of systems thought to be

quite secure. When the vast majority of systems can be decoupled as needed or are routinely decoupled for resilience, the very weak or the very strong become the focus of the remaining and quite powerful population of exceptionally skilled adversaries. The weak cyberpower is easy prey itself, but it may be more valuable as a weak link into the rest of a secure system or alliance. The strong cyberpower is likely to be a central pillar of defense for itself and its allies, thus not only a great challenge but also a great coup. If its resilience and disruption efforts fail, then much of the rest of the allied system, including the midlevel systems thought to be secure, are likely to fail with it.

Furthermore, the dynamic evolution of basic technologies continues unabated, but as these are implemented across societal systems, new technologies have often introduced new lines of fragility unseen or neglected by defenders and designers. These are discoverable by ever attentive sophisticated malicious actors routinely seeking advantages along the whole spectrum.[51] While proximity and scale of organizing advantages decline systemically with the rise of effectively implemented national cyberborders, the precision advantage remains as the most difficult threat over time because of the complexity inherent in cyberspace. New technologies have a strong propensity to quickly spread globally even if critical systemic flaws are not yet discerned. Once a systemic flaw common to many users is known to be exploitable, everyone connected to those weak links also becomes a vulnerable downlink target, and adversaries will attempt as ever, to use the advantage to target as precisely as desired.

Third, ironically enough, the transition process to stabilize the interstate cybertopology and reduce the slow massive bleed-out of national well-being may

also encourage a more rapid move to the end of the spectrum involving kinetic exchange. More resilient states are also much more frustrating targets for adversaries. Depending on the gains, the grievances, or the perception of losses, some adversaries may be more willing to escalate if lower level campaigns are routinely unsuccessful. Their plan to obtain access or leverage may not deliberately include movement to kinetic exchange, but depending on where along the path to resilience and disruption a victim state is, the adversary's operations through complex systems accidentally may initiate a cascade of disruptive events across those and adjacent critical systems requiring a major and strenuous response by the victim state or states.

The frustration of adversaries determined to succeed could encourage brinkmanship against more robust cyberpowers as targets. One consistent characteristic of the higher skilled hackers is an arrogance about their abilities to control the systems in which they work or on which they prey. Suggesting escalation to the targeting of state leaders is appealing as a tool of leverage, otherwise known as blackmail, and it usually requires some demonstration of ability and intent. Even the cleverest of Mafia bosses have inadvertently triggered gang wars to their own destruction.

Frustration works in both directions, however, as does miscalculation when adversaries are convinced they are existentially at threat, the time to react effectively short, and both the tools and the arena of battle are opaque.[52] Robust cyberpowers will strike back in a more controlled fashion to disrupt the blackmailing organization, and probably increase their resilience along the perceived lines of possible attacks. The problem will be the less robust powers, especially those

weak in resilience. As Douglas Gibler notes, territory, regime, and policy are the three major sources of disputes that lead to war, and of these three, violating territory by far outweighs the other two as an impetus to battle.[53] In a Cyber-Westphalian world, states will be no less concerned about protecting their territory, especially if they have been sensitized to the existential costs of not doing so in cyberspace. Soon enough, all states will possess a cybercommand or equivalent for disruption capacities. Not all states, however, will have the systemic resilience necessary to be a robust cyberpower, nor the wisdom to know how and when to use cyberdisruption capabilities if provoked. The weaker cyberpowers, especially if not in a moderating alliance, are more likely to strike back rapidly and strongly out of concern that delay will allow considerable harm to their less resilient home society. Thus, they are more likely to engage inadvertently wider swaths of collateral damage and start sequences of events that more easily escalate into kinetic exchanges.

No trends discernible today can indicate how those exchanges or cascades will develop or harm, save by monitoring the institutionalized developments of resilience and disruption capacities over time. However, systems, indeed, depend on their weakest links. The more openly linked and less able to decouple are the rest of the states as one or more ramp up in escalation into cybered kinetic exchanges, the less other states will be able to stay out of harm's way at the very least. Analogies to the web of alliances that triggered World War I are inescapable.

At the end of the day, the cyberspace substrate will still be a huge, man-made socio-technical system that is being constantly, iteratively restructured by the human societies living with it, securing their future

through it, and struggling for advantage across it. In the best of all possible futures, the democratic civil societies succeed for themselves at least in securing a smaller but still liberal inter-alliance system based on redesigned socio-technical-economic systems resilient to surprise and mutually maintained with shared foreknowledge and constant learning. Then their example of how this beneficial cybered substrate may be restructured to benefit all participants proves enduring despite the advent of disruptive technologies, the population growth throughout the rest of the less liberal world, and the active menace of less liberal external cyberpowers. As a gold standard, then, the example is envied and copied more broadly with minimal cybered conflict over time, resulting again in a globally liberal and less predatory system.

Unfortunately, none of this happy vision is in any way inevitable, and decisions made now across the world's democratic civil societies will determine if any part of it is still possible when the Cyber-Westphalia system fully solidifies. What is built now by the democratic civil societies will play a major role in how they experience cybered conflict over the transition and in determining which, if any, of these states, are robust enough as cyberpowers to defend their well-being in this coming less liberal global topology without finding themselves at the end of the spectrum in a cyberkinetic exchange.

ENDNOTES - CHAPTER 19

1. For discussions of the relations between internal governance, conflict, and international system, see Michael Mann, *The Sources of Social Power: Global Empires and Revolution, 1890-1945*, Vol. 3, New York: Cambridge University Press, 2012; Anthony Giddens, *Modernity and Self-identity: Self and Society in the Late Modern Age*, Stanford, CA: Stanford University Press, 1991.

2. Robert Gilpin, *War and Change in International Relations*, Cambridge, UK: Cambridge University Press, 1981.

3. Raymond Aron, *Peace and War*, Cambridge, UK: Cambridge University Press, 1966; K. N. Waltz, *Theory of International Politics*, New York: McGraw-Hill, 1979; Thomas Hobbes, *Leviathan: Or the Matter, Forme and Power of a Commonwealth Ecclesiasticall and Civil,* New Haven, CT: Yale University Press, 1960 (reprinted); Niccolò Machiavelli, *The Prince*, Vol. 36, New York: P. F. Collier, 1910 (reprinted); Sun Tzu, *The Art of War*, Samuel B. Griffith, trans., New York: Oxford University, 1963 (reprinted).

4. The term is deliberately an adjective, as in "cybered," in order to represent the transitional nature of the observation. When in the future, every conflict is cybered, the adjective will seem redundant.

5. John C. Mallery, "A Strategy for Cyber Defense" (earlier title: "Multi-spectrum Evaluation Frameworks and Metrics for Cyber Security and Information Assurance"), MIT/Harvard Cyber Policy Seminar, Cambridge, MA, Massachusetts Institute of Technology Computer Science & Artificial Intelligence Laboratory, 2011 and 2009.

6. The term "substrate" is the most accurate depiction of the phenomena. While it is not everything, much like the ground underneath one's feet or the water in which one floats, as it changes, so change the conditions of survival, competition, and long-term well-being.

7. Chris C. Demchak, *Wars of Disruption and Resilience: Cybered Conflict, Power, and National Security*, Athens, GA: University of Georgia Press, 2011.

8. Dan Goodin, "Upstart crimeware wages turf war on mighty Zeus bot: All your bots belong to us," *El Register*, February 9, 2010.

9. Riva Richmond, "The RSA Hack: How They Did It," *The New York Times*, April 2, 2011; "networked and cloud-based digital businesses are . . . vulnerable targets for cross-border mischief that . . . [could cause] international conflict," quoted from Michael Schrage, "How Amazon or Apple Could Cause a War with Chi-

na," *Harvard Business Review*, May 6, 2011; Dan Goodin, "IE zero-day used in Chinese cyber assault on 34 firms: Operation Aurora unveiled," *El Register*, January 14 2010; "HP Research: Cybercrime Costs Rise Nearly 40 Percent, Attack Frequency Doubles," Hewlitt Packard Research, October 8, 2012, available from *hp.com/hpinfo/newsroom/press/2012/121008a.html*; David Goldman, "The cost of cybercrime—The price tag on corporate data breaches is soaring: The rise in cybercrime is costing hundreds of billions of dollars each year," *CNNMoney.com*, July 22, 2011.

10. The Nortel Corporations bankruptcy is a major and clear case of this kind of slow roll of national knowledge stocks. Nortel went bankrupt in 2009, having been exploited by the Chinese firm Huawei in 2006-07 due to cyberextractions of critical data, and then beat to the broadband Wi-Fi market for which Nortel was preparing its major and existential launch. In 2010, the chief technology officer of the former Nortel was publicly listed as working for Huawei and seeking small technology startups for Huawei "investment." Siobhan Gorman, "Chinese hackers suspected in long-term Nortel breach," *The Wall Street Journal*, February 14, 2012; Mike Rogers and Dutch Ruppersberger, "Investigative Report on the US National Security Issues Posed by Chinese Telecommunications Companies Huawei and ZTE: A Report," Washington, DC: U.S. House of Representatives, 2012.

11. H. Rheingold, *Virtual Communities: Homesteading on the Electronic Frontier*, Cambridge, MA: MIT University Press, 1993.

12. Chris C. Demchak and Peter J. Dombrowski, "Rise of a Cybered Westphalian Age," *Strategic Studies Quarterly,* Vol. 5, No. 1, 2011.

13. Gilpin.

14. "Cybered" is the adjective deliberately used to indicate the coming ubiquity of cybermeans in systemic struggles. Eventually its use as an adjective will wither away as redundant. Conflict will naturally have cybered means involved.

15. Peter J. Dombrowski and Chris C. Demchak, "Cyber War, Cybered Conflict, and the Maritime Domain," *U.S. Naval War College Review*, March 2014.

16. See, for example, David Shenk, *The Immortal Game: A History of Chess, or How 32 Carved Pieces on a Board Illuminated Our Understanding of War, Art, Science and the Human Brain*, Random House Digital, Inc., 2006.

17. Several scholars argue that cyber "war" is not likely to ever happen. These authors do not account for the presence of other forms of conflict involving the long-term enfeeblement and disruption (or even systemic blackmail) more typical of the cybered conflict age, such as cyberoperations aimed at, for example, financial systems of targeted states. For examples, see Thomas Rid, "Cyber war will not take place," *Journal of Strategic Studies*, Vol. 35, No. 1, 2012. For a more complacent view reminiscent of early cyberprophets, see David Betz, "Cyberpower in Strategic Affairs: Neither Unthinkable nor Blessed," *Journal of Strategic Studies*, Vol. 35, No. 5, 2012.

18. Kenneth Neal Waltz, *Man, the State and War: a Theoretical Analysis*, New York: Columbia University Press, 2001 (1959).

19. Alexander Klimburg, "Mobilising Cyber Power," *Survival*, Vol. 53, No. 1, 2011.

20. Dan Kuehl, "The Information Revolution and the Transformation of Warfare," in K. de Leeuw, ed., *The History of Information Security: a Comprehensive Handbook*, Amsterdam, The Netherlands: Elsevier Science, 2007.

21. Tim Wu, *The Master Switch: The Rise and Fall of Information Empires*, New York: Vintage Books, 2011.

22. David Day, *Conquest: How Societies Overwhelm Others*, Oxford, UK: Oxford University Press, 2008.

23. While acknowledging that war changes the international system, it has proven difficult for some international relations scholars to accept that cyberspace and all its associated changes have the momentum to change the international system. This position is puzzling since it is well-known how the effects of technological changes in wars definitively changed the international system over history, from the stirrup, the long bow, gunpowder, the steam engine, telegraph, radar, to nuclear fission. See W. H.

McNeill, *The Pursuit of Power: Technology, Armed Force, and Society Since AD 1000*, Chicago, IL: University of Chicago Press, 1982.

24. As of April 2013, the European Network and Information Security Agency counted 14 among the 28 European Union nations with a published strategy and identified about 12 other nations in the world that had or planned to specifically issue a cybersecurity strategy. The list does not include the nations that are updating their national security strategies to include a section on cybersecurity or cyberoperations, however. See *enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/national-cyber-security-strategies-in-the-world*.

25. The scope of this chapter does not permit an exhaustive list of all these efforts. Exemplars include the following: a new cybersecurity center in India available from *business-standard.com/article/economy-policy/india-launches-policy-to-secure-cyber-space-113070200449_1.html;* the formation of a cybercommands in the United States available from *fcw.com/articles/2009/06/24/dod-launches-cyber-command.aspx*; and in Norway 2009 available from *eurosecforum.com/2012/07/roar-sundseth-chief-information-officer-and-commanding-general-cyber-command-norwegian-armed-forces/*; and the spread of computer emergency readiness teams (CERTs) with greatly enlarged missions from the early days of Carnegie-Mellon's CERT simply alerting subscribers to malicious software in the wild (see *cert.org/*) to the spread of a second and third model, each with more forceful missions, available from *apcert.org/*, *enisa.europa.eu/activities/cert/background/inv/files/inventory-of-cert-activities-in-europe*, *us-cert.gov/*, and a longer list of basic sites available from *en.wikipedia.org/wiki/Computer_emergency_response_team*.

26. See also the 2009 law allowing Swedish national police to filter all the Internet packets traveling to, from, or across the country, a law which in comparison is much broader than the legally constrained authorities used by the U.S. National Security Agency as revealed by Snowden in 2013. Merlin Münch, "Do as the Swedes do? Internet policy and regulation in Sweden—a snapshot," *Internet Policy Review*, Vol. 2, Issue 2, May 2013. Furthermore, these are all democratic civil societies, not the more authoritarian states of the world such as those which attempt to control rather than just monitor the connectivity and content of their Internet assets. For the last, see the extensive documentation

available at the Monk Institute's Open Net Initiative site, University of Toronto, Canada, available from *opennet.net/about-oni*.

27. Demchak and Dombrowski, "Rise of a Cybered Westphalian Age."

28. I discuss national cyberpower, resilience, disruption, and the new layers of national systems surprise of the cybered conflict era extensively in the following work: (The main points of those arguments are summarized and incorporated here but will not be specifically cited unless the observation in this chapter seems to require that sourcing.) Demchak, *Wars of Disruption and Resilience*; Chris C. Demchak, "Resilience, Disruption, and a 'Cyber Westphalia': Options for National Security in a Cybered Conflict World," in Nicholas Burns and Jonathon Price, eds., *Securing Cyberspace: A New Domain for National Security*, Washington, DC: The Aspen Institute, 2012.

29. Charles Tilly, *Coercion, Capital, and European States, Ad 990-1992*, Cambridge, MA: Blackwell Pub, 1990, 1992.

30. Demchak, *Wars of Disruption and Resilience*; Demchak, "Resilience, Disruption, and a 'Cyber Westphalia.'"

31. Britain's Office of Cyber Security and Information Assurance, available from *gov.uk/government/policy-teams/office-of-cyber-security-and-information-assurance*; France's Agence nationale de la sécurité des systèmes d'information, available from *ssi.gouv.fr/*.

32. William Jackson, "DOD creates Cyber Command as U.S. Strategic Command subunit," FWC, The Business of Federal Technology, June 24, 2009, available from *fcw.com/articles/2009/06/24/dod-launches-cyber-command.aspx*.

33. Cyber Security Incident Response Team is the general definition, but variations abound.

34. For data on the original CERT, see *cert.org*.

35. See Goldman for an insightful discussion of how these powers tend to array themselves when challenged systemically. Emily Goldman, *Power in Uncertain Times: Strategy in the Fog of Peace*, Stanford, CA: Stanford University Press, 2010.

36. Tilly; Samuel Edward Finer, *The History of Government from the Earliest Times: Ancient monarchies and empires, Vol. 1*, Oxford, UK: Oxford University Press, 1997.

37. Ellen Nakashima, "With Plan X, Pentagon seeks to spread U.S. military might to cyberspace," *The Washington Post*, May 30, 2012.

38. For discussions of these approaches, some more indirect, see Münch, "Do as the Swedes do?"; John Mueller and Mark G. Stewart, "Three Questions about NSA Surveillance," *Chronicle of Higher Education*, June 13, 2013; Sandro Gaycken, "Does not compute—old security vs new threats," *Datenschutz und Datensicherheit-DuD*, Vol. 36, No. 9, 2012; Ronald Deibert *et al*., *Access Contested Security, Identity, and Resistance in Asian Cyberspace,* Cambridge, MA: The MIT Press, 2012.

39. Germany has proven an exception with its national industrial sector governing councils able to negotiate directly with the government. See Henrik Sattler, Stephan Schrader, and Christian Lüthje, "Informal cooperation in the US and Germany: cooperative managerial capitalism vs. competitive managerial capitalism in interfirm information trading," *International Business Review*, Vol. 12, No. 3, 2003.

40. Micah Springut, Stephen Schlaikjer, and David Chen, "*China's Program for Science and Technology Modernization: Implications for American Competitiveness: Prepared for the US-China Economic and Security Review Commission,*" Washington, DC: CENTRA Technology, 2011.

41. U.S. House, Permanent Select Committee on Intelligence, Representative Mike Rogers and Representative Dutch Ruppersberger, "Investigative Report on the U.S. National Security Issues Posed by Chinese Telecommunications Companies Huawei and ZTE," *Chairman and Ranking Member Investigative Report*, Washington, DC: U.S. Government Printing Office, 2012, available from *intelligence.house.gov/sites/intelligence.house.gov/files/Huawei-ZTE%20Investigative%20Report%20(FINAL).pdf*.

42. Barry Buzan, "China in International Society: Is 'Peaceful Rise' Possible?" *The Chinese Journal of International Politics*, Vol. 3, No. 1, 2010; William C Hannas, James Mulvenon, and Anna B. Puglisi, *Chinese Industrial Espionage: Technology Acquisition and Military Modernisation,* New York: Routledge, 2013; James McGregor, *No Ancient Wisdom, No Followers: The Challenges of Chinese Authoritarian Capitalism*, Westport, CT: Prospecta Press, 2012.

43. Judith Banister, David E. Bloom, and Larry Rosenberg, "Population aging and economic growth in China," Program on the Global Demography of Aging, Working Paper No. 53, March 2010.

44. Gene Healy, "Spying's the Story, Not Edward Snowden," *DC Examiner*, June 24, 2013.

45. Michael J. Gross, "Stuxnet Worm: A Declaration of Cyber-War," *Vanity Fair*, April 2011.

46. Kuehl, "The Information Revolution and the Transformation of Warfare."

47. Ronald J Deibert and Masashi Crete-Nishihata, "Global Governance and the Spread of Cyberspace Controls," *Global Governance: A Review of Multilateralism and International Organizations*, Vol. 18, No. 3, 2012.

48. Deborah Brautigam, *The dragon's gift: the real story of China in Africa*, Oxford, UK: Oxford University Press, 2009; Chris Alden and Christopher R. Hughes, "Harmony and discord in China's Africa strategy: Some implications for foreign policy," *The China Quarterly*, Vol. 199, No. 1, 2009.

49. David E. Sanger, David Barboza, and Nicole Perlroth, "Chinese Army Unit Is Seen as Tied to Hacking Against US," *The New York Times*, February 18, 2013.

50. Goldman, *Power in Uncertain Times: Strategy in the Fog of Peace*; J. S. Nye, Jr., *The Future of Power in the 21st Century,* Cambridge, MA: Public Affairs, 2011.

51. Stuxnet traveled through a well-known vulnerability in printers linked in networks, making the otherwise closed system vulnerable whenever someone simply wanted to print something. See Nicolas Falliere, Liam O Murchu, and Eric Chien, "W32.Stuxnet Dossier: version 1.3," Symantex Inc., 2010, available from *symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf*.

52. Robert Jervis, "War and Misperception," *The Journal of Interdisciplinary History*, Vol. 18, No. 4, Spring 1988, pp. 675-700.

53. Douglas M. Gibler, *The Territorial Peace: Borders, State Development, and International Conflict*, Cambridge, UK: Cambridge University Press, 2012.

CHAPTER 20

CONCLUSION

Dighton Fiddner

Most chapters in this volume seem to agree that cyberspace fundamentally alters the environment in which we currently operate and to which we respond, that the threats in cyberspace differ from traditional threats in ways that complicate the calculus of response, and that there is no turning back from this. The innovations have also brought about enormous changes in global politics that are proving difficult to manage. Indeed, both Nazli Choucri's and Chris Demchak's chapters provide a view of the future interstate system that foresees "disequilibrium." Demchak's virtual anarchy and Choucri's seven disconnects between traditional and familiar conditions and current realities portray an environment in which cyberspace increasingly has an effect on levels of governance providing security.

As Figure 20-1 illustrates, cyberspace seems to be diffusing (much in the same way that it does for the threat vectors identified by Dighton Fiddner) the level of governance that most effectively provides security, especially personal (human), economic, or physical security. Although the traditional means of local and state governance acting in the physical domain still persist, there is evidence that global collectives have acted collaboratively to enforce generally accepted norms of behavior through and in cyberspace. None of this is to suggest that global collectives are replacing the traditional levels of governance, but that cyberspace appears to be facilitating movement to some effective forms of governance (either higher or lower)

when the traditional level(s) cannot or will not provide the security desired by some segment of the society.

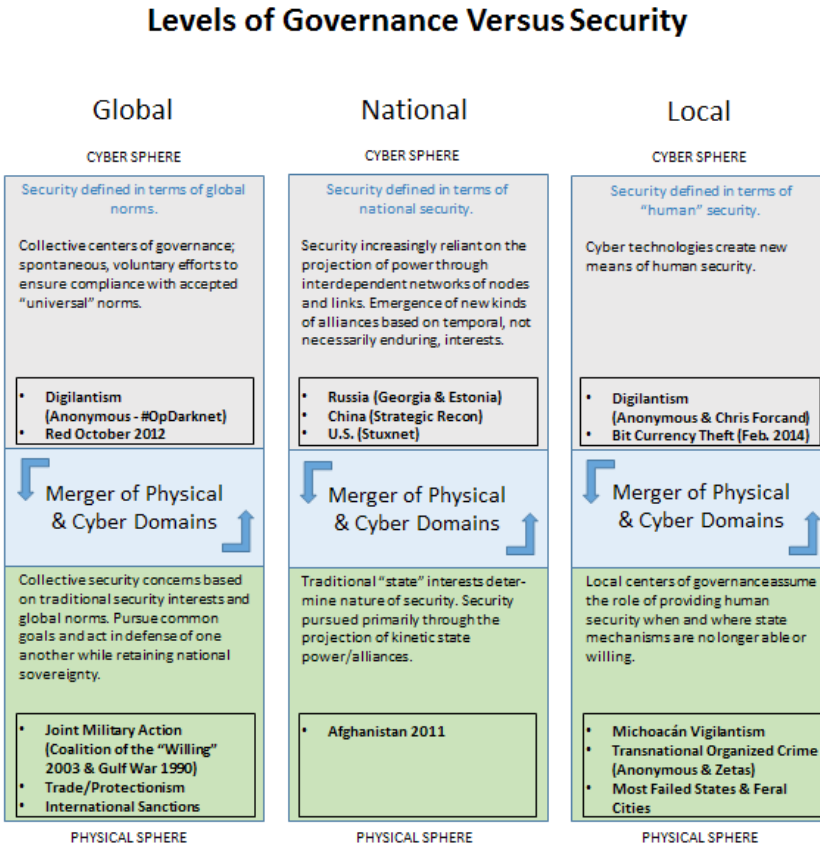


Figure 20-1. Spheres of Interaction.

Figure 20-1 and the following discussion is not intended to imply that cyberspace is unrelated to the more traditional physical sphere of interaction because it most assuredly is connected. Cyberspace is just too expansive and pervades (through the superposition principle) all spheres of activity as well as all the strategic domains—land, sea, air, and space. The Russian intervention in Georgia, as well as the analysis of the

new net in megacities and megaslums, displays such a melding of the physical and cyberspheres of interaction that it becomes difficult to locate in which sphere of interaction the activity is most prominent.

Against this background, Figure 20-1 represents the merging of the cyber and physical domains (horizontal rows) in global, state, and individual levels of governance (columns). The center column represents the normally accepted provision of security where personal (human), economic, and physical security results from behavior to protect the state's interests. As personal (human), economic, and physical security become more and more important, individuals are less concerned which level of governance provides it than that it is provided.

The bottom right square represents a local level of governance (vigilantes) in the physical domain providing personal security when the usual provider (the state) was unable or unwilling. The upper right represents a cybercollective (Anonymous acting as a global level of governance) providing personal security through enforced compliance with collective social norms where or when the state was unable or unwilling. The left column represents a global level of governance which is becoming more and more involved in providing security, to include personal economic and physical security. Ida Kelsey in Chapter 16 provides substantiation that, as cybertechnologies create global communities of like interests, these communities are taking responsibility to enforce generally accepted norms of social behavior. Digilantes "are not necessarily prone to partake in organized crime activities" but "have the ability to rationally recognize the problems of the status quo, and also, perhaps, the power to redress the situation" and "act as collaborative regulators" (upper left square). The lower left square repre-

sents the accepted norm of collaborative security (for both national and collective interests) practiced within the Westphalian state system.

CYBERSPHERE

Global-Cyber Domain (Left Top Square).

#OpDarknet (October 2011). In the case of the upper left square of global governance in the cyberdomain, Anonymous (a global collective) in early October 2011 removed links to pornographic images and videos on the Hidden Wiki, located on The Onion Router (TOR) Network's Hidden Service Protocol to expose the underground pedophile community known as "Lolita City." Shortly after the links returned online, the site became inaccessible in its entirety, presumably as a result of distributed denial of service (DDoS) attacks initiated by the group. Following the initial attack, Anonymous members discovered the digital fingerprint of the pornography and issued the host a warning to remove the content from its server at 9 p.m. central standard time on October 14. Freedom Hosting refused to comply, and 2 1/2 hours later, Anonymous completely shut down Freedom's services with DDoS attacks that created a 1-gigabyte structured query language and 100,000 American Standard Code for Information Interchange files of Guy Fawkes masks every 5 minutes.

On October 18, Anonymous released the names of the 1,589 users of Lolita City via PasteBin, including their usernames, volume of images uploaded, and age of the account. They invited Interpol and the Federal Bureau of Investigation (FBI) to investigate the records further. Later, through "an interview with a user named 'arson' in the #OpDarknet IRC channel,"

Anonymous stated that its "mission was only to take down illegal materials and the operation was not triggered by any particular event."[1] The organization also explained, "We vowed to fight for the defenseless, there is none more defenseless than innocent children being exploited."[2] In this case, the fight was successful. The FBI installed malware that infected all users who accessed the "onion" sites during the occupation period, unmasked the TOR routing protocol, and revealed the users' real locations.[3]

Red October (October 2012). In October 2012, the Russian cybersecurity firm Kaspersky Labs discovered a worldwide cyberattack dubbed "Red October," that had been operating since at least 2007. Even though there is no evidence linking this with a nation-state sponsored attack, the campaign appears at the least to be an example of strategic economic or political reconnaissance and espionage. The true identity of the perpetrators has not been definitively determined since the component and connector (C&C) architecture is arranged to hide the mothership server through proxy functionality of every node in the malicious structure. The exploits appear to point to Chinese hackers, although many believe the perpetrators are members of the Russian Business Network (RBN), who are comfortable using Chinese malware and adapting it for their own use.[4] According to the Kaspersky Labs report, RBN is believed to have had a working relationship with the Russian government.[5]

The hackers gathered information through vulnerabilities in Microsoft's Word and Excel programs and obtained a huge quantity of information such as service credentials that were reused in later attacks. The primary targets of the attacks appeared to be countries in Eastern Europe, the former Union of Soviet Socialist Republics, and Central Asia, although Western Europe

and North America reported victims as well. The virus collected information from governments, embassies, research firms, trade and commerce, aerospace, military installations, energy providers, nuclear installations, and other critical infrastructures.[6] The information stolen by the attackers was of the "highest level" and included geopolitical data that could be used by nation-states or could be traded in the underground and sold to the highest bidder.[7] See Figure 20-2.

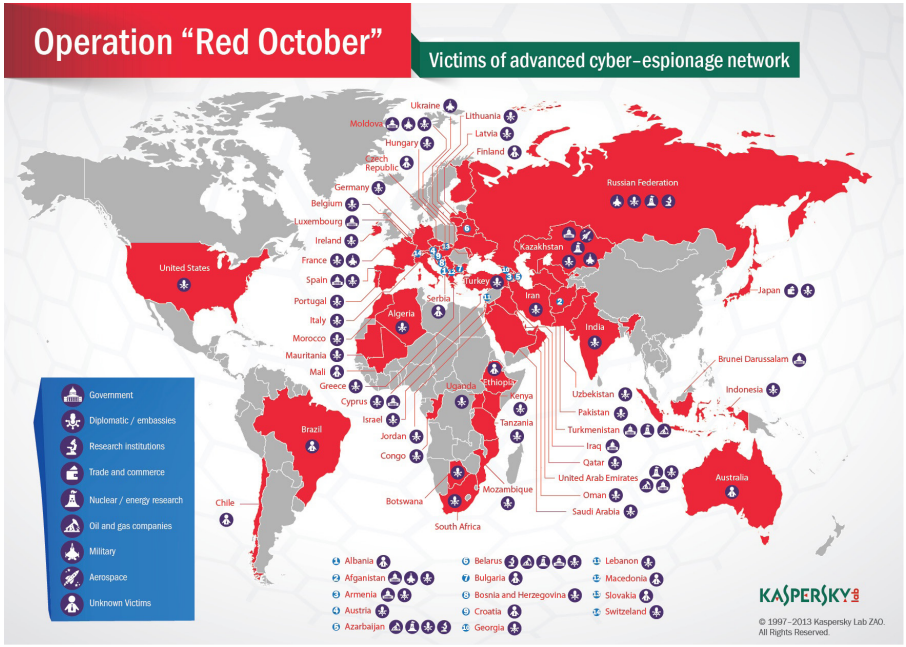


Figure 20-2. Operation Red October: Cyberespionage Campaign against Many Governments.[8]

National-Cyber Domain (Center Top Square).

China.

As Timothy Thomas discussed in Chapter 7 in this volume ("China's Reconnaissance and System Sabotage Activities"), the Chinese aggressively probe and enter global networks not only to gain an advantage in economic matters, business, military, and political bargaining but also for strategic reasons: to "win victory before the first battle" by mapping the opponent's digital terrain. Most of their behavior is driven by three beliefs: The United States maintains hegemonic power over global cyberspace; Information superiority is a key component of national power; China will be at a strategic disadvantage in any conflict with the United States (and its allies) unless it can take steps to neutralize U.S. superiority.

Strategic digital reconnaissance comes not only from all of the cyberactivities the Chinese conduct but also from activities specifically targeted and directed for such purposes to provide knowledge of the digital landscape, or virtual *shi,* to allow more effective offensive and defensive activities, if needed. Active offense (system sabotage) is the Chinese preferred strategy for winning a cyberconflict. In such an offensive move, the Chinese will seek to damage or disrupt the material and technical foundations of the opponent's cybersystems, making it impossible to adjust to problems on the battlefield. Strategic digital reconnaissance provides the knowledge of where are those critical nodes to be destroyed. By controlling information, the opponent essentially is left in the dark about what is going on and is hindered and limited in what it can do, making it impossible to turn war potential into actual capabilities for engaging in war.

Chinese strategic thought does not foresee information deterrence acting alone. On the contrary, nuclear deterrence capabilities, conventional deterrence, space deterrence, and information deterrence provide a "cocktail" for use in future conflicts.

Russia.

Much like China, Russia, as illustrated by Stephen Blank (in Chapter 8, "Information Warfare A La Russe" in this volume), views cyberspace strategically. The Russian experience in Estonia and in Georgia, not to mention the other probes that have taken place against Eurasian governments from Ukraine to Kyrgyzstan, indicate that Moscow is thinking about what U.S. analysts have called strategic information war to achieve victory by paralyzing a target country's social infrastructure networks, i.e., what might be called its central nervous system.

The elements that make up this strategy are cyberwar, economic sanctions, a domestic and international public information campaign, the manipulation of youth organizations or gangs, and the ongoing Russian efforts to penetrate key sectors of the target economy and subvert politicians through connections with the energy industry or intelligence penetration. In effect, cyberspace becomes a surrogate for large-scale military capabilities that are unavailable or simply not usable.

The attacks on Estonian socio-economic and political institutions were allegedly the reaction to Estonian authorities' transferal of the site of a monument—the Bronze Soldier of Soviet liberators of Estonia from the Nazis—in Tallinn to another site. In fact, the computer attacks and the other steps taken by Moscow against

Estonia reflected a coordinated strategy that was devised in advance of the removal of the Bronze Soldier from its original pedestal. Moreover, in Estonia and in subsequent manifestations of cyberspace operations, the Russian government cooperates with organized crime structures like the RBN to launch these attacks. While it is currently not possible to prove that RBN—before its disappearance—worked in tandem with the Russian Secret Police or other security services, it is likely that they were at least connected. It is also likely that the Russian leadership was well aware of the capabilities RBN offered and utilized them to assist in achieving international Russian strategic objectives.[9]

In Georgia, we see for the first time an attempt to attack military forces' command-and-control and weapons systems on the one hand, and information-psychological attacks against media, communications, and perceptions on the other. The plan of attack dated back, at least, to 2006.[10] Most attacks actually were carried out by civilians with little or no direct (or certainly traceable) involvement by the Russian government or military. But these organizers of cyberattacks were being recruited through the Internet and social technology, were aided by Russian organized crime even to the point of hosting software ready for use, probably had advance notice of Russian military intentions, and were tipped off about the timing of Russian military operations while they were taking place.[11]

United States.

Stuxnet, the computer malware designed to attack Iran's nuclear facilities, was initially discovered in June 2010 and is generally attributed to the United States and Israel. The worm includes a highly special-

ized malware payload designed to target only Siemens supervisory control and data acquisition (SCADA) systems that are configured to control and monitor specific industrial processes. It subsequently almost ruined one-fifth of the Iranian nuclear centrifuges by causing them to spin out of control while simultaneously replaying the recorded system values which showed the normal functioning centrifuge values during the attack. According to *The Washington Post*, International Atomic Energy Agency (IAEA) cameras installed in the Natanz facility recorded the sudden dismantling and removal of approximately 900–1,000 centrifuges during the time the Stuxnet worm was reportedly active at the plant.[12]

Unlike most malware, Stuxnet does little harm to computers and networks that do not meet specific configuration requirements; "The attackers took great care to make sure that only their designated targets were hit. . . . It was a marksman's job."[13] This is not surprising. Experts believe that Stuxnet required the largest and costliest development effort in malware history. Developing its many capabilities would have required a team of highly capable programmers, in-depth knowledge of industrial processes, and an interest in attacking industrial infrastructure. *The Guardian*, the BBC, and *The New York Times* all claimed that (unnamed) experts studying Stuxnet believe the complexity of the code indicated that only a nation-state would have the capabilities to produce it.[14]

Individual-Cyber Domain (Right top square).

Anonymous-Chris Forcand.

The arrest of Chris Forcand illustrates one of the first examples of cybervigilantism (the term "diligantism" has been coined to describe this type of activity) for individual personal physical security/safety (upper right square). On December 7, 2007, alleged Internet predator Chris Forcand, aged 53, was charged with two counts of luring a child under the age of 14, attempting to invite sexual touching, attempted exposure, possessing a dangerous weapon, and carrying a concealed weapon. Cybervigilantes from Anonymous who seek to out anyone with "a sexual interest in children" tracked Forcand and contacted the police after he propositioned some of their members with "disgusting photos of himself." Sexually explicit conversations were then forwarded to Forcand's church and a blog he wrote at praize.com, and his name, address, and phone number were posted online.[15] Reportedly, this was also the first time a suspected Internet predator was arrested by the police as a result of Internet vigilantism.[16]

Bit (Crypto) Currency 2013-14.

At the end of 2013 and into 2014, several crypto currency exchanges saw their repositories of the legitimate legal tender used to purchase the crypto currency significantly reduced or depleted with losses of hundreds of millions of dollars: Pony Botnet ($220,000), Mt. Gox ($500,000), Silk Road 2 ($2.7 million), Sheep Marketplace ($56.4 million), Silk Road ($127.4 million), and Mt. Gox ($436 million). Most of these thefts

appear to have been committed by "insiders" (those responsible for maintaining or administering the exchanges).[17] Users "responded with anger . . . and threats. But Bitcoin being Bitcoin, the money was lost and gone forever."[18]

The crypto currency thefts and near collapse highlighted a case in which actions in cyberspace led to cyberindividuals and voluntary collectives both identifying activity and the individual(s) violating generally accepted norms of accountability. Identifying those responsible for the losses exposed them to possible physical security or economic loss, most likely through vigilantism since the traditional levels of governance were still lagging behind in their efforts to regulate digital currency. Indeed, the appeal of this crypto currency was that it was "outside" the normal governance of regulated currency and economic commerce operating on the World Wide Web's "Deep Web," (DarkNet, or TOR) network, thereby allowing people to make one-to-one transactions, buy goods and services, and exchange money across borders without involving banks, credit card issuers, or other third parties. To some extent, however, this has changed as governments have started to impose some regulations on a space that had initially been unregulated.

PHYSICAL SPHERE

Global-Physical Domain (Left bottom square).

The global-physical domain is not an unusual arena of action within international security. States ostensibly collaborate to enforce accepted global norms (generally also in their individual state's inter-

est). Although primarily physical, instruments of the cyberdimensions of national power are increasingly being used in conjunction with instruments of the military dimension of national power.

National-Physical Domain (Center bottom square).

This represents the usual realist notion of national security; a state acting for no other reason than in its own self-interest generally employs the military dimension of national power. The U.S. intervention in Afghanistan in 2001 is an example of behavior in this arena of action.

Individual-Physical Domain (Right bottom square).

Humans living in uncertain locales desiring physical safety and the basic necessities of every-day life seem to be turning to anyone who can provide security, whether they are state or nonstate armed groups.

Michoacán Vigilantism.

The situation in Michoacán, Mexico, (as well as most under-governed spaces) seems to substantiate this observation. When authorities there could not or would not provide safety for the populace, self-defense groups (vigilantes) emerged hoping to drive the Knights Templar drug cartel (which ran an extensive extortion racket and had come to control a number of local governments, as well as much of the agricultural business in the region) out of Michoacán.

In late January 2014, the Mexican federal government sent troops and federal police to the region after the vigilantes began seizing control of communities

around a key Knights Templar stronghold, and openly declaring their intention to attack the organization's members there. The situation calmed with the arrival of the troops and officers, who controlled 27 of Michoacán's 113 municipalities. Federal authorities detained more than 1,200 local police and subjected them to tests to determine their trustworthiness since many locals suspected their local police of being enforcers for the cartel. Though federal authorities demanded the vigilantes lay down their arms, they continued to sport assault rifles and other weapons at roadblocks outside the towns they had seized; there were some early standoffs between government forces and vigilante groups over the demand that they disarm, but they later appeared to be cooperating in some parts of the state.[19]

Failed States and Feral Cities.

As in Michoacán, residents of failed states and feral cities look to whoever can provide some order to their everyday lives, be it the recognized and formal level of governance, or what Jeff Boleng and Colin Clarke (in Chapter 5, "Big Data Challenges, Failed Cities, and the Rise of the New 'Net," in this volume) call terrorists, insurgents, militias, warlords, transnational criminal organizations, and violent drug trafficking organizations. As Kelsey Ida noted (in Chapter 16, "The Age of E-Superheroes?" in this volume), the lack of a single coercive actor with Weberian legitimate monopoly on the use of force creates the conditions that lead to alternative forms of governance. Those who cannot afford to pay for security grudgingly will accept their personal security from wherever they can get it. In the end, these inhabitants are only seeking some level of physical security in the lives.

Anonymous-Zetas.

Ida provides evidence of a global collective (Anonymous) using the cybersphere to compete with a physical threat to one of its members. In October 2011, following the kidnapping of an Anonymous member residing in the state of Veracruz, Mexico, Anonymous threatened to publicize online the personal information of Los Zetas and their associates unless Los Zetas freed their kidnapped member by November 5. Despite attempts at "reverse hacking" and death threats sent to Anonymous members, Los Zetas released the kidnapped member on November 4. Admittedly, they only did so with a warning to Anonymous that they would execute 10 people for each name that Anonymous might publicize, but what is significant here is that Los Zetas "blinked" first.

Notable here, too, is that Anonymous (through a local branch in Acuña) has since re-engaged Los Zetas, publishing photos of known cartel properties online, with little retribution thus far. Kan (in Ida's chapter in this volume) warns the group to take care with their activities. By choosing to "out" the various parts of their "organizational infrastructure," Anonymous has once more struck at Los Zetas' "criminal brand," and Los Zetas are likely to respond in kind. However, here again, the digilantes—with notable public support[20]—have engaged organized crime even beyond state enforcement.

RESPONSE TO CYBERTHREATS

In the final analysis, security in cyberspace is not a narrow technical issue. Rather, it involves fundamental issues of politics and strategy and great power

relations, issues of global commerce and financial stability, and issues of personal privacy and the safety of personal information. Malevolence in cyberspace takes many forms, and there is no single response or overarching solution. But efforts can be made at a variety of levels to enhance both governance and security. The responses and recommendations in this volume are highly varied, ranging from increased use of big data, to cultural shifts about the nature of security in cyberspace, to digilantism and the reliance on nonstate actors to police the system. At the end of the day, all these components have their place. Cyberspace is best understood as an emergent and evolving system; efforts to enhance both governance and security in cyberspace need to be understood in the same light. There are no definitive and final responses: Governance and security initiatives in cyberspace need to be both top-down (state) and bottom-up (individual and group), to combine short-term palliatives and long-term goals, and to be as dynamic, responsive, and adaptable as cyberspace itself.

ENDNOTES - CHAPTER 20

1. "Operation Darknet: Part of a series on Anonymous," available from *knowyourmeme.com/memes/events/operation-darknet*, accessed on February 16, 2014.

2. *Ibid*.

3. *Ibid*.

4. The exploits appear to have been created by Chinese hackers, but Russian-speaking operatives have created the Rocra malware modules. "Based on registration data of the component and connector (C&C) servers and numerous artifacts left in executables of the malware, we strongly believe that the attackers have Russian-speaking origins," said the (Kaspersky) report. Dan

Holden, "Global Espionage Network Hacks Computers, Smart Phones," SV411.com, available from *sv411.com/index.php/2013/01/global-espionage-network-hacks-computers-smart-phones*, accessed on July 4, 2014.

5. Pierluigi Paganini, "Operation Red October: Cyber Espionage Campaign Against Many Governments," The Hacker News, January 14, 2013, available from *thehackernews.com /2013/01/operation-red-october-cyber-espionage.html*, accessed on July 4, 2014.

6. "Cyber—the good, the bad and the bug-free: The history of cyber attacks—a timeline," *NATO Review Magazine*, available from *nato.int/docu/review/2013/Cyber/EN/index.htm,* accessed on July 4, 2014; and Paganini.

7. Holden.

8. Paganini.

9. Dighton Fiddner, "National Cyber Security Strategy Against Malevolent Use of the Global Cyberspace," paper presented at the World International Studies Committee 3rd Global International Studies conference, "The World in Crisis: Revolution or Evolution in the International Community?" Porto, Portugal, University of Porto, August 17-20, 2011.

10. Putin has admitted that the war in 2008 with Georgia was planned by Moscow from 2006. Attacks were planned in advance and, at least, somewhat coordinated; Russian-language forums were full of the preparations and planning in the days leading up to the attacks. A concise description of the attacks may be found in Rebecca Grant, *Victory in Cyberspace*, Washington, DC: U.S. Air Force Association, p. 39; and Stephen Blank, Chapter 8, "Information Warfare A La Russe," in this volume.

11. Lack of reconnaissance or mapping of sites and directly attacking them signifies a prior deep intelligence penetration by the Russians of the Georgian networks. Similarly, Jeff Carr, an investigator for Project Grey Goose concluded, "the level of advance preparation and reconnaissance strongly suggests that Russian hackers were primed for the assault by officials within the Russian government." Blank, "Information Warfare A La Russe."

12. Wikipedia, "Stuxnet: Natanz nuclear facilities," available from *en.wikipedia.org/wiki/Stuxnet*, accessed on March 31, 2014.

13. William J. Broad, John Markoff, and David E. Sanger, "Israel Tests on Worm Called Crucial in Iran Nuclear Delay," *The New York Times*, January 16, 2011, p. A1.

14. Wikipedia, "Stuxnet: Target and origin," available from *en.wikipedia.org/wiki/Stuxnet*.

15. Jonathan Jenkins, "Man trolled the web for girls: cops," available from *cnews.canoe.com/CNEWS/Crime/2007/12/07/4712680-sun.html*, accessed on February 17, 2014.

16. Ian Fortey, "Vigilantism: #1. Chris Forcand vs. Anonymous," available from *cracked.com/article_17170_8-awesome-cases-internet-vigilantism_p2.html*, accessed on June 25, 2015.

17. "History of Bitcoin: The World's First Decentralized Currency," available from *historyofbitcoin.org/*, accessed on March 7, 2014.

18. Comments of DefCon, administrator of Silk Road, exchange after the 2nd theft of Silk Road:

> This community has suffered great financial loss over and over again. . . . All three users who have exploited this vulnerability are very much at risk until they approach us directly to assist with any information. . . . Stop at nothing to bring this person to your own definition of justice.

See "List of Bitcoin Heist: Silk Road 2 Incident: Official signed statement from 'Defcon,' operator of Silk Road 2: SR has been HACKED!" available from *reddit.com/r/DarkNetMarkets/comments/1xtqty/sr_has_been_hacked/*, accessed on June, 27, 2015.

19. Richard Fausset "Mexican vigilante groups refuse to lay down arms in Michoacan," *The Los Angeles Times*, available from *latimes.com/world/worldnow/la-fg-wn-mexico-vigilante-groups-michoacan-20140120-story.html,* accessed on April 11, 2016.

20. A spokesperson of the local branch, Anonymous FreeAcuña, reported that the organization is collecting "hundreds of pieces of information" from sources across the area, implying a broad public support. See Paul Kan in Ida's chapter in this volume.

ABOUT THE CONTRIBUTORS

STEPHEN J. BLANK is a Senior Fellow at the American Foreign Policy Council in Washington, DC. From 1989-2013, he was a Professor of Russian National Security Studies and Professor of National Security Affairs at the Strategic Studies Institute (SSI) of the U.S. Army War College (USAWC) in Carlisle, PA. From 1998-2001 he was also Douglas MacArthur Professor of Research at the USAWC. From 1980-86 Dr. Blank was Associate Professor for Soviet Studies at the Center for Aerospace Doctrine, Research, and Education of Air University at Maxwell AFB, and Assistant Professor of Russian History, University of Texas, San Antonio, TX. From 1979-80 he was a Visiting Assistant Professor of Russian history, University of California, Riverside, CA.

Dr. Blank has published over 1,000 articles and monographs on Soviet/Russian, U.S., Asian, and European military and foreign policies; testified frequently before Congress on Russia, China, and Central Asia; consulted for the Central Intelligence Agency, major think tanks and foundations; chaired major international conferences in the United States and abroad; and has served as a commentator on foreign affairs in the media in the United States and abroad. He has also advised major corporations on investing in Russia and is a consultant for the Gerson Lehrman Group.

Dr. Blank authored or edited 15 books focusing on Russian foreign, energy, and military policies and on International Security in Eurasia. His most recent book was *Russo-Chinese Energy Relations: Politics in Command* (London, UK: Global Markets Briefing, 2006). He has also authored *Natural Allies? Regional Security in Asia and Prospects for Indo-American Stra-*

tegic Cooperation (Carlisle, PA: Strategic Studies Institute, U.S. Army War College, 2005); *The Sorcerer as Apprentice: Stalin's Commissariat of Nationalities* (Santa Barbara, CA: Greenwood Publishing Group, 1994); and co-edited *The Soviet Military and the Future* (Santa Barbara, CA: Greenwood Publishing Group, 1992). He is currently writing *Light From the East: Russia's Quest for Great Power Status in Asia* (Farnum, Surrey, UK: Ashgate Publishers, forthcoming 2016).

Dr. Blank holds a B.A. in history from the University of Pennsylvania and an M.A. and Ph.D. in Russian history from the University of Chicago.

DAVIS B. BOBROW is Professor Emeritus of Public and International Affairs, University of Pittsburgh. He has been a member of the Defense Science Board and the Science and Technology Advisory Panel to the Director of Central Intelligence, and president of the International Studies Association. Dr. Bobrow co-authored with Mark Boyer, *Defensive Internationalism: Providing Public Goods in an Uncertain World* (Ann Arbor, MI: University of Michigan Press, 2005); and he edited and co-authored *Hegemony Constrained: Evasion, Modification, and Resistance to American Foreign Policy* (Pittsburgh, PA: University of Pittsburgh Press, 2008).

Dr. Bobrow holds degrees from Oxford University and the University of Chicago, and a Ph.D. from the Massachusetts Institute of Technology.

JEFF BOLENG is a Principal Researcher on the Advanced Mobile Systems team. His interests and experience span a wide gamut of computer science from network protocols, operating systems, distributed computation, and embedded systems to numerical

analysis, scientific computing, parallel processing, and concurrency. He is currently focused on innovative applications of advanced technologies to aid the safety and effectiveness of tactical soldiers at the edge.

Dr. Boleng joined the Software Engineering Institute (SEI) at Carnegie Mellon University in 2012 after 21 years of service as an active duty cyber operations officer in the U.S. Air Force. During his service, he was a member of the computer science faculty at the U.S. Air Force Academy for 8 years. He was honored with the Outstanding Academy Educator in Computer Science award for academic year 2007-08. He has operational Air Force experience as a deployed network engineer with the 1st Combat Communications Squadron where he deployed in support of the Bosnian War; leading an Intelligence software development team in U.S. Air Forces Europe; leading the command-and-control interoperability efforts for U.S. Forces Korea; and leading the net-centric integration efforts in the Air Force Space Command. Additionally, he served as a Flight Commander and Chief of Maintenance in the 21st Space Communications Squadron and he commanded the 21st Mission Support Squadron at Peterson Air Force Base, CO. In 2010, he deployed to Kabul, Afghanistan, in support of Operation ENDURING FREEDOM as a mentor to the Computer Science Department Head at the National Military Academy of Afghanistan and a member of the International Security Assistance Force.

JEFFREY L. CARASITI was the recipient of the 2014 Matthew B. Ridgway Center for International Security Studies Fellowship and has interned at the center, as well as at the James Martin Center for Nonproliferation Studies at the Middlebury Institute of Internation-

al Studies at Monterey, CA. His current interests are in East Asian security and transborder or borderless crimes and issues: organized crime and cybercrime, weapons of mass destruction proliferation, outer space policy, and human trafficking. Mr. Carasiti has coauthored an article on network analysis for the *McGill Sociological Review*, titled "Evaluating Knowledge Production Systems in Security Studies and Health Sciences: Citation Network Analysis."

Mr. Carasiti holds an M.P.I.A., with a major in in security and intelligence studies from the University of Pittsburgh and a M.I.S. from Japan's Kobe University, with a thesis on regional space technology rivalries.

NAZLI CHOUCRI is a professor of political science at the Massachusetts Institute of Technology (MIT), Cambridge, MA. Her work is in the area of international relations, most notably on sources and consequences of international conflict and violence. Dr. Choucri is the architect and Director of the Global System for Sustainable Development, a multilingual web-based knowledge networking system focusing on the multi-dimensionality of sustainability. As principal investigator of an MIT-Harvard multiyear project on Explorations in Cyber International Relations, she directed a multidisciplinary and multi-method research initiative. She is editor of the *MIT Press Series on Global Environmental Accord* and, formerly, general editor of the *International Political Science Review*. She also previously served as the associate director of MIT's Technology and Development Program. Dr. Choucri is a member of the European Academy of Sciences. She has been involved in research or advisory work for national and international agencies, and for a num-

ber of countries, notably Algeria, Canada, Colombia, Egypt, France, Germany, Greece, Honduras, Japan, Kuwait, Mexico, Pakistan, Qatar, Sudan, Switzerland, Syria, Tunisia, Turkey, the United Arab Emirates, and Yemen. She served two terms as President of the Scientific Advisory Committee of the United Nations Educational, Scientific and Cultural Organization, Management of Social Transformation Program. Dr. Choucri is the author of 11 books and over 120 articles.

COLIN P. CLARKE is an associate political scientist at the RAND Corporation, where his research focuses on insurgency/counterinsurgency, unconventional/irregular/asymmetric warfare (including cyber) and a range of other national and international security issues and challenges. From a methodological standpoint, he is interested in measurement, assessment, and evaluation, from tactical to strategic levels. At the Matthew B. Ridgway Center for International Security Studies, he is an affiliated scholar with research interests related to transnational terrorism and violent nonstate actors. He is also an adjunct professor at the University of Pittsburgh, where he teaches courses on international organized crime and threat finance. At Carnegie Mellon University, Mr. Clarke teaches contemporary comparative political systems and diplomacy and statecraft (with a focus on U.S. foreign and security policy and American grand strategy). In 2011, he spent 3 months embedded with Combined Joint Interagency Task Force (CJIATF) Shafafiyat in Kabul, Afghanistan, working on anti-corruption efforts and analyzing the nexus between terrorists, drug traffickers, and a range of political and economic power brokers. CJIATF Shafafiyat was commanded by Lieutenant General H. R. McMaster. Mr. Clarke recently

completed *Terrorism, Inc.: The Financing of Terrorism, Insurgency, and Irregular Warfare* (Santa Barbara, CA: Praeger Security International, 2015).

RONALD J. DEIBERT is a professor of political science and Director of the Citizen Lab at the Munk School of Global Affairs, University of Toronto. The Citizen Lab is an interdisciplinary research and development hothouse working at the intersection of the Internet, global security, and human rights. He was a co-founder and a principal investigator of the OpenNet Initiative (2003-14) and Information Warfare Monitor (2003-12) projects. Dr. Deibert was one of the founders and (former) vice president of global policy and outreach for Psiphon, Inc. He has been a consultant and advisor to governments, international organizations, and civil society/nongovernmental organizations on issues relating to cybersecurity, cybercrime, online free expression, and access to information. He presently serves on the editorial board of the journals *International Political Sociology, Security Dialogue, Explorations in Media Ecology, Review of Policy Research*, and *Astropolitics*. Dr. Deibert is on the advisory board of Access Now and Privacy International and is a member of the Steering Committee of the World Movement for Democracy.

Dr. Deibert has authored numerous articles, chapters, and books on issues related to technology, media, and world politics. Dr. Deibert was one of the authors of the "Tracking Ghostnet" report that documented an alleged cyberespionage network affecting over 1,200 computers in 103 countries, and the "Shadows in the Cloud" report, which analyzed a cloud-based espionage network. He co-edited three major volumes with the MIT Press: *Access Denied: The practice and policy of Internet Filtering* (2008); *Access Controlled: The shap-*

ing of power, rights, and rule in cyberspace (2010); and *Access Contested: Security, Identity, and Resistance in Asian Cyberspace* (2011). He is the author of *Parchment, Printing, and Hypermedia: Communications in World Order Transformation* (New York: Columbia University Press, 1997); and *Black Code: Inside the Battle for Cyberspace* (Signal/McClelland & Stewart/Random House, 2013).

Dr. Deibert was awarded the Order of Ontario, and holds a Ph.D. from the University of British Columbia.

CHRIS C. DEMCHAK is the Rear Admiral Grace M. Hopper Professor of Cyber Security and Co-Director, Center for Cyber Conflict Studies (C3S), Strategic Research Department, U.S. Naval War College. Her research and many publications address global cyberspace's influences from a rising "Cyber-Westphalia" to the security of complex socio-technical-economic systems as globally shared, insecure substrates penetrating throughout the critical organizations of digitized democratic civil societies. Dr. Demchak takes a systemic approach in focusing on emergent structural changes, comparative operational institutional learning, adversary/defensive use of systemic cybered tools, the use of virtual worlds for operationalized organizational learning, and designing systemic resilience against normal or adversary imposed complex systems surprise. She has taught international security studies, comparative organization theory, international management, enterprise information systems, and currently systemic cyber and international/national security structures. Dr. Demchak co-edited *Designing Resilience* (2010); and authored *Wars of Disruption and Resilience: Cybered Conflict, Power, and National Security Conflicts* (2011). She is currently working on a manu-

script in production tentatively entitled *Cyber Westphalia: Organizing for Resilience and Cyber Security*.

Dr. Demchak holds degrees in engineering, economics, and comparative complex organization theory/political science.

DIGHTON FIDDNER is an assistant professor in the Department of Political Science at Indiana University of Pennsylvania. He currently teaches international relations, American foreign policy, and public policy courses. His interests also include national and international security policy, complexity, and the information system as a national security risk. Dr. Fiddner has hosted seven collaborative roundtables on cyberspace's role in national security. He has also presented his research on cybersecurity at four national and four international conferences. Prior to his academic career, Dr. Fiddner served in the U.S. Army, retiring as a lieutenant colonel in September 1988. During his military career, he worked on various national security issues. His career included service in the Office of the Secretary of Defense. In recent years, Dr. Fiddner has published numerous articles on cyberspace.

Dr. Fiddner holds a B.S. in psychology from Davidson College, an M.A. in political science from Kansas University, and a Ph.D. in political science from the School of Public and International Affairs at University of Pittsburgh.

SHAWN C. HOARD formerly worked as a private investigator. His current area of focus is the study of cybercrime and the methods by which criminals utilize computer technology to subvert outdated security measures. He is particularly interested in virtual currencies and the challenges and opportunities

they present to law enforcement and cybercriminals, respectively.

Mr. Hoard holds a B.A. in criminology and investigations, and an M.I.A. from the Graduate School of Public and International Affairs at the University of Pittsburgh, with a concentration in security and intelligence studies.

RICK HUTLEY is the Chief Executive Officer of StrataThought LLC., a global consulting firm that specializes in identifying technological trends and advising major corporations on their strategic opportunities. Mr. Hutley is also the Program Director and Clinical Professor of Analytics at the University of the Pacific. In this role, he is responsible for the 26-course Master of Science in Analytic program as well as the Executive Analytics Workshop program. Mr. Hutley is a highly seasoned information and communications technologist (ICT) with 28 years in the telecommunications/ information technology (IT) industry; a former chief information officer (CIO) of a global service provider; and 14 years of executive consulting experience to the C-suites of the largest corporations in the world as the vice president of innovation at Cisco Systems. For the last 5 years, he has been assisting major global corporations with their adoption of the Internet of Everything, including Big Data and Analytics. As vice president of Cisco Consulting Services, he was responsible for leading the rollout of technology-based business and IT solutions to enterprise and service provider customers globally. His work was focused on how the Internet of Everything will drive innovation and transform business operations and profitability over the next decade. Prior to joining Cisco, Mr. Hutley was chief information officer for British Telecom's Concert

Communications Company, a $1.5 billion global telecommunications service provider operating through 53 distributor companies around the world. As CIO, he was responsible for the development and operation of Concert's network and business management systems, including its intranet and extranet solutions for both Concert and their global partners. Prior to Concert, Mr. Hutley was director of information systems for Syncordia Corporation in Atlanta, GA, responsible for the development and operation of all systems for the first global telecommunications outsourcing company. He has appeared on BBC Television's series on computing and is a frequent speaker at industry conferences and seminars.

Mr. Hutley holds an honors degree in computer science from Hatfield University, UK, and an M.B.A. from Cranfield University, UK.

KELSEY IDA is currently consulting on an assessment of refugee needs and case-management services in Bulgaria. She previously worked with nonprofits in India to design and implement programs on ethnic conflict and gender. Her primary areas of interest are in social identity, migration, and transnational criminal justice.

Ms. Ida holds a B.A. in political science and philosophy from the University of Nebraska, an M.P.I.A. from the Graduate School of Public and International Affairs at the University of Pittsburgh, and an M.Sc. in global governance and diplomacy from Oxford University.

MICHAEL KENNEY is an associate professor and Program Director of International Affairs at the Graduate School of Public and International Affairs at the University of Pittsburgh. Dr. Kenney has published numerous articles on terrorism, Islamist militancy, and drug trafficking in *Orbis*, *Survival, Terrorism and Political Violence*, and *Studies in Conflict and Terrorism*, among other publications. He is also the author of *From Pablo to Osama: Trafficking and Terrorist Networks, Government Bureaucracies, and Competitive Adaptation* (Penn State University Press, 2006).

MARTIN LIBICKI has been a senior management scientist at RAND since 1998, a distinguished visiting professor at the Naval Academy since 2011, and an adjunct professor at Columbia University since 2014. Prior employment includes 12 years at the National Defense University, 3 years on the Navy Staff as program sponsor for industrial preparedness, and 3 years with the U.S. Government Accountability Office. He focuses on the impacts of information technology on domestic and national security. Dr. Libicki wrote two commercially published books: *Conquest in Cyberspace: National Security and Information Warfare* (Cambridge University Press, 2007); and *Information Technology Standards: Quest for the Common Byte* (Elsevier, 2016); as well as numerous monographs, notably *Crisis and Escalation in Cyberspace, Global Demographic Change and its Implications for Military Power, Cyberdeterrence and Cyberwar, How Insurgencies End* (with Ben Connable); *How Terrorist Groups End* (with Seth Jones); and (as editor) *New Challenges New Tools for Defense Decisionmaking*.

Dr. Libicki holds a master's degree in city planning and a Ph.D. from University of California at Berkeley.

EDWARD J. MASTEN was a Matthew B. Ridgway Center for International Security Studies Fellow. A former U.S. State Department intern, he has worked as a research analyst for a nonprofit cyberintelligence firm that collaborates with private industry and law enforcement agencies to counter cyberfinancial threats. His interests include energy security, extremism in the Caucasus, North Atlantic Treaty Organization affairs, and private military corporations.

Mr. Masten holds an M.P.I.A. in security and intelligence studies, with a regional specialization in Russian, Eastern European, and Eurasian affairs, from the University of Pittsburgh.

BENOÎT MOREL joined the faculty at Carnegie Mellon University in 1987 in the Department of Engineering and Public Policy, with the Program on International Peace and Security. At Carnegie Mellon, his research interests have focused on military high technology, its technical details and structure, and its impact on security and arms control, as well as its effects on American defense policy. His particular interest is cybersecurity policy and its international dimension. Dr. Morel is also interested in nonlinear dynamic models, and the study of complex systems and chaos, with application to a variety of areas, such as immunology, fluid mechanics, organization theory, economics, pollution, and environment. Dr. Morel has worked in physics at Harvard University as a postdoctoral fellow, at CERN (the European Organization for Nuclear Research), the University of Geneva, and at the California Institute of Technology. After attending Caltech, he went to Stanford as a Science Fellow in arms control. While there, he pursued research in the security implications and the technology of antiballistic missile defense.

Dr. Morel holds a Ph.D. from the University of Geneva in theoretical high energy physics.

ISAAC R. PORCHE, III is a senior engineer at the RAND Corporation and associate director of the RAND Arroyo Center's Forces and Logistics Program. His areas of expertise include cybersecurity; network and communication technology; intelligence, surveillance, and reconnaissance; information assurance; big data; cloud computing; and computer network defense. He has led research projects for the U.S. Navy, U.S. Army, the Department of Homeland Security, the Joint Staff, and the Office of the Secretary of Defense. He is a member of the U.S. Army Science Board, serving on the data-to-decisions panel. He has assessed collaboration and information-sharing issues, and modeling and simulation of tactical network communication technologies. For the Navy, he led the Analysis of Alternatives for both the Distributed Common Ground System-Navy and the Maritime Tactical Command and Control programs of record.

Dr. Porche has published articles in *Military Operations Research* on "The Impact of Networking on Warfighter Effectiveness" (2007) and "Game-Theoretic Methods for Analysis of Tactical Decision-Making Using Agent-Based Combat Simulations" (2009). His RAND publications include *Redefining Information Warfare* (Porche *et al*., 2012); *The Impact of Network Performance on Warfighter Effectiveness* (with Bradley Wilson, 2006); *Navy Network Dependability: Models, Metrics, and Tools* (Porche *et al*., 2010); and *Finding Services for an Open Architecture: A Review of Existing Applications and Programs in PEO C4I* (Porche *et al*., 2011).

Dr. Porche holds a Ph.D. in electrical engineering and computer science from the University of Michigan.

JOHN SCOTT-RAILTON has conducted applied work to support the free and open flow of information during Internet shutdowns in Egypt and Libya and researches threats to secure connectivity in similar contexts, including Syria. His doctoral work focuses on the human security implications of climate change and failures of climate change adaptation.

Mr. Railton is a doctoral student in the Department of Urban Planning, School of Public Affairs, University of California at Los Angeles and is a research fellow at the Citizen Lab at the University of Toronto.

TIMOTHY J. SHIMEALL is a senior member of the technical staff with the Computer Emergency Readiness Team (CERT) Program at the Software Engineering Institute (SEI). The CERT Coordination Center is also a part of this program, and his work draws heavily on data from there. Dr. Shimeall is responsible for overseeing and participating in the development of analysis methods in the area of network systems security and survivability. This work includes development of methods to identify trends in security incidents and in the development of software used by computer and network intruders. Of particular interest are incidents affecting defended systems and malicious software that are effective despite common defenses. Before joining the SEI, Dr. Shimeall was an associate professor at the Naval Postgraduate School in Monterey, CA. He was an active instructor on a variety of topics in software engineering, information warfare and security, and supervised in excess of 30 M.S. theses and three Ph.D. theses. He has taught courses for a variety of educational institutions and private corporations, in both local and distance learning formats. Dr. Shimeall's work has included theoretical studies

of the behavior of software faults; evaluation of testing methods; development, and implementation of tool sets for safety-critical software analysis; development of security policy and techniques; development of strategic frameworks for information warfare; and development of security evaluation methods for military systems.

Some of Dr. Shimeall's more than 30 reviewed technical publications include: "An Empirical Investigation of Six Software Error Detection Methods," *International Journal of Software Testing, Verification and Reliability*, May 2002, written with S. S. So, S. D. Cha, and K. R. Kwong; "Cyber Intelligence Analysis," *Contemporary Security Policy*, August 2002, written with C. Dunlevy and P. Williams; "Countering CyberWar" *NATO Review*, Winter 2001-02, written with C. Dunlevy and P. Williams; "Software Security in an Internet World: An Executive Summary," *IEEE Software*, July 1999, written with J. J. McDermott; "EASEL: Emergent Algorithm Simulation Environment Language," *Information Survivability Workshop*, Orlando FL, November 1998, written with D. Fisher; "Don't Waste Your Bugs," *Software Development*, March 1997, written with S.C. Shimeall; "A Matrix Model of Information Infrastructure in Expeditionary Warfare," *Asilomar Conference in Advanced Technology*, Pacific Grove, CA, December 1996, written with J. Arquilla; "Safety Verification of Ada Using Fault Tree Analysis," *IEEE Computer*, July 1991, with S. S. Cha and N. G. Leveson; and "An Empirical Comparison of Software Fault Tolerance and Fault Elimination," *IEEE Transactions on Software Engineering*, February 1991, with N. G. Leveson.

TIMOTHY L. THOMAS is a senior analyst at the Foreign Military Studies Office at Ft. Leavenworth, KS. He conducts extensive research and publishing in the areas of peacekeeping, information war, psychological operations, low intensity conflict, and political-military affairs. He is an adjunct professor at the U.S. Army's Eurasian Institute; an adjunct lecturer at the U.S. Air Force Special Operations School; and a member of two Russian organizations, the Academy of International Information and the Academy of Natural Sciences. Mr. Thomas was a U.S. Army foreign area officer who specialized in Soviet/Russian studies. His military assignments included serving as the Director of Soviet Studies at the U.S. Army Russian Institute in Garmisch, Germany; as an inspector of Soviet tactical operations under the Commission on Security and Cooperation in Europe; and as a brigade S-2 and company commander in the 82nd Airborne Division.
Mr. Thomas has written six books on information warfare topics, focusing on recent developments in China and Russia.

Mr. Thomas holds a B.S. in engineering science from the U.S. Military Academy, and an M.I.R. from the University of Southern California.

ROB VAN KRANENBURG is co-founder of Bricolabs and the founder of Council, *theinternetofthings.eu*. He currently works as Community Manager at the European Union Project Societal. Mr. van Kranenburg is consultant to IoT China, Shanghai 2014. He Chairs AC8-Societal Impact and Responsibility in the Context of IoT Applications of the Illinois Education Research Council, The European Research Cluster on the Internet of Things. He and Rasmus Blom have launched Council Global, the professional service arm of the Council think tank.

Together with Christian Nold, Mr. van Kranenburg published *Situated Technologies Pamphlets 8: The Internet of People for a Post-Oil World* (Architectural League, 2011). He is the author of *The Internet of Things: A critique of ambient technology and the all-seeing network of RFID,* Network Notebooks Series No. 02 Report for the Institute of Network Cultures (2008).

PHIL WILLIAMS holds the Wesley W. Posvar Chair in International Security Studies at the Graduate School of Public and International Affairs at the University of Pittsburgh and is the director of the University's Matthew B. Ridgway Center for International Security Studies. From 2007 to 2009, he was a visiting research professor at the Strategic Studies Institute (SSI), U.S. Army War College (USAWC). During the last 22 years, his research has focused primarily on transnational organized crime.

Dr. Williams has published extensively in the field of international security. He wrote two monographs for the USAWC—*The New Dark Age: The Decline of the State* and *U.S. Strategy and Criminals, Militias and Insurgents: Organized Crime in Iraq*. He has written on international security in *Survival*; *Washington Quarterly*; *The Bulletin on Narcotics*; *Scientific American*; *Crime, Law and Social Change*; and *International Peacekeeping*. In addition, Dr. Williams was founding editor of a journal entitled *Transnational Organized Crime* and edited several volumes on organized crime. Since then, Dr. Williams has published chapters and articles on terrorist networks and finances, the Madrid bombings, Mexican drug violence, Nigerian organized crime, and human trafficking. He is currently working on the crisis of governance in the northern triangle of Central America.

U.S. ARMY WAR COLLEGE

Major General William E. Rapp
Commandant

*****

STRATEGIC STUDIES INSTITUTE
and
U.S. ARMY WAR COLLEGE PRESS

Director
Professor Douglas C. Lovelace, Jr.

Director of Research
Dr. Steven K. Metz

Editors
Dr. Phil Williams
Dr. Dighton Fiddner

Editor for Production
Dr. James G. Pierce

Publications Assistant
Ms. Denise J. Kersting

*****

Composition
Mrs. Jennifer E. Nevil

Cover Artist
Shutterstock.com/Anton Balazh

Cover Designer
Ms. Aileen St. Leger

FOR THIS AND OTHER PUBLICATIONS, VISIT US AT
http://www.carlisle.army.mil/

U.S. ARMY WAR COLLEGE
SSI
STRATEGIC STUDIES INSTITUTE

Image by artist Anton Balazh under licensing agreement with Shutterstock.com.
Cover design by Aileen St. Leger.

ISBN 1-58487-726-X
9 781584 877264 90000>


This Publication


SSI Website


USAWC Website