Hudson Institute

Cyber-Enabled Economic Warfare: An Evolving Challenge

Edited by
Samantha F. Ravich, Ph.D.

August 2015
Research Report

Hudson Institute

Cyber-Enabled Economic Warfare: An Evolving Challenge

A Research Report Edited by
Samantha F. Ravich, Ph.D.

For more information about obtaining additional copies of this or other Hudson Institute publications, please visit Hudson's website, www.hudson.org

ABOUT HUDSON INSTITUTE

Hudson Institute is an independent research organization promoting new ideas for the advancement of global security, prosperity and freedom.

Founded in 1961 by strategist Herman Kahn, Hudson Institute challenges conventional thinking and helps manage strategic transitions to the future through interdisciplinary studies in defense, international relations, economics, health care, technology, culture, and law.

Hudson seeks to guide public policy makers and global leaders in government and business through a vigorous program of publications, conferences, policy briefings and recommendations.

Visit **www.hudson.org** for more information.

Hudson Institute
1015 15th Street, N.W.
Sixth Floor
Washington, D.C. 20005

P: 202.974.2400
info@hudson.org
www.hudson.org

TABLE OF CONTENTS

ACKNOWLEDGMENTS

It is always interesting to note how an intellectual pursuit moves from some random musings to more structured thought to an eventual written product that seeks to ask and answer the questions raised at the beginning. For this work, the origin goes back nearly twenty years ago to a discussion with Marin Strmecki of the Smith Richardson Foundation about the intersection of economics and national security. That conversation waxed and waned over the years but never really ended. Over the last few years, however, our discussion once again picked up in intensity as we noticed with alarm the increasing scale and scope of cyberattacks on financial and economic institutions around the world. Marin encouraged me to start thinking in a more structured way about cyber-enabled economic warfare and this project was born. The support of Marin, Nadia Schadlow, and the Smith Richardson Foundation was instrumental for this project's success.

My goal for this work was never to write the definitive text on cyber-enabled economic warfare. It was to help energize a much broader conversation about the threats the U.S. and our allies are now facing from a range of hostile actors seeking to undermine critical economic assets and systems in order to cause harm to a target state's security capabilities. I also hoped it would serve as a clarion call to energize the U.S. government to create both the strategy and the capabilities needed to confront this menace.

Each of the authors I recruited for this volume—Abe Shulsky, Mark Dubowitz, Annie Fixler, Michael Hsieh, Juan Zarate, and Tiffany Rad—bring a particular knowledge base to the problem set and I hope that each will use their chapter as a launching pad for continued work in the area. I thank each of them for their hard work, dedication to the topic, and forbearance with my questions, comments, and editorial process.

In addition, I thank Jeffrey Cooper, Drew Lomax, Doug Feith, Karen Evans, Terry Boston, Michael Madon, Michael Schrage, Charles Wolf, Kevin Gates, Lewis Libby, Ken Weinstein, Emily Goldman, Andrew May, Laurence Zuriff, and Chris Rodriguez for attending the working seminar at Hudson Institute where the other authors and I presented and defended our theses. The seminar participants were critical in helping us hone our thinking. I thank the fine people at Hudson Institute, including but not limited to Joel Scanlon, for shepherding this project from proposal to publication.

Finally, I thank my husband Richard Brahm, whose guidance and intellectual rigor helped make this work a reality.

Cyber-Enabled Economic Warfare: An Evolving Challenge

By Samantha F. Ravich

Project Rationale

Economic aggression against adversarial social groups is probably as old as societies' discoveries of economically productive activities: the economic success of some societies inevitably became intertwined with adversarial relations with others. As societies evolved and inevitably clashed, economic aggression tactics evolved as well. For example, historically notable blockades that were intended to cause economic harm include those imposed by the Athenians against the island of Aegina during the Peloponnesian War; by Fatimid Caliphate against the Kingdom of Jerusalem during the Crusader-Muslim wars; by French and Flemish nobles' against the island of Cadsand, which triggered the Hundred Years War; by Napoleon's "Continental System," which closed European ports to British trade in the early nineteenth century; and by the Soviet Union against Berlin at the start of the Cold War. Today there is a common arsenal for economic warfare consisting of many long established techniques to weaken an adversary through actions—some legal and some not—aimed at economic targets. Examples include trade embargoes, blacklists, blockades, sanctions, tariff and/or quota discrimination, sabotage of economic targets, preclusive purchase of scarce critical resources, freezing of capital assets, counterfeiting, suspension of aid, restrictions on investment and other capital flows, and expropriation. These practices are all well established, and a considerable body of literature exists on them as well.

It has also become increasingly common since the initial rise of European nations in the fifteenth and sixteenth centuries for individual nations to utilize economic warfare strategies as vital elements within their Great Power rivalries. England's attempt to weaken its rebellious American colonies by blockading their ports in the mid-eighteenth century is one example.[1] Napoleon's attempt to blockade British trade with Europe in the early nineteenth century, mentioned above, is another.[2] Germany and Great Britain each pursued sophisticated and complex economic warfare strategies during World War I.[3] Great Britain created a Ministry of Economic Warfare prior to World War II to help plan and implement its strategies leading up to, and during, the war.[4] The U.S. created a similar department prior to WWII,[5] implementing a multi-dimensional economic warfare strategy against the Japanese in particular.[6] Both the Soviet Union and the United States attempted to implement economic warfare strategies to weaken the other during the Cold War.[7]

With the advent in recent decades of the information age and its accompanying 'virtual' world of 'cyberspace,' something new has developed in the realm of economic warfare: the

potential for use of cyber-enabled attack methods to cause an adversary economic harm that is far disproportionate to the size or resources of the attacker. Examples of malicious cyber-enabled actions against economic targets include cybercrime (such as cyber fraud against banking and payment platforms), cyberespionage (such as trade secret and intellectual property theft), cybersabotage (such as the malware attack on the Saudi Aramco oil company in 2012), and cyberterrorism (attacks involving the convergence of cyberspace and terrorism that cause violence against persons or property and generate fear—so far mostly theoretical, although the recent North Korean sponsored cyberattack on Sony Pictures Entertainment began to cross that line with the threats that followed the attack). With the information technology revolution having already contributed to growth in annual U.S. gross domestic product by approximately two trillion dollars and with a high percentage of U.S. economic activity now dependent upon information technology and internet connectivity,[8] the potential economic stakes are quite high.

Numerous pieces of the puzzle have already received considerable attention. During the last few years, the U.S. government has reported on numerous large-scale cyber operations aimed at U.S. businesses, banks, and critical infrastructure.[9] General Keith Alexander of NSA/Cyber Command has described this hacking as the "greatest transfer of wealth in history."[10] FBI Director Robert Mueller testified in January 2012 that the "threats from cyberespionage, computer crime, and attacks on critical infrastructure will surpass terrorism as the number one threat facing the United States."[11] In October 2012, Defense Secretary Leon Panetta warned that the U.S. faces a rising threat of a "cyber-Pearl Harbor" from potential cyberattacks that could cripple portions of the nation's power grid, transportation system, financial networks, or government agencies.[12]

Accordingly, both traditional economic warfare[13] and, more recently, cyberwarfare[14] have been extensively studied. What is much less understood, however, is the intersection between these two subjects: *the contemporary evolution of economic warfare within the new realities of cyberspace has not received the focused, comprehensive scrutiny and policy attention that it warrants*. The rise of the global, electronically networked economy and the growing cross-border integration and interdependence of its constituent parts has produced sizable opportunities for various actors to develop new methods and strategies of economic warfare.[15] Both states and non-state actors increasingly can contemplate new possibilities for using pernicious cyber penetration of critical economic assets and systems in order to cause harm to a target state's security capabilities.[16] We label this new class of security threats "cyber-enabled economic warfare." Fleshing out the precise details of this construct and identifying its real world manifestations are among the principal objectives of this project.

It bears emphasizing that this class of security threats is relatively new.[17] Moreover, the interdependencies among the technological systems of global communications and computing, information flows, and economic infrastructures upon which the global economy rests, are themselves rapidly increasing and becoming more complex. These are among the central features of the 'cybered' world of the early twenty-first century, and they spawn the new opportunities for cyber-enabled economic warfare. However, the changing nature and rising amount of various forms of cybercrime, espionage, hacking, sabotage, etc., raises the questions: within the escalating cyberattacks on U.S. public and private organizations, is there lurking a new type of action— some form of concerted strategy to undermine the U.S. economically? What if some adversaries' strategies are designed to cause economic harm that would weaken or significantly debilitate U.S. security capabilities? Is the U.S. prepared to identify and address such strategies effectively?

The U.S. is currently at risk of being unprepared for the manner in which contemporary economic warfare is evolving. There is a new class of threats arising from emerging opportunities for cyber-enabled economic warfare. The threats are posed by both state and non-

state actors, though likely in different ways. But the U.S. homeland security system appears to be inadequately constructed or attuned at present to address the way these threats are evolving. The U.S. system for detecting, evaluating, and addressing cyber-enabled economic threats seems structurally inadequate and insufficiently focused on the matter. This raises concerns about the U.S.'s preparedness for identifying and responding to existing economic warfare threats and, even more so, about its ability to match the rate of their evolution.

One result is that the threat to the U.S. that these new opportunities pose is growing quickly without adequate attention from the research or policymaking communities. At best this is dangerous; at worst, it could prove disastrous. This project aims to help address this problem in a manner that will facilitate improved understanding of the fundamental issues; shine a light on where the U.S. seems most vulnerable and to attacks by whom; identify aspects of the problem in need of corrective policy responses and additional research; and promote communication about these matters within the relevant academic, research, and government communities.

Overview of Project

This project seeks to extend the understanding of one emerging dimension of contemporary economic warfare—the subset that is cyber-enabled. Its ambition is to help fill an important knowledge gap by examining cyber-enabled economic warfare in the context of broader adversarial strategy. The project is investigating five fundamental questions regarding the contemporary evolution of cyber-enabled economic warfare:

1) *How and why is the threat to the U.S. from economic warfare evolving*? Changes in the global economy are creating opportunities for new methods of cyber-enabled economic warfare. What are these new methods, and how do they differ from conventional methods of economic warfare? How are they evolving, and why? What U.S. vulnerabilities do they expose? How do the new, cyber-enabled methods link to more traditional methods of economic warfare?

2) *Which actors pose the main threat to the U.S.?* If it is, or could become, possible for a cyber-enabled economic warfare attack on the U.S. to succeed, which adversarial states or non-state actors could or would pursue such a strategy? Do these (would these) actors consider economic warfare a substitute for actual battle?; a precursor to armed conflict?; both? How robust are the capabilities of the states and actors that do, or could, have the intention to embark on economic warfare against the U.S.?

3) *What are the greatest vulnerabilities of the U.S to evolving economic warfare?* Since 9/11, the U.S. has made substantial investments in improved planning and enhanced capacity for emergency preparedness and homeland defense. But have these changes gone far enough to identify and counter the emerging new threats from economic warfare and to keep up with those threats as they evolve? What vulnerabilities do the new methods create in our critical infrastructure (CI)? In particular, how exposed are the primary systems necessary for maintaining the public's food and water supply (e.g. water and power utilities, and information technology and communications grid)? How exposed is the U.S. financial system?

4) *How can the USG recognize, monitor, deter, defend, and defeat such warfare?* What additional skill sets would the USG need to create to establish anticipatory intelligence, warning, and response capabilities against adversaries' acts of economic warfare? In what ways does the U.S. need to improve protection through multi-lateral actions (e.g. legal

reforms, better intelligence mechanisms, stronger deterrent and punitive capacities, etc.) in response to risks arising from economic interdependence with other nations?

5) *What policy reforms and further research are needed on the above topics?* What areas for policy reform seem to be priorities at present? How should such needs be addressed? Where is further research needed on any or all of the above topics?

The project is designed to address these questions in phases. Phase one occurred during June – November 2014 and entailed commissioning a group of experts to research and write papers on designated aspects of cyber-enabled economic warfare. The authors then presented their drafts at a full day seminar graciously hosted by Hudson Institute in Washington DC in November 2014. The papers were discussed there by the presenters and other leading experts to consider opportunities to improve the drafts, evaluate potential policy responses to the problems they identified, and develop topics most in need of further research.

Phase two of the project lasted from December 2014 until March 2015. The authors of the seminar papers revised their drafts in light of feedback from the participants and the project's principal investigator, Samantha Ravich. Ravich then integrated the five papers into the current monograph and added both this introduction and a concluding chapter. Hudson Institute then prepared the final copy of the monograph and printed it.

The remainder of this project involves the continued socialization of the work throughout the policy making community as well as follow-on work in the service of building a greater body of knowledge about the topic and the capabilities needed to secure and safeguard the country from this growing threat.

Overview of the Monograph

This monograph is divided into six chapters: one dissecting the U.S.'s use of cyber-enabled economic warfare; two providing analyses of cyber-enabled economic warfare threats posed to the United States by state and non-state actors; two offering case studies of emerging cyber-enabled economic warfare in two key sectors, financial services and critical infrastructure; and a concluding chapter that reviews key takeaways and next steps.

Chapter 1 was written by Mark Dubowitz and Annie Fixler and is titled "Cyber-Enabled 'Swift' Warfare: Power, Blowback, and Hardening American Defenses." The chapter addresses the U.S. practice of cyber-enabled economic warfare. However, it is not a broad review of all major aspects of this subject, including for example prior U.S. history and lessons learned with traditional economic warfare; U.S. defensive strategy for protecting against threats from adversaries' use of cyber-enabled economic warfare; or U.S. clandestine cyber-enabled economic warfare capabilities and operations. Rather it describes one of the United States' most important *offensive* programs for conducting cyber-enabled economic warfare—although the program is seldom so labeled.

Dubowitz and Fixler provide a revealing analysis of how the U.S. Treasury Department's "smart sanctions" regime has developed during the past dozen years into a powerful "instrument of coercive statecraft" against international rogue actors—"from the terrorists and nuclear proliferators of Iran's Revolutionary Guards to Sunni jihadists to Russian arms dealers and oligarchs."[18] They describe the origins of the current financial sanctions regime in the U.S.'s history of broad embargos of limited efficacy, and its transformation by Treasury after the 9/11 attacks into today's highly effective national security weapon. The critical change that enabled Treasury's campaign was the international establishment of the SWIFT (Society for Worldwide Interbank Financial Telecommunication) financial messaging system as the "electronic bloodstream of the global financial system."[19] Dubowitz and Fixler explain why expulsion from the SWIFT system is such a powerful instrument, and how the United States successfully

employed it against Iran in a particularly important case. Finally, the authors offer exceptional insights into the risks of potentially very damaging blowback from Treasury's "de-Swifting" program, and conclude their paper with recommendations for improving U.S. policy in this regard.

In chapter 2, "Cyber-Enabled Economic Warfare and State Actors," Abe Shulsky steps back from the particulars of the Dubowitz and Fixler financial sanctions study and provides a broad overview of how cyber-enabled economic warfare has arisen in the past two decades and how it presents a host of new challenges, even in times of relative peace, to U.S. national security. He focuses on "the threat to the U.S. posed by the possible use of economic warfare means by state adversaries."[20]

Shulsky begins by explaining key terms such as "economic warfare," and then gives brief summaries of numerous traditional economic warfare methods. He offers a provocative discussion of how to determine when the use of such methods rises above "economic competition" and actually constitutes an intended strategy of "economic warfare," properly speaking. This is a problem at the core of this monograph because, while it is widely recognized that many U.S. adversaries are engaged in various types of serious economic "cyberattacks" on U.S. targets, there is very little discussion, much less consensus, on which attacks actually constitute, either individually or in concert with other hostile acts, economic warfare against the United States. Shulsky goes on to explore the possible threats of economic warfare posed to the U.S. by leading adversarial states, including China, Russia, Iran and North Korea.

In the final sections of his chapter, Shulsky examines new opportunities for conducting cyber-enabled, rather than traditional, economic warfare, and explores how global interconnectedness in cyberspace is producing a new calculus of economic warfare among states. He reviews four settings where the threat to the U.S. is particularly troubling and concludes with a number of suggestions for policy improvements and future research.

In chapter 3, "Intellectual Property Piracy as Economic Privateers," Michael Hsieh provides a highly original response to one of the most vexing challenges to a pillar of American power and national security: intellectual property protection. Numerous studies and government reports have established the harm being done to the U.S. economy, and ultimately to U.S. power, through massive theft of U.S. intellectual property assets. Much of this piracy occurs through cyber-theft of one form or another; both firms and the U.S. government have struggled to devise adequate protection.

Hsieh approaches the problem in a fascinating way. First, he takes us through a quick case study of the UK's analogous difficulty, and ultimate inability, to protect the intellectual property assets underlying its economic preeminance during the Industrial Revolution and afterwards. Ironically for readers of this monograph, it was U.S. rivals – state and non-state actors – who most successfully engaged in "the unlawful, large-scale extraction of intellectual property (IP) to increase the productive capacity of the home economy while freeriding on the research and development investments of the target economy."[21] Hsieh uses the UK case to illuminate core difficulties for the U.S.'s attempts to protect its vital intellectual property interests today. In particular, he shows how challenger nations can adopt a form of economic warfare by deliberately fostering conditions that encourage private, non-state actors to engage in intellectual property piracy and thereby become "economic privateers" in service of both themselves and the challenger nations that encourage them.

Hsieh provides convincing parallels between the UK's challenge in a prior era and the U.S.'s conundrum and inadequate preventative measures today. In particular, he relates how "the revolution in information and cyber technologies has profoundly empowered IP thieves by giving them tools with latencies, scope and cost undreamt of before now."[22] He then argues that

radical breakthroughs already on the horizon may soon make it possible to use technology and "techno-economic" strategy, rather than simply legal and diplomatic action, as a means to change the economics of IP piracy in ways sure to reverse the current attackers' advantages by raising the "technical difficulty of IP theft … to sufficiently high levels that it no longer becomes a cost-effective activity."[23] His is an argument that merits considerable attention in U.S. policy circles.

Chapter 4 was written by Juan C. Zarate and is entitled, "The Cyber Financial Wars on the Horizon: The Convergence of Financial and Cyber Warfare and the Need for a 21st Century National Security Response." As the individual perhaps most responsible for the Treasury Department's "de-Swifting," the smart sanctions campaign described by Dubowitz and Fixler in chapter 1, Zarate is intimately familiar with the offensive "financial war" the United States has been waging against terrorism and rogue regimes. In this chapter, he turns his attention to the flip side of the coin and provides a very thorough and disturbing account of the rapidly evolving cyber war that adversarial state and non-state actors are ramping up against the U.S. financial system and especially its core constituent, U.S. banks.

Zarate contends that "nation states unable to compete in open markets are increasingly turning to illicit tools for financial gain" while using "shadow proxy forces to do the dirty work"[24] through hacking, cyberespionage, cyber fraud, massive data theft, and the like, with U.S. banks as their principal target. Banks not only are repositories for vast financial assets, but "nation states and their proxies realize that banks serve as both key systemic actors important for the functioning of the global economy and as chief protagonists in the isolation of rogue regimes and actors from the financial system. Thus, the financial community finds itself drawn into combined financial and cyber battles."[25]

Zarate convincingly paints the picture of how this situation has evolved and how serious the threat to the U.S. (and global) financial system as well as to U.S. national security has become. He analyzes four primary threats to the financial sector; describes some of the actors who pose these threats; and gives a summary review of how the public and private sectors are responding to the growing cyber threat. Zarate goes on to explain why, despite real progress, the existing system remains deeply vulnerable. In his concluding section, he develops with substantial detail a provocative "new cyber-privateering framework" that could go a long way toward addressing the fundamental need for improved coordination between the banks and the government in combating the cyber-enabled financial war they now jointly confront.

In chapter 5, "Threats to Critical Infrastructure and the Transportation Sector," Tiffany Rad provides a case study of the development of cyber threats to U.S. critical infrastructure. Rad is very familiar with independent research on cybersecurity issues and particularly with work on hackers and hacktivists. As a result, when she reviews cyber threats to automobile traffic management systems as well as to electronic communications and controls technologies in airplanes, trains, and automobiles, she brings a wealth of realistic details that most will find chilling. Rad then summarizes how the U.S. government is responding to these kinds of threats, including how it is organized to respond and what is the basic distribution of responsibilities across government agencies.

Rad also describes government initiatives designed to improve public-private sector cyber threat communication and cooperation. While lauding most of this work, she criticizes the omission of adequate protections for the legitimate work of independent cybersecurity researchers. Particularly problematic is the tendency for private or public sector authorities to respond with hostility or even criminal complaints when individual researchers identify cyber vulnerabilities within an organization's computer and communications system, instead of welcoming the information and sharing it with appropriate others.

Rad's chapter provides particularly worrisome information about the growing asymmetric threat posed to large corporations or even nation states by small groups of non-state actors pursuing their individual agendas—with or without any adversarial state sponsorship. Technological change in the cyber realm has made it possible for small numbers of hostile actors to commit cyberattacks with devastating consequences grossly disproportionate to their numbers or resources—and this problem is only growing. Rad concludes with a discussion of several policy recommendations for how the U.S. could address its shortage of skilled cybersecurity professionals, enhance beneficial cooperation between government and industry, and address technical vulnerabilities in critical infrastructure core technologies.

In the final chapter, "Conclusions," principal investigator and editor, Samantha Ravich, reflects upon the rapid changes occurring in the nation's awareness and response to cyber threats as presented in the five previous chapters. She relates how the cyber policy landscape in the U.S. has evolved substantially even in the relatively brief time since this project was conceived in the autumn of 2013. The threat of cyber-enabled economic warfare against the U.S. also has escalated dramatically.

Ravich then identifies several key concerns about ways in which the U.S. response to emerging cyber-enabled economic warfare threats seem inadequate at best. She poses three concerns as particularly important. The first is the general inattention within the policy community today to the U.S.'s long history of both using and defending against traditional economic warfare. Much of the policy response to today's cyber threats seem to occur almost in a vacuum, as if policy makers had no memory of our extensive history with economic warfare and had learned no lessons from it. Second, the current analysis of emerging cyber threats to the United States seems also largely oblivious to the relevance of the U.S.'s extensive clandestine capabilities and use of *offensive* cyber-enabled economic warfare against our adversaries. If we do not reasonably analyze what we are doing and how it is being perceived by our adversaries, it is quite unlikely that we will properly understand how their intentions, strategies and actions are responding to it. This seems to be a very serious and dangerous blind spot. Third, and related to the first two, despite the fact that there has been a tremendous increase in awareness of U.S. vulnerability to cyber threats and a corresponding increase in plans and initiatives to take corrective action, there seems to be a basic disconnect between all this activity and any sound problem analysis rooted in a deep understanding of cyber-enabled economic warfare. The U.S. seems to believe it is sufficient to prepare for cyber threats without really understanding either the actors and plans behind them or the wide variations therein.

---

[1] Merrill Jensen. (2004) *The Founding of a Nation: A History of the American Revolution 1763–1776* (Hackett Publishing).

[2] Geoffrey James Ellis. (1991) *Napoleon's Continental Blockade: The Case of Alsace* (Oxford Publisher Press).

[3] Nicholas A. Lambert. (2012) *Planning Armageddon: British Economic Warfare and the First World War* (Cambridge, MA: Harvard University Press).

[4] Nechama Janet Cohen Cox. (2001) "The Ministry of Economic Warfare and Britain's Conduct of Economic Warfare, 1939-1945," doctoral thesis, King's College, University of London.

[5] Percy W. Bidwell. (1942) "Our Economic Warfare," *Foreign Affairs*, 20(3): pp. 421-437. http://www.jstor.org/stable/20029165

[6] Edward S. Miller. (2007) *Bankrupting the Enemy: The U.S. Financial Siege of Japan Before Pearl Harbor* (Annapolis, MD: Naval Institute Press).

[7] See for example Robert Loring Allen (1960) *Soviet Economic Warfare* (Public Affairs Press); Norman A. Bailey (1998) *The Strategic Plan that Won the Cold War: National Security Decision Directive 75* (McLean, VA: Potomac Foundation) http://www.iwp.edu/news_publications/book/the-strategic-plan-that-won-the-cold-war ; and Thomas Reed (2004) *At the Abyss: An Insider's History of the Cold War* (Presidio Press).

[8] Robert D. Atkinson, Stephen J. Ezell, Scott M. Andes, Daniel D. Castro and Richard Bennett. (2010) *The Internet Economy 25 Years After .Com: Transforming Commerce & Life* (Washington: The Information Technology and Innovation Foundation, March 2010): p. 43.

[9] See, for example, Office of the National Counterintelligence Executive (2011) "Foreign Spies Stealing U.S. Economic Secrets in Cyberspace: Report to Congress on Foreign Economic Collection and Industrial Espionage, 2009-2011," Oct; and Gregory C. Wilshusen (2012) "Information Security: Cyber Threats Facilitate Ability to Commit Economic Espionage," Testimony Before the Subcommittee on Counterterrorism and Intelligence, Committee on Homeland Security, House of Representatives; June 28.

[10] Keith Alexander. (2012) Speech at the American Enterprise Institute, July 9.

[11] Jason Ryan. (2012) "FBI Director Says Cyberthreat Will Surpass Threat From Terrorists," ABC News, Jan. 31. http://abcnews.go.com/blogs/politics/2012/01/fbi-director-says-cyberthreat-will-surpass-threat-from-terrorists/

[12] Elisabeth Bumiller and Thom Shanker. (2012) "Panetta Warns of Dire Threat of Cyberattack on U.S.," *New York Times*, Oct. 11. http://www.nytimes.com/2012/10/12/world/panetta-warns-of-dire-threat-of-cyberattack.html?_r=0

[13] See, for example, Tor Egil Forland (1993) "The History of Economic Warfare: International Law, Effectiveness, Strategies," *Journal of Peace Research*, 30(2): pp. 151-162; R. T. Naylor (2001) *Economic Warfare: Sanctions, Embargo Busting, and Their Human Cost* (Northeastern University Press); Gary M. Shiffman and James J. Jochum (2011) *Economic Instruments of Security Policy: Influencing Choices of Leaders*, 2nd ed. (Palgrave Macmillan); or Nicholas A. Lambert, op cit. at # 3.

[14] For recent examples, see Heather Harrison Dinniss (2012) *Cyber Warfare and the Laws of War* (Cambridge: Cambridge University Press); Franklin D. Kramer, Stuart H. Starr, and Larry K. Wentz (ed.s) (2009) *Cyberpower and National Security* (Washington, DC: National Defense University and Potomac Books, Inc.); NATO Cooperative Cyber Defence Centre of Excellence (2013) *Tallinn Manual on the International Law Applicable to Cyber Warfare* (Cambridge: Cambridge University Press); or Paul Rosenzweig (2013) *Cyber Warfare: How Conflicts in Cyberspace Are Challenging America and Changing the World (The Changing Face of War)* (Santa Barbara, CA: Praeger).

[15] See, for example, Paul Cornish (2011) "The Vulnerabilities of Developed States to Economic Warfare," working paper, June (London: Royal Institute of International Affairs) http://www.chathamhouse.org/publications/papers/view/176093 ; or Paul Cornish, David Livingstone, Dave Clemente, and Claire Yorke (2010) *On Cyber Warfare* (London: Royal Institute of International Affairs).

[16] See, for example, Richard Clarke. (2008) "Seven Questions: Richard Clarke on the Next Cyber Pearl Harbor," *Foreign Policy*, April 2.

[17] The part of the problem that is new is the "cyber-enabled" aspect. Economic warfare is a very old idea/practice, and U.S. vulnerability to physical terrorist attacks and/or natural disasters that could debilitate critical elements in the U.S. economy has been a major focus of concern at least since 9/11.

[18] Dubowitz and Fixler, Monograph, chapter 1, p. 1.

[19] Ibid, p. 2.

[20] Shulsky, chapter 2, p. 2.

[21] Hsieh, chapter 3, p. 2.

[22] Ibid, p. 2.

[23] Ibid, p. 19.

[24] Zarate, chapter 4, p. 2.

[25] Zarate, chapter 4, p. 3.

CHAPTER 1

Cyber-Enabled 'Swift' Warfare: Power, Blowback, and Hardening American Defenses

By Mark Dubowitz and Annie Fixler

Part 1: Swift, Smart Sanctions, and the Financial War Against Iran

Introduction

Economic warfare is now the default instrument of coercive statecraft for confronting challenges to the international order. Sanctions have become President Barack Obama's weapon of choice to combat Iran's nuclear program, Russia's invasion of Ukraine, the Assad regime in Syria, and the financing of terrorist groups such as the Islamic State, al-Qaeda, and others.

Leveraging the power of the U.S. dollar to isolate rogue actors—from the terrorists and nuclear proliferators of Iran's Revolutionary Guards to Sunni jihadists to Russian arms dealers and oligarchs—the U.S. Department of Treasury has established itself as a key national security agency. Economic sanctions, once thought to cause humanitarian crises without impacting the calculus of authoritarian regimes, have become a sophisticated tool for targeting the financial resources of a range of rogue actors. Financial sanctions became the key driver of an overall economic sanctions architecture that used conduct-based sanctions to isolate illicit financial activities.

The transformation of blunt and broad state-based embargos into the "smart sanctions," as they are characterized today,[1] has its roots in the wake of 9/11 and the all-out offensive against al-Qaeda, when the U.S. government began targeting not only its top operatives, but also the funders that enable and facilitate the terror group's violent activities.

These tools of economic coercion treat reputation as a currency in an environment in which companies cannot afford the risk of being associated with bad actors. The rules of this new world are straightforward: You can do business with the United States or you can do business with rogue actors. You can choose, but you can't do both. And if you choose the latter, prepare to be excommunicated from the global financial community.

The system is self-reinforcing: As rogue actors become more isolated, they engage in more suspicious behavior to evade restrictions. And the more suspicious their behavior, the more they find themselves isolated from financial networks. The approach is based on persuading private sector players—principally financial institutions—to act in their own self-interest to avoid unnecessary business and reputational risk.

As smart sanctions matured and the U.S. government discovered a new form of coercive power, the use of cyber-enabled financial measures became an integral part of the global financial sanctions architecture. At the heart of this architecture is SWIFT (the Society for Worldwide Interbank Financial Telecommunication), a financial messaging service that is the electronic bloodstream of the global financial system.

The story of how Iran became the first country to be expelled from the SWIFT system provides a glimpse into how economic warfare has changed in the past decade, and the importance of American economic preeminence in this pursuit. It also raises questions, however, about whether Washington is prepared to respond when states like China and Russia, looking to challenge the U.S.-led international order, turn their own economic power against the United States and its allies.

While tools of economic coercion and cyber-enabled economic warfare have both offensive and defensive components, the United States, to date, has primarily used those of an offensive nature. This paper analyzes offensive tools while acknowledging the importance of, and the danger in neglecting, defensive planning. While economic warfare encompasses a broad range of tools, financial sanctions are the foundation for the larger architecture of economic sanctions. As a result, this study addresses the rise of financial tools generally and cyber-enabled financial and economic sanctions specifically. This study also focuses on the tools used by the U.S. Treasury Department rather than attempting to address the range of economic coercion tools available to all agencies of the U.S. government. In the final section of this paper, however, we provide broader economic warfare recommendations and highlight ways that greater coordination across agencies might be facilitated.

Financial Intelligence

Financial intelligence (FININT) is at the heart of American efforts to leverage its financial assets in the pursuit of rogue actors and key to understanding the central role of SWIFT in these efforts. In the years before the formal creation of the Treasury Department's Office of Terrorism and Financial Intelligence (TFI) in 2004 and Treasury's intelligence agency, the Office of Intelligence and Analysis (OIA), the department developed a financial intelligence capability to block the assets of rogue actors and uncover and dismantle illicit financial networks. As a result, while the smallest agency in the U.S. government's intelligence behemoth, OIA punches well above its weight, unraveling illicit financial networks and providing evidence for thousands of designations.

The use of financial intelligence has been instrumental in disrupting terrorist cells and foiling plots including, for example, the planned attack on JFK airport in 2007—an attack linked to Iran's intelligence and covert networks in Latin America.[2]

FININT relies on traditional sources and methods of intelligence gathering and also on financial papers found in terrorist safe houses, detailed records from formal and informal financial institutions, suspicious activity reports from banks, and wire-transfer records. One of the critical elements of cyber-enabled, financial intelligence is messaging data from SWIFT.

Formed in 1973, SWIFT replaced telex messages between banks with a more secure, highly encrypted communications system. The consortium, headquartered in Belgium with 23 offices worldwide, has "the mission of creating a shared worldwide data processing and communications link and a common language for international financial transactions."[3] While other companies can enable secure financial transactions, SWIFT is the worldwide leader, far and away, with estimates of $6 trillion each day in payments value. SWIFT claims to link more than 10,500 institutions in 215 countries,[4] allowing the daily exchange of millions of standardized financial messages between banks, corporate customers, and financial institutions.

SWIFT "does not hold funds nor does it manage accounts on behalf of customers, nor does it store financial information on an on-going basis."[5] SWIFT is merely the courier that delivers financial messages between banks.

In the 1990s, the CIA tried to access SWIFT clandestinely to gather information on al-Qaeda's financial network, but the Treasury Department blocked the operation over concerns about a backlash from the banking community and perceptions that it would compromise the integrity of the financial system.[6] After 9/11, however, Treasury officials immediately began to reconsider how information from SWIFT could be legally and effectively leveraged as part of counterterrorism operations.

Within six weeks, Treasury built an innovative program, which became known as the Terrorist Finance Tracking Program (TFTP), to leverage SWIFT data to expose links between terrorists and their funders. The program analyzed the cyber data that formed the language of global financial transactions. Prior to the widespread adoption of SWIFT, such analysis may only have been possible by subpoenaing individual banks, compiling records from thousands of financial institutions (mindful that the worst offenders would be least likely to comply), and then analyzing the data to establish links. Instead, using data from SWIFT alone, Treasury was able to build a highly effecting program for uncovering terrorists' financial ties.

Treasury built a separate database to search SWIFT records and provided SWIFT with subpoenas on a monthly basis for select tranches of data that were then entered into the quarantined database. Only select officials could access the database and only for counterterrorism efforts—not operations related to proliferation, money laundering or other criminal activities. SWIFT had negotiated the most stringent restrictions to protect its data. To ensure compliance, SWIFT "scrutineers" had access to the system to verify each query was based on a counterterrorism investigation. Former SWIFT chief executive Leonard Schrank, who worked with Treasury to create the program, noted, "The use of the data was legal, limited, targeted, overseen, and audited," and the program could be considered the "gold standard" for how to balance national security and civil liberties.[7]

Although kept secret from the public for five years, the program was known to a targeted group in the intelligence community and executive branch, select members of Congress, and numerous banking officials in Europe and the United States.[8]

Carefully constructed by the leadership of SWIFT and Treasury's general counsel David Aufhauser to protect customer privacy, while also providing vital information to disrupt terrorist financing, the program proved invaluable to disrupting terrorist networks and uncovering dangerous plots. The TFTP provided information on "a key facilitator of terrorism in Iraq"[9] and led to the capture of Riduan Isamuddin,[10] aka Hambali, who was believed to be the mastermind of a string of bombings in Asia including the 2002 bombing in Bali and the 2003 attack on the Marriott hotel in Jakarta.[11] According to the Treasury Department, the program "helped to disrupt terrorist cells and operations and has helped save lives."[12]

Despite the program's legality and its importance to U.S. counterterrorism efforts, on June 23, 2006, *The New York Times* revealed the existence of TFTP,[13] jeopardizing not only its effectiveness but also U.S. relations with countries in Europe. The Treasury tried to persuade them not to publish the article by explaining the details of the program and its legality, but were unsuccessful after *The New York Times'* editors learned that the *Los Angeles Times* was going to run a similar story.[14] Treasury, it should be noted, was prepared for public revelations about the program since its inception.[15] When the article came out, the administration launched a full-throttled defense of TFTP and equally strong criticism of *The New York Times*' decision to publish the article.

The articles alerted terrorist financers to Treasury's methods. More damaging, however, were the revelations about Treasury's relationship with SWIFT, which prompted political attacks and challenges in European courts against the financial messaging service and accusations that SWIFT's actions were illegal and violated laws on data privacy. Even those European officials who had known about TFTP claimed not to understand the extent of the program.[16] SWIFT itself weathered the storm but was thrust into a bruising political debate.

Tensions between the U.S. and EU intensified with a February 2010 vote in the EU Parliament to block the agreement between the U.S. government, European Commission, and EU Council of Ministers permitting U.S. law enforcement access to SWIFT data.[17] Although a new agreement was reached with the European Union later that year, the program remained under intense scrutiny and was challenged again in October 2013 when the European Parliament called for a suspension of U.S. access to SWIFT data amid concerns over the National Security Agency's unrelated data-mining program.[18] The program and relationship between the U.S. government and SWIFT has required constant diplomatic attention.

The Iran Playbook

Meanwhile, Iranian threats to global security and the integrity of the financial system continued to grow. Building on the administration's work with the private sector to isolate terrorist finance, Treasury devised a new campaign to isolate Iran from the global financial system based on Iran's illicit business and banking practices. Iran was first added to the State Department's State Sponsors of Terrorism list in 1984 and had been under U.S. sanctions for its support for terrorism, missile proliferation, human rights abuses, and its nuclear program.[19] These sanctions had not halted Iran's illicit activities, so Treasury, with extensive congressional support, designed a new campaign to take financial warfare to a completely different level of impact.

In February 2006, then-Treasury Undersecretary for Terrorism and Financial Intelligence Stuart Levey formally pitched Treasury's new idea to Secretary of State Condoleezza Rice, and, with interagency approval and coordination, the Treasury Department began its campaign to persuade the global financial market to isolate Iran.

In the first two and a half years of the effort, Levey made more than 80 visits to foreign countries to meet not only with his government counterparts but also with the heads of more than 60 banks.[20] Levey presented detailed information about Iran's illicit activities and specific examples of suspicious transactions involving foreign banks.[21] The dossiers had the effect of conditioning the environment to reject Iranian transactions. As former Treasury official Juan Zarate explained, "Levey's job was to stage the financial assault on Iran's banks and its financial system—in large part by demonstrating to CEOs and compliance officers around the world that the risk of doing business with Iran was too high."[22]

Simultaneously, utilizing Executive Orders 13224 (2001) and 13382 (2005) targeting the financing of terrorism and weapons proliferation, respectively, Treasury started to designate individual Iranian banks for their role in facilitating illicit financial activities. These two executive orders set the precedent for not only targeting the illegal trade in illicit goods but also for isolating the financial transactions that enable the movement of physical commodities. Beginning in 2007, the Treasury Department designated 23 Iranian and Iranian-allied foreign financial institutions as "proliferation supporting entities" under Executive Order 13382.[23] Of these, at least eight banks were designated for their ties to Iran's Islamic Revolutionary Guard Corps (IRGC) or because they were controlled by banks with IRGC links.[24] In 2006, Treasury also sanctioned Bank Saderat as a "terrorism supporting entity" under Executive Order 13224

for facilitating fund transfers to Hezbollah, Hamas, Palestinian Islamic Jihad, and other terrorist organizations.[25]

The State Department supported Treasury's efforts through a diplomatic push to explain the financial campaign, as well as to increase the political pressure on Iran. Working bilaterally and within the United Nations, State sought to build international buy-in for broader sanctions against Iran. While the U.N. Security Council eventually passed four sanctions resolutions against Iran starting in 2006,[26] each resolution required months of negotiations and significant compromises in order to get Chinese and Russian approval. It became clear that by working outside traditional international bodies like the U.N., the U.S. Treasury Department could leverage the power of the dollar and the central role that the U.S. plays in financial markets in order to cut off Iranian financial transactions. However, the U.N. resolutions provided a foundation for other countries to implement their own multilateral and unilateral sanctions. This was especially true in the case of U.N. Security Council Resolution 1929 (2010) that provided the European Union with political cover for implementing its own oil embargo. The U.N. resolutions also gave a semblance of multilateralism to what the United States was already implementing unilaterally.

Treasury's new efforts to lead the way on a tougher and smarter sanctions regime were strengthened significantly by the bipartisan passage of multiple pieces of congressional legislation between 2010 and 2013. These congressional measures targeted Iran's financial, energy, shipping, insurance, precious metals, and industrial trade, including a successful effort, initially opposed by the Obama administration, to squeeze Iran's economic lifeline: its crude oil exports.

In 2010, Congress passed the Comprehensive Iran Sanctions, Accountability, and Divestment Act of 2010 (CISADA),[27] overhauling the Iran Sanctions Act, which had been on the books since 1996 but was never effectively enforced because of resistance from European governments and companies. With Europe now moving ahead with its own sanctions against Iran's nuclear program, this resistance diminished. CISADA now provided the Obama administration with the threat of congressional action to persuade foreign companies to choose between their business ties to Iran and their access to the U.S. market.

The legislation prompted dozens of foreign companies, especially European energy firms, to terminate the provision of refined petroleum products to Iran and to cease further investments in the Iranian energy sector. It also provided a package of powerful financial measures to strengthen Treasury's financial sanctions campaign by threatening to cut off foreign financial institutions from their banking relationships in the United States, and their ability to offer U.S. banking services, including the use of the U.S. dollar, to their banking clients. Six months after the passage of CISADA, then-Undersecretary for Political Affairs Bill Burns testified before Congress that the legislation had already cost Iran between $50 and $60 billion.[28]

From FININT to Economic Coercion: Disconnecting Iranian Banks

During this time of escalating sanctions pressure, Iran continued to refuse to cooperate with the International Atomic Energy Agency (IAEA) or to address concerns raised in U.N. Security Council Resolutions, and rejected a proposal in October 2009 to export its 20 percent enriched uranium for reprocessing and fuel fabrication for the Tehran Research Reactor. Iran continued to support U.S.-designated terrorist groups including Hezbollah, Hamas,[29] and, as Treasury revealed, even al-Qaeda.[30]

As Iran's nuclear program moved ahead, policymakers looked to Treasury for new innovations in tools of cyber-enabled economic warfare. Although the value of SWIFT data was

recognized as a key source of financial intelligence, until early 2012, its value as a coercive instrument of economic warfare was not understood fully.

Financial institutions and multinational companies have long been responsible for knowing their customers, but SWIFT was the exception. SWIFT was treated like a simple messaging service responsible neither for the contents of the message nor for the actions of the sender or receiver.

In 2011, responding to increased international attention on more effective sanctions enforcement, SWIFT announced it had implemented a screening program to allow its customers to route messages through an application that checks the information against a selected sanctions designation list.[31] At the time, SWIFT claimed that it "manages the screening engine and is responsible for configuring and maintaining the screening algorithm."[32] However, the option of which lists to use was left to the discretion of each individual user,[33] and the use of the screening system was not mandatory for SWIFT clients. The screening program was a tool for SWIFT members to do their own due diligence, but SWIFT was not responsible if its customers used its messaging system to engage in illicit financial activities.

Developments over the next six months would begin to change the way policymakers saw SWIFT's role. After 9/11, Section 311 of the USA PATRIOT Act gave Treasury new authority to designate illicit financial actors as entities of "primary money laundering concern." While a Section 311 regulation advises only U.S. banks to end relationships with a designated entity and requires no action by foreign banks, the effect is a stark public indictment. While the United States does not order any asset freezes, financial institutions around the world typically freeze assets and close accounts in reaction to a 311 declaration that a bank, for example, is financially radioactive.

On November 22, 2011, expanding on its designations of individual Iranian financial institutions, Treasury issued a Section 311 finding that the entire country of Iran was "a jurisdiction of primary money laundering concern," citing Iran's "support for terrorism," "pursuit of weapons of mass destruction," and "the illicit and deceptive financial activities that Iranian financial institutions … engage in to facilitate Iran's illicit conduct and evade sanctions." Treasury targeted the Central Bank of Iran (CBI) and made it clear that the country's entire financial system posed "illicit finance risks for the global financial system."[34]

This action against the CBI built on the experience of using "the 311" as part of a full-scale, multifaceted pressure campaign against North Korea that culminated in the September 2005 finding against Banco Delta Asia (BDA), a Macao-based financial institution that enabled a range of illicit financial activities by the North Korean regime. In that case, the designation of a bank that the North Korean regime used to evade sanctions and engage in proliferation-sensitive financing, drug smuggling, money laundering, and other illicit activities spurred the private sector to dump Pyongyang like a toxic asset. Within days of BDA's designation, North Korean accounts and transactions were frozen or blocked in banking capitals around the world—notably including Beijing.

Treasury's 311 finding against the Iranian financial sector led to the "Menendez-Kirk amendment," congressional sanctions under Section 1245 of the National Defense Authorization Act (NDAA) of 2012, targeting foreign financial institutions conducting transactions with the Central Bank of Iran (CBI).[35] The legislation blocked the assets of designated Iranian financial institutions, including the CBI. Section 1245 also prohibited the opening or maintenance of any correspondent or payable-through accounts for any foreign financial institution that the president determined had conducted or facilitated significant financial transactions with the Central Bank of Iran or any other designated Iranian financial institution with narrow humanitarian and crude oil exceptions (that depended on a country "significantly reducing" its

volume of crude oil imports). The implementation of these sanctions effectively cut off the CBI from the global financial system and reduced Iranian crude oil exports, which accounted for approximately 80 percent of Iran's export earnings, from 2.5 million barrels per day to approximately 1 million.[36]

The Section 311 finding and Section 1245 of the FY2012 NDAA strengthened arguments that SWIFT should be responsible for blocking the financial messaging instructions of designated financial institutions and other related entities. The argument began to build for the expulsion of these designated entities from SWIFT's messaging service.

Iran, not surprisingly, had been using SWIFT's ubiquitous financial messaging service to conduct business with its trading partners, to sell its oil, to raise capital for its energy sector, to procure energy-related equipment and technology, and to buy and sell other goods and services. In 2010, 19 Iranian banks and 25 Iranian entities reportedly used SWIFT more than two million times, sending 1,160,000 messages and receiving 1,105,000.[37] These messages and transactions amounted to $35 billion in trade with Europe alone.[38]

By 2012, SWIFT represented one of Tehran's last entry points into the global financial system, as the United States and the European Union had sanctioned scores of banks, energy companies, and other entities under the control of the IRGC.

Treasury was initially hesitant about the idea of using SWIFT as a tool of economic warfare. Following the backlash in response to public revelations about the Terrorist Finance Tracking Program, Treasury was particularly sensitive to the perception that SWIFT was being politicized in the dispute over Iran's nuclear program. Treasury did not want to further complicate Washington's relationship with SWIFT and of the value of its financial data for counterterrorism operations. There may also have been hesitation because of a concern about the loss of financial intelligence into Iranian activities that Iran's participation in SWIFT provided.

SWIFT's bylaws required that its "services should not be used to facilitate illegal activities," and to prohibit access if a "user is subject to sanctions." Moreover, senior executives of the global financial institutions that form the board of SWIFT have the power to expel a user who "has adversely affected … SWIFT's reputation, brand, or goodwill."[39]

SWIFT was also a critical financial gateway to the European Central Bank's Trans-European Automated Real-Time Gross Settlement Express Transfer (Target2) system. Target2 is the European Central Bank's proprietary electronic interbank payment system, equivalent to the U.S. Fedwire, and the system that settles transactions in euros through the SWIFT gateway. The ECB's guidelines were even more specific than SWIFT's. The guidelines explicitly barred any entity engaged in "money laundering and the financing of terrorism, proliferation-sensitive nuclear activities and the development of nuclear weapons delivery systems."[40] That fit Iran to the letter.

Target2 was important to Iran because U.S. financial sanctions already had curtailed much of Iran's dollar-denominated business. In response, Tehran relied increasingly on the euro, the world's second largest and most liquid currency reserve holding. The regime shifted part of its foreign exchange reserves to euros and began denominating a substantial portion of its international trade contracts in euros.

In early 2012, as discussions about SWIFT's role in enforcing sanctions intensified, SWIFT responded to challenges about its compliance with international sanctions against Iran by stating that "all decisions on the legitimacy of financial transactions under applicable regulations … rest with financial institutions and the competent international and national authorities."[41] However, SWIFT provides more just the "envelope and postage stamp" for a

financial message and more than mere technical assistance. SWIFT provides the prerequisite codes that allow financial institutions to process a transaction.

Determined to block Iran from SWIFT, U.S. policymakers and EU regulators now focused on clarifying that financial messaging services fell under existing authorities regarding Iran sanctions. The Senate Banking Committee began working on an amendment to sanctions legislation that ultimately became the Iran Threat Reduction and Syria Human Rights Act (ITRA) of 2012. Co-authored by Senators Robert Menendez (D-NJ) and Roger Wicker (R-MI), and inspired by Senator Mark Kirk (R-IL), who was recovering from a stroke at the time, the amendment provided the administration with the authority to sanction financial communications services providers, including SWIFT, servicing European Union-designated financial institutions. The amendment was adopted into the legislation, and passed out of committee on February 2, 2012.[42]

The Obama administration sought to persuade key legislators that it was better positioned to pursue this matter quietly rather than having Congress adopt punitive measures against a critical global financial actor like SWIFT. However, as in other cases of sanctions against Iran, congressional pressure proved to be useful leverage in persuading international companies and governments to pass and enforce their own sanctions.

Six weeks after the Senate Banking Committee's actions, the European Union Council clarified that "no specialized financial messaging shall be provided to those persons and entities subject to an asset freeze." EU regulators instructed SWIFT to remove specified Iranian banks from the SWIFT network.[43] SWIFT's chief executive Lázaro Campos announced that the consortium would remove Iranian banks from its system noting that, "disconnecting banks is an extraordinary and unprecedented step for SWIFT. It is a direct result of international and multilateral action to intensify financial sanctions against Iran."[44]

While the expulsion from SWIFT of most Iranian banks was ultimately a direct consequence of EU regulations,[45] the threat of U.S. sanctions played an important role in persuading the EU to "de-SWIFT" a number of these banks.[46]

The Impact of "De-SWIFTing" Iran

The ban from SWIFT was not total, however. The Treasury Department, in an attempt to leave open a channel for humanitarian funds to reach Iran and to avoid measures that would unduly harm the Iranian people, intentionally left a handful of Iranian banks undesignated and, therefore, not targeted for SWIFT disconnection.

Treasury officials and EU regulators assured the international community that they would keep an eye on both designated and undesignated banks and prevent illicit funds from moving through the SWIFT system.

Despite these assurances, a December 2013 corruption scandal in Turkey revealed that Iranian banks were still using SWIFT for illicit financial transactions. According to a leaked prosecutor's report,[47] Iran's Pasargad Bank, Parsiyan Bank, Sarmaye Bank, Bank Tos-e-Sadarat, Karafarin Bank, and Saman Bank allegedly processed sanctions-busting transactions for the network of Turkish-Iranian businessman Reza Zarrab,[48] who allegedly processed more than €87 billion in illicit transactions between 2012 and 2013.[49] The corruption scandal quickly became politicized as the probe implicated ministers, their family members including Prime Minister Recep Tayyip Erdoğan's son, and politically connected businessmen including the head of state-owned Halkbank.[50] The AKP government responded to the allegations with a "wholesale replacement of police, prosecutors and judges."[51] A number of police officers that had been involved in the investigation were later arrested on charges of "attempting a coup."[52] Anti-

corruption NGO Transparency International said the subsequent decision by the new prosecutors to drop the charges "calls into question the rule of law in Turkey."[53] The Organization for Economic Co-operation and Development (OECD), an organization of 34 advanced and emerging countries,[54] raised serious concerns about Turkey's ability to investigate corruption cases and about political interference in the investigation and influence over the judiciary.[55]

Although the Turkish government's actions have effectively blocked further investigation into the case[56]—and media coverage of the inquiry[57]—the prosecutor's report in December 2013 showed actual SWIFT transaction receipts. This raises questions about the wisdom of leaving Iranian banks on the SWIFT system given allegations that these banks engaged in the falsification of invoices to obscure the nature of the transactions and used unscrupulous international banks to certify that the transactions were in compliance with international sanctions.

Meanwhile, another loophole had emerged. A year after the "de-SWIFTing," of the Iranian banks, it was revealed that some Iranian banks were still accessing Target2. U.S. lawmakers began pressing EU regulators to block Iranian government entities and their affiliates "direct or indirect" access to Target2 in order to prevent Iran from using its "foreign-held euros."[58]

Following the provision in ITRA regarding SWIFT,[59] Congress inserted a similar measure banning Iranian banks from accessing Target2 in the Nuclear Iran Prevention Act of 2013 (H.R. 850), which passed the House of Representatives in July 2013 by a vote of 400-20.[60] The Senate companion legislation, the Nuclear Weapons Free Iran Act of 2013 (S. 1881), contained similar language.[61] This legislation garnered the 60 co-sponsors needed for cloture and reportedly had support from a veto-proof majority of the Senate.[62] However, the legislation stalled following the election of Iran's new president Hassan Rouhani, the start of P5+1-Iran nuclear negotiations in Geneva, and a direct threat from President Obama to veto the legislation.[63]

Despite implementation problems, and stalled new legislation, the expulsion of most Iranian banks from SWIFT successfully limited Iran's ability to access the global financial system. SWIFT had become a critical part of the multiyear effort to persuade scores of foreign banks to restrict Iranian access to global financial markets and further demonstrated the influence of Congress, which had successfully targeted Iran's financial, energy, shipping, and insurance sectors and crude oil exports. These sanctions applied greater pressure on the Iranian leadership than anything in the previous decades. Iranian leaders particularly understood the damage to their economy from the SWIFT cutoff. During multiple rounds of nuclear negotiations since the fall of 2013, Iranian negotiators reportedly have demanded that SWIFT be included as one of the first Western sanctions to be reversed.[64]

Contemplating Russia

The Iranian sanctions playbook became a model for policymakers to respond to other international crises. With Russia's annexation of Crimea and invasion of eastern Ukraine, policymakers re-opened that playbook for applicable economic warfare tools to persuade market players to voluntarily cut their business ties with Moscow.

To date, U.S. and EU governments have cautiously imposed calibrated sanctions to inflict steadily increasing costs while signaling to Russia and market players that there is more to come. With its closer integration into the global economy and greater scope for retaliatory measures, Russia however was a much larger and more difficult target than Iran. As a result, the U.S. and EU have been slow to impose broad, sector-based sanctions on Russian oil and gas, block Russian access to the global banking sector, or target Russian arms exports. There is genuine concern that Russia could retaliate by cutting off natural gas exports to Europe, freezing

or appropriating the assets of Western businesses operating in Russia, or launching cyberattacks against Western business interests. Russia could also expand import bans on EU and U.S. goods, restrict commercial air traffic over Siberia, suspend U.S. and NATO access to the Northern Distribution Network to Afghanistan, and serve as a financial outlet or supplier to rogue regimes, with the potential use of Russian banks by Iran and North Korea. Russia could deliver advanced weapons systems, like the anti-aircraft S-300s, to Iran and Syria, weapons systems for which these countries previously had contracts.[65] Moscow could also respond to U.S. and EU sanctions by undermining the P5+1 nuclear negotiations with Iran through Russian support for Tehran's negotiating positions or sanctions-busting Russian-Iranian economic deals.

Obama administration officials have maintained that the crisis in Ukraine and the Iranian negotiations with the P5+1 are completely separate and that they are not concerned that Russia will undermine the nuclear negotiations and the international sanctions regime. However, reports of a $20 billion oil-for-goods deal between Moscow and Tehran indicate that both Russia and Iran are keeping their options open.[66] Russia also built and supplies the fuel for Iran's Bushehr Nuclear Power Plant after German company Siemens abandoned the project following the 1979 Revolution.[67] Moscow has outstanding contracts with Iran to provide surface-to-air defense missiles and other military goods and is providing diplomatic, economic, and military support to Bashar Assad in Syria. Russia has also repeatedly provided diplomatic cover for the Assad regime at the United Nations and prevented the passage of multiple U.N. Security Council Resolutions. Indeed, following the passage of U.S. legislation authorizing additional sanctions and the provision of lethal aid to Ukraine and the announcement of designations of Russian human rights violators at the end of December 2014, the Russian Foreign Ministry spokesman warned that sanctions "are putting in doubt prospects for bilateral cooperation on solving the situation around the Iranian nuclear program, the Syrian crisis, and other acute international problems."[68]

Starting in March 2014, following Russia's invasion of the Crimean peninsula, the United States and European Union began implementing measures to pressure Russia politically and economically. Efforts began by designating individuals directly involved in the invasion of Crimea, and later those directly involved in the rebellion in eastern Ukraine including separatist leaders, officials of the Russian intelligence and government, and oligarchs closely connected to President Vladimir Putin. These individuals were subject to asset freezes and visa bans. The United States issued three executive orders in March 2014 (and a fourth in December) outlining these restrictions.[69] At the same time, the Group of Seven (G-7)[70] countries announced that they would not attend the planned G-8 summit in Sochi but instead would hold meetings as the G-7 in Brussels.[71] The announcement effectively kicked Russia out of the group.

On March 20, the United States sanctioned the first Russian bank, Bank Rossiya, under Ukraine-related sanctions.[72] The "deeply obscure but hugely powerful"[73] bank is reportedly "the personal bank for senior officials of the Russian Federation" and its "shareholders include members of Putin's inner circle."[74]

Over the next several months and especially following the downing of Malaysia Airlines Flight MH17, which killed 298 people, the European Union and United States began restricting exports of dual-use goods,[75] and certain technologies for Russia's oil sector related to deep-water, arctic offshore, and shale exploration and production operations.[76] Initially, these restrictions excluded natural gas and applied only to future military sales, not existing contracts.[77]

As the situation continued to deteriorate—and following a de facto Russian invasion of Ukraine[78]—Western countries began looking for additional ways to pressure Putin to respect Ukraine's sovereignty and territorial integrity. On September 12, 2014, the United States and

Europe announced additional sanctions targeting Russia's financial, defense, and energy sectors.[79] The U.S. Treasury expanded sanctions on Russia's financial institutions, including Russia's largest bank Sberbank, on Russia's energy sector, and on the Russian defense sector.[80] The measures restrict the ability of designated Russian banks to obtain credit, and the energy-sector related measures apply not only to future contracts but also to existing business, providing U.S. firms only two weeks to cease relevant business interactions.[81] These sanctions built on debt and equity restrictions that the United States began implementing over the summer, and addressed the gap between designations by the United States and those by Europe, which had designated Sberbank in July. The sanctions will affect Russia's access to Western technology and services that are needed to develop Moscow's medium- to long-term oil exploration and production capacity.

However, notably absent from U.S. and EU designations has been Russia's state-owned arms exporter, Rosoboronexport, which plays a leading role in Russian weapons provisions to Ukrainian rebels, the Assad regime in Syria, and the government of Iran. The Bush administration had previously sanctioned Rosoboronexport in 2006 for assisting Iran's nuclear program, but all sanctions on the company expired in May 2010.[82] Despite pressure from Congress to sanction Rosoboronexport, the Treasury Department has not taken steps against the company in large part because of existing Defense Department contracts to provide helicopters to the Afghan military.[83]

Were U.S. officials to contemplate mirroring the Iran sanctions architecture, a next step in the sanctions escalation might be the issuing of a Section 311 finding against a Russian bank found to be financing the government's support for the rebels in the illegal invasion of eastern Ukraine, Russia's support for and weapons exports to President Assad in Syria (which violates U.S. and EU sanctions against Damascus), or other examples of illicit financial activity including money laundering and proliferation-sensitive financing in contravention of U.S. law. In accompanying statements, U.S. officials could indicate that other Russian banks are being investigated for similar conduct and that there are concerns that the entire Russian financial sector might be a jurisdiction of primary laundering concern.

U.S. officials could then partner with their EU counterparts and other members of the Financial Action Task Force (FATF), a financial standards body comprised of 34 members plus the European Commission and the Gulf Co-operation Council,[84] to issue warning notices to foreign financial institutions about Russian money laundering concerns. As both international economic sanctions and global financial standards gained prominence, this international body, whose focus on combating the classic money laundering schemes of drug cartels and organized crime, was retooled to build international standards surrounding terrorist financing and proliferation. If Moscow's financial sector failed to implement anti-corruption and anti-money laundering measures, FATF could decide to issue a notice adding Russia to the "gray list" of countries with money laundering and terror finance deficiencies. Unlike Iran, however, Russia is a member of one of the "FATF-Style Regional Bodies,"[85] and this may need to be factored into the strategy vis-à-vis any FATF statements on Russia.

Meanwhile, Congress could begin—and, indeed, already has begun—discussing financial and sector-based sanctions like those found in CISADA. This legislation would ban investments in key sectors of the Russian economy and would designate foreign financial institutions doing business with blacklisted Russian companies. Senator Mark Kirk (R-IL) has drafted legislation mirroring some of the measures imposed on Iran, including sanctions targeting the Russian central bank and Russian access to SWIFT.[86] His involvement in this draft legislation is especially notable as he is the co-author of many of the most stringent sanctions against Iran.

While EU governments have not yet considered measures like those contained in Senator Kirk's draft legislation, there are reports that they may be looking at SWIFT as a possible

alternative tool.[87] The British government reportedly has been pressing its EU partners to remove Russian banks from the SWIFT system and tabled the issue at a EU ministers meeting at the end of August 2014.[88] Other members of the EU, however, have been more hesitant to support punitive measures against Russia, and the bloc has not yet taken action to remove Russian financial institutions from the SWIFT system.[89]

"De-SWIFTing" even one Russian bank would have far reaching consequences for the Russian economy. Coupled with removal from the Target2 euro clearing system, the exclusion of a small number of already designated Russian banks from SWIFT would have painful consequences for Moscow. If implemented, this could be legitimized as an essential regulatory step to protect the integrity of the financial system from Russian banks whose illicit financial activities explicitly contravene the bylaws of both SWIFT and Target2. However, the use of SWIFT as a financial sanctions tool carries certain risks that will be discussed in more depth in the next section.

As Russia's economy has dramatically declined in recent months, its leadership and central bank have intervened not only to try to stem inflation but also to provide a mechanism for companies—including designated entities—to refinance their foreign debt.[90] The Russian leadership understands the significance that such a de-SWIFTing would have for the economy and Russia's ability to transact with global markets. Andrei Kostin, head of Russia's state-owned VTB Bank, warned that de-SWIFTing Russian banks would be tantamount to a declaration of war. "In my personal opinion it would mean war—if this type of sanction will be introduced… If Russian banks' access to SWIFT will be prohibited, the U.S. ambassador to Moscow should leave the same day. Diplomatic relations must be finished. Banking is the most vulnerable part of the Russian economy because the system is based so strongly on the dollar and the euro," he said.[91] Russian experts believe that this statement likely reflected President Putin's perspective as well given Kostin's close relationship with the Russian leader. Reportedly, Kostin is Putin's close friend, a member of the board of Rosneft, and Putin's second-most consulted adviser.[92] The U.S. Treasury also added VTB Bank to its Sectoral Sanctions Identification list prohibiting U.S. persons from transacting in debt of longer than 90 days maturity with VTB Bank.[93]

It is debatable whether sanctions will affect Moscow's political calculations or have been a key driver of Russia's current economic difficulties. While the ruble lost half of its value in 2014 and the Russian central bank projects that the economy could shrink by 4.7 percent next year,[94] Russia has yet to reverse its policies on Ukraine. It also is not clear how much of the crisis in the Russian economy is a result of the sanctions, structural problems in the Russian economy, or the drop in oil prices from $110 in July 2014 to under $60 per barrel in January 2015. As former U.S. Ambassador to Russia Michael McFaul noted, "Sanctions raise uncertainty about the Russian economy. Their own minister of economic development said today that the ruble is falling faster than the macroeconomic indicators would suggest it should be."[95] Russia's Finance Minister Anton Siluanov, however, has said that sanctions are costing Russia $40 billion per year and that the drop in oil prices is costing between $90 and $100 billion per year.[96]

The impact of the price of oil on the Russian economy raises questions—beyond the scope of this study—about the extent to which U.S. policymakers can influence market prices as well as restricting Russian market access through sanctions. While some experts believe that Saudi Arabia convinced OPEC not to reduce production, even as oil prices fell, in order not to lose market share to U.S. shale-oil companies and other non-OPEC producers,[97] others speculate that Riyadh's real target was Iran, with whom the kingdom finds itself at odds throughout the Middle East, from Syria to Yemen.[98] Future economic coercion might include a more active role by the U.S. government in influencing markets; however, such policies could move the government away from a focus on conduct-based economic measures towards the politicization

of markets with negative consequences for America's role as a global arbiter of economic activity.

Unlike the sanctions against Iran, sanctions on Russia were crafted in a way to protect specific economic and financial trade flows that the U.S. government deemed essential and areas in which the U.S. government saw specific risks of retaliation. The U.S. government identified a different kind of financial vulnerability, namely the dependence of Russian banks and corporations on external financing. The application of economic tools against a larger, more complex, and more globally integrated economy like Russia's required innovations in sanctions and not just a wholesale application of the Iran sanctions playbook. The complexity of dealing with a target like Russia reinforces the need for the development of a doctrine of economic warfare and the importance of a forward-leaning policy planning process to identify financial vulnerabilities and design appropriate tools to be used against a range of targets. A further discussion of the importance of developing a doctrine of economic warfare is included in Part 3.

The use of economic coercion to achieve national security goals provides the United States with an important policy tool for changing the policy calculations of other countries. However, economic measures should supplement but not replace the use of other coercive measures. To affect not only the Russian economy but also Moscow's political calculations, Western economic warfare must be combined with other means of coercion—from tough diplomacy to covert action to the credible threat of military force or the provision of meaningful military aid to Ukrainians and other Eastern Europeans prepared to fight for their freedom. Offensive economic warfare also must have a defensive component that strengthens Western resiliency against Russian responses.

Part 2: If Economic Warfare Tables Were Turned

From Old-School to Cyber-Based Sanctions Busting

Rogue actors are responding to economic isolation by using traditional and cyber-based sanctions-busting techniques. In response to threats to remove its banks from the SWIFT system, for example, the Russian parliament drafted legislation to set up an alternative financial messaging system. The Association of Russian Banks also announced that if its members were removed from SWIFT, it could use other financial communications systems, including more costly secure Internet and fax exchanges.[99] Russian officials have reportedly discussed a SWIFT alternative with their Chinese counterparts.[100] However, it is not clear how quickly such a system could be created and whether major banks outside Russia would be willing to use this alternative system if it exposed them to reputational damage or legal sanction from the U.S. and EU.[101]

Banking experts believe, however, that the creation of an alternative system could have a significant impact on international trade, including making global payments less efficient.[102] If Russia and China created a SWIFT-competitor, the system likely would place less of a priority on monitoring and blocking illicit financial activities and might enable Iran and other rogue financial actors to operate freely.

The elaborate scheme revealed in the Turkish prosecutor's report, through which Iran moved tens of billions of dollars in illicit funds between Turkey and Iran, also allegedly involved numerous sanctions-busting techniques including "over-invoicing." This is one of the many classic money laundering techniques, which "allows illegal organizations the opportunity to earn, move, and store proceeds disguised as legitimate trade."[103] In the Turkish example, a

luxury yacht company sold the Iranian Pasargad Bank 5.2 tons of brown sugar for a massively inflated price of about $240 per pound.[104] EU regulators had permitted the Iranian bank, which electronically transferred the illicit funds, to remain on SWIFT to provide a humanitarian channel for Iran's people. Iran abused this.

In other attempts to skirt sanctions, Iran has reflagged numerous vessels from Islamic Republic of Iran Shipping Lines (IRISL) and NITC (formerly the National Iranian Tanker Company) to places like Tuvalu and Tanzania,[105] and renamed ships repeatedly with non-Farsi names.[106] The objective was to evade international sanctions following the U.S. Treasury Department's designation of IRISL in 2008 under Executive Order 13382 for "facilitat[ing] shipments of military-related cargo destined for [Iran's Ministry of Defense] MODAFL and its subordinate entities." At the time, Treasury noted that IRISL "has deliberately misled maritime authorities through the use of deception techniques" to transport military-related goods and other banned items.[107]

As noted above, sanctions on Iran's crude oil exports were aimed at reducing government revenue for Iran's nuclear program and support for terrorism and pressuring the government to cease its illicit activities. As these sanctions were increasing, Iran engaged in another sanctions-busting scheme. Using ship-to-ship transfers in order to disguise the origin of its crude oil, NITC tankers would move the Iranian crude oil into foreign-owned ships to be sold in Southeast Asia. There were also instances of Iranian crude being blended with other crudes or held in mislabeled barrels.[108]

These and numerous other sanctions evasion schemes run by Iran and other rogue actors are well documented.[109] As a result, the U.S. Treasury Department has created a "Foreign Sanctions Evaders" list as a complement to its Specially Designated Nationals (SDN) list.[110]

But the U.S. government is always playing catch-up as new schemes emerge and new players willing to take the risks for large profits enter the market. As those unwilling to take risks leave the market, the remaining players exercise their increased market power by negotiating deep discounts, steep premiums, or high commissions to help rogue actors evade sanctions.

The birth of cyber-enabled tools and financial mechanisms present new sanctions-busting opportunities for criminal organizations, terrorists, weapons proliferators, and rogue states.[111] Nontraditional, digital, virtual, or cryptocurrencies like bitcoin—an online, decentralized, peer-to-peer currency that is issued based on a computer algorithm rather than from a national bank—for example, are not subject to the same regulations and reporting requirements (although this is beginning to change) as the traditional financial sector and thus may provide a space for illicit financial activities to flourish.[112]

New, alternative technologies do not yet pose a realistic, large-scale alternative to traditional financial channels—the commodities market is not pricing barrels of oil in bitcoin nor are companies financing their debt in "Linden" dollars from the popular virtual world Second Life or "Ven," a digital currency from the social networking site Hub Culture, which focuses on the virtual and physical exchange of goods and services. However, the continued development of new cyber-enabled tools requires proactive engagement with the creators of these financial mechanisms and in-depth policy planning across multiple agencies of the U.S. government to properly assess vulnerabilities. This topic will be explored in Part 3.

Future Threats: The Use of Cyber-Enabled Economic Warfare Against the United States and U.S. Allies

While sanctions evasion threatens the efficacy of economic coercion and requires constant vigilance by enforcement authorities, cyber-enabled economic warfare against the U.S. and its allies is a much greater threat to national and economic security. In the past decade, the United States has been at the forefront of using economic warfare against rogue actors, but it can only be a matter of time before adversaries and enemies turn the tables on the U.S. and its allies. Developing an arsenal of defensive tools for America and its allies has become an urgent task.

In an indication of challenges ahead, on October 6, 2014, SWIFT announced that pro-Palestinian organizations had petitioned SWIFT to disconnect Israeli financial institutions and the entire country from its financial messaging system.[113] SWIFT made the following statement:

> SWIFT regrets the pressure, as well as the surrounding media speculation, both of which risk undermining the systemic character of the services that SWIFT provides its customers around the world. As a utility with a systemic global character, it has no authority to make sanctions decisions. SWIFT will not respond to individual calls and pressure to disconnect financial institutions from its network.[114]

Although SWIFT rejected the pressure and explained that it would not take action without direction from EU regulators, SWIFT would presumably comply, as it did in the Iran case, if the EU designated Israeli financial institutions because they operate in the West Bank and issued orders requiring that SWIFT expel these institutions from its system.

Israel, of course, has long been a target of economic warfare. The Israeli Chamber of Commerce estimates that the Arab boycott, which began more than 40 years ago, has cost the country $45 billion.[115] On a global scale, the Arab oil embargo of 1973 is estimated to have caused a 4.7 percent decline in America's GDP and a 7 percent and 2.5 percent decline in Japan's and Europe's GDP, respectively.[116]

Ten years ago, an anti-Israel "Boycott, Divestment and Sanctions" (BDS) campaign began to coalesce.[117] The United States should view this movement in its broader economic warfare context: The campaign is attempting to persuade corporations and financial institutions to discriminate against the State of Israel, its corporate entities, and its citizens.

The BDS movement and the idea of using tools of economic warfare against Israel appear to be gaining some ground in Europe. In 2012, the EU's consuls general in East Jerusalem and Ramallah issued a Heads of Mission report recommending sanctions on Israeli settlements,[118] and in January 2014, PGGM, a large Dutch pension fund, withdrew its investments from Israel's five largest banks because they have branches in the West Bank.[119] In November 2014, an internal EU document was leaked to the press. The document included an assessment of what economic sanctions against Israel could possibly include.[120]

Although the BDS movement and similar efforts are directed against Israel today, such strategies could be employed against other American allies—and the United States itself—down the road. The strategic assessment and institutional reforms necessary to protect the United States and its allies from economic coercion (discussed in Part 3) should include an understanding of the BDS movement as a manifestation of economic warfare.

In the following scenario, we lay out an unlikely but entirely plausible situation through which SWIFT could become a political football in a regional conflict and a dangerous tool employed by America's global competitors. This scenario is entirely hypothetical, and the authors have no reason to believe that countries are contemplating the steps outlined below. However, there is also nothing preventing such a scenario.

Hypothetical: SWIFT and the Crisis in the South China Sea

In the South China Sea, the Paracel and Spratly Islands are hotly contested, in part, because of estimates of their significant oil and gas reserves. Although the area has been under-explored due to territorial disputes among China, Vietnam, the Philippines, and others, there may be up to 11 billion barrels of oil reserves and 190 trillion cubic feet of natural gas reserves in the South China Sea.[121]

In recent years, China, Vietnam, and Malaysia have been dredging and enlarging islands and building large structures on newly reclaimed land.[122] China, in particular, is aggressively building up reefs,[123] and the state-owned China National Offshore Oil Corporation (CNOOC) placed its first oil rig in the Paracels in May 2014, sparking anti-Chinese protests in Vietnam and a rare statement from the United States calling China's actions "provocative and unhelpful to the maintenance of peace and stability in the region."[124] Although China removed the rig in July 2014 reportedly because it completed the task, additional oil rigs are expected to appear in the South China Sea in the coming years.[125] When China places its next oil rig, increased tensions are likely.

Imagine the following hypothetical scenario:

After the typhoon season, China returns its oil rig to the Paracel Islands, announcing its intention to install additional rigs in the coming year. In response, anti-Chinese protests again erupt in Vietnam. To contain the growing unrest and prevent a recurrence of the May 2014 protests that escalated to include other domestic grievances,[126] the Vietnamese government pledges an aggressive response to China's encroachment on its sovereignty. Hanoi urges the international community to condemn China's actions and emphasizes its desire for increased cooperation with the United States as part of the "comprehensive partnership."[127] Meanwhile, Chinese state media is filled with propaganda and negative stories about Vietnam, encouraging already negative populist sentiment about China's neighbors. The two nations step up their naval presence around the Paracels and engage in a dangerous game of chicken—coming within 200 yards of each other's vessels and shooting off flares. The Vietnamese government announces that it intends to hold another live-fire drill in the South China Sea, a repeat of its June 2011 exercise. Tensions reach levels not seen since the 1988 Johnson South Reef crisis when 64 Vietnamese border guards were killed in a Chinese naval attack.[128]

Meanwhile, in the Spratly Islands, there has been a dangerous accident aboard the Filipino ship, the *Sierra Madre*. The formerly American, World War II-era ship was scuttled in 1999 by the Filipino navy and has been an important outpost marking Filipino claims to the nearby reef.[129] Two members of the crew of Filipino marines were seriously injured while attempting to reinforce an area of the ship's near rusted-through hull that had become structurally unsound.

Although the two marines are in stable condition, the decision is made that they require greater medical attention than the crew can provide onboard the ship. The Philippines sends another naval vessel to retrieve and relieve the two injured men, but China repeatedly blocks the ship's attempts to reach the *Sierra Madre*, claiming that the Filipino vessel is carrying military supplies. Although China has previously blocked vessels from resupplying the *Sierra Madre*,[130] tensions on the Paracel Islands prompt a more aggressive response from Chinese vessels, which come dangerously close to ramming the Filipino ship.

The government of the Philippines and its citizens are outraged and request U.S. diplomatic intervention to pressure China to allow the rescue of the injured men. Following private meetings with U.S. officials, Beijing announces that it will send one of its coast guard ships to evacuate the injured marines but on the condition that the rest of the crew also board the Chinese vessel for safe transport back to the Chinese mainland, followed by a flight to

Manila. The Philippines refuses China's offer, recognizing that once the marines are off the *Sierra Madre*, China could sabotage the ship, making the marines' return impossible and removing the barrier to Chinese expansion.

The United States continues to try to negotiate a compromise between China and the Philippines, but the Chinese, Vietnamese, and Filipinos become more entrenched as the international press begins to cover the escalating conflict. Although its bilateral Enhanced Defense Cooperation Agreement with the Philippines does not explicitly require a U.S. response to disputes in the South China Sea,[131] the U.S. administration feels increasing domestic pressure from a wave of press articles and congressional statements about a rising, aggressive China to engage diplomatically to support its ally and stand up to Chinese intimidation. The U.S. administration begins to take a more outspoken approach to the tensions, publicly condemning China's unilateral attempts to change the status quo in the contested region. The United States announces that it is prepared to airlift the injured marines out of the region and that China and the Philippines, and the other nations with claims in the South China Sea, should submit to binding, international arbitration to resolve the territorial disputes and map the lines of each nation's Exclusive Economic Zone.

Outraged by U.S. interference in China's backyard, Beijing reverses its hesitation about using economic sanctions for geopolitical goals (despite its public opposition to sanctions, China banned exports of rare earth minerals to Japan in 2010[132] and used economic and diplomatic pressure in the past to challenge international recognition of Taiwan). China has previously been cautious about the use of economic coercion against Washington, recognizing its mutual dependence on the United States. In 2008, China rejected a Russian proposal to jointly sell each of their holdings in Fannie Mae and Freddie Mac, which would have forced a U.S. government defense of the two institutions and dramatically exacerbated the already serious financial crisis.[133]

Recognizing that direct action against the United State might put its export relationship at risk or cause repercussions for its own economic growth, Beijing decides to employ an indirect approach modeled on the escalation of sanctions on Iran. A direct assault on the U.S. financial system is likely to be unsuccessful given the dollar's preeminence and would likely also prompt a forceful response from the United States. Instead, China decides to target U.S. allies in efforts to convince Washington to remove itself from the South China Sea conflict and concede to Beijing's territorial ambitions.

After first announcing a ban on Chinese energy exploration technology provided to the Philippines, Beijing then declares that it is imposing sanctions on the Philippines and secondary sanctions against those foreign companies and banks doing business with designated Filipino entities.

Markets are initially skeptical of this announcement of "CISADA-like" sanctions, but China begins a full-court press urging European companies to cease their business relationships with Manila. China then identifies a few instances of sub-par reporting of suspicious activity by Filipino banks and urges European banks to close euro-denominated accounts for Filipino customers and correspondent accounts for select Filipino banks at which the suspicious activity occurred. China begins simultaneously to exert diplomatic pressure on other members of FATF's Asia/Pacific Group on Money Laundering[134] to begin a formal review of the Philippines.

At each stage, the United States and U.S. companies serve as a backstop against a severe impact on the Filipino economy. Initially U.S. companies back-fill those contracts that EU firms relinquish while extracting more favorable terms given the risk premium of doing business in the Philippines. Beijing issues statements warning against these relationships and threatens to ban U.S. firms from the Chinese market if they provide goods and services related to the

Philippine's oil exploration. China does not impose secondary sanctions on American companies, concerned that this step could provoke direct retaliation, and satisfied that the replacement contracts alone are costing Manila.

When European banks begin closing correspondent accounts, Filipino non-dollar trade converts to dollars and foreign businesses use banks in New York to transact. However, China soon begins pressuring private American banks to close their correspondent accounts or risk losing access to the Chinese financial system. U.S. banks soon comply, acknowledging the vast difference in the economic scale of China versus the Philippines.

As they become more isolated, Filipino leaders appeal to the United States government to intervene and protect their country's access to international financial markets. The State Department begins pressing federal bank regulators to find a solution to the current situation. In the past, when foreign embassies were having difficulty accessing banking services because banks were concerned about reputational risk associated with any transactions with certain countries, the State Department intervened and urged banks to accept the accounts.[135] In that case, banking regulators also issued guidance alerting banks that they could accept these accounts and still comply with anti-money laundering regulations.[136] However, in this scenario with China and the Philippines, private banks make their own risk assessments and begin closing accounts. The Fed responds by creating a special mechanism at a Federal Reserve bank through which trade can continue in dollars.

Beijing then turns its attention back to the EU and begins urging EU regulators to issue guidance to SWIFT and to the European Central Bank's Target2 euro-clearing system to remove designated Filipino banks from the financial messaging systems. When EU regulators initially respond that the behavior of the banks does not reach a threshold to pose a threat to the financial system and warrant removal from the systems, China slows the renewal of select contracts with EU businesses. These companies interpret this initial move as a warning that Beijing may reduce select imports from the European Union, China's largest trading partner.[137] Meanwhile, strategically placed Chinese ministers and economic advisers raise questions about whether China's purchase of euro-zone junk bonds,[138] particularly those bonds issued by Greece and Italy, are responsible investments. Well-respected economic analysts in Europe and the United States issue reports that a large-scale sale of these bonds would cripple Greece's fragile economy, damage Italy's, and undermine the EU economic recovery.

EU regulators assess that the de-SWIFTing of Filipino banks would be a significant inconvenience for Manila but would not have the devastating impact it had on Iran. At the time of Iran's de-SWIFTing, the country had few remaining access points to international markets. As long as trade can be conducted in dollars, the impact on the Filipino economy would not be profound. Thus unwilling to sacrifice its own economy to save Manila from what is likely to be no more than a costly annoyance, the European Union begins to seriously consider China's request. Acknowledging that China and other BRICS have taken steps to create an alternative international development bank,[139] EU regulators also assess that China may move forward with an alternative messaging system in direct competition with SWIFT if China's geopolitical demands in the South China Sea are not met. SWIFT itself expresses strong reservations to the de-SWIFTing but ultimately must adhere to EU sanctions regulations.

The EU pressures Washington to reconsider its support for the Philippines, Vietnam, and other countries with competing claims over the South China Sea. EU policymakers make it clear to their America counterparts that, in order to protect their bilateral trade interests with Beijing, they may have to consider heightened sanctions against Filipino banks and persons operating in the European Union or European persons operating in the Philippines. Washington is put on notice: If China escalates its economic warfare campaign, the U.S. will have to find a political resolution to the South China Crisis even if it means agreeing to Beijing's demands.

Although the United States has prevented the worst of the economic impact on its ally, it has paid a high political price—increasing tensions not only with China but also with European leaders. SWIFT has indeed become the political football that the U.S. Treasury Department had feared, and the traditional mechanisms of global financial markets are being called into question.

Is Washington prepared to deal with scenarios, like the SWIFT and the South China Sea crisis, where the tools of economic coercion are turned against the U.S. and its allies? While the scenario described above is a hypothetical and, perhaps, a low-probability scenario, it is useful for understanding the challenges that the United States might face. Could Washington implement "whole-of-government" systems and tools to head off other potential economic warfare scenarios and avoid responding to crises in an ad-hoc and ultimately ineffectual way? What economic and policy planning mechanisms ought we have in place to anticipate and manage such a scenario? How can Washington coordinate with the U.S. and international business and financial community to defend American interests and the interests of our allies effectively? The following section offers recommendations to help develop a better whole-of-government approach to defensive economic warfare.

Part 3: Recommendations

Introduction

The offensive and defensive tools of American economic coercion depend on the power of the U.S. dollar. As long as global finance is structured as it is—with the dominance of the U.S. dollar as the currency of choice for global trade and foreign exchange reserves, and with the U.S. Treasury bill seen as the safest investment even during financial crises—the United States enjoys a strong economic advantage. Despite analysts' predictions over the past decade and especially after the 2008 financial crisis that the dollar would lose its preeminence, the overwhelming majority, 87 percent,[140] of international trade is still conducted in U.S. dollars, and about 61 percent of total allocated global foreign exchange reserves is denominated in U.S. dollars.[141]

Yet, countries are looking at non-dollar options. For example, the Chinese credit card UnionPay has taken over nearly half of the global credit card market, with 45 percent of the credit cards in circulation, accepted in 135 countries, and representing 25 percent of transaction volume for the second half of 2012.[142] These credit cards are delinked from New York, providing an alternative for countries facing U.S. sanctions. When MasterCard and Visa froze accounts in Russia in response to U.S. sanctions, designated Russian banks turned to UnionPay as an alternative.[143] Washington and its allies might be exposed to economic coercion and America's own financial warfare tools would be blunted if systems that avoid the dollar grow in prominence. The combination of a Chinese global credit card, an alternative SWIFT system backed by Russia and China, and Chinese and Russian banks willing to defy the global financial order might create that perfect storm.

Based on our discussions with government officials and private sector experts, neither the U.S. government nor the private sector has engaged in serious planning about how to protect America and its allies against economic warfare. As the hypothetical scenario in Part 2 indicates, although other countries may not have the ability to affect the macroeconomic landscape in as profound a way as the United States, Washington can still be forced to make difficult political and economic choices when confronting the use of economic warfare against its interests.

New thinking and new structures are needed to effectively engage in defensive economic warfare. In response to the development of offensive missiles and then missile defense shields, the United States created a Space and Missile Defense Command.[144] In response to the proliferation of cyberattacks, both by the U.S. against its adversaries and by its adversaries against the U.S. and its allies, Washington created a U.S. Cyber Command,[145] crafted a Department of Defense "Strategy of Operating in Cyberspace,"[146] and is expanding CYBERCOM even as the Pentagon, like the rest of the federal government, is facing budget cuts.[147] The evolving power of economic warfare, including cyber-enabled economic warfare, and the willingness of countries like Russia, China, and Iran to devote significant state resources to their offensive cyber capabilities mean that America's adversaries could one day bring down a country's financial system or disrupt millions of miles of critical infrastructure. As it develops cyber command capabilities and defenses, the U.S. government ought to be developing defensive and offensive economic warfare capabilities now rather than waiting for a crisis to occur.

The First Phase of Organizational Rearrangement

In our consultations with U.S. government experts, we have identified three initial changes in organizational structure and legal authorizations for the U.S. to engage more effectively in strategic planning on economic warfare. As part of this initial phase, base-line assessments of U.S. vulnerabilities and existing institutional structures should be undertaken immediately within existing institutional structures without waiting for institutional reform.

These initial changes, and the broader reorganization discussed in the fourth recommendation below, are primarily, although not exclusively, focused on questions of the use of financial sanctions but are also likely to have an impact on broader policy and doctrinal discussions on the broader use of economic warfare strategies. This larger conversation within the U.S. government about the full range of offensive and defensive economic warfare capabilities may yield additional institutional reforms, which are beyond the scope of these recommendations.

1. Create an Office of Policy Planning at the U.S. Department of the Treasury

Unlike the State Department and the Pentagon, the Treasury Department does not have an office responsible for policy planning. The priorities of the policy planning office at the State Department are focused elsewhere. Additionally, as with many bureaucracies, the State Department must balance regional and subject matter experts, career civil servants, and political appointees. Those with economic expertise historically have not played leadership roles in the State Department. Instead, Treasury should have its own policy planning office to examine economic statecraft, economic warfare, and other challenges. The office should report directly to the Secretary of the Treasury. The Treasury has the resources and expertise to take the lead in this area.

This new Office of Policy Planning would emphasize creativity in the development and deployment of new economic tools. It would assemble experts from different offices throughout the department who can bring different expertise and assets to the table, including specialists from the Office of Foreign Assets Control (OFAC)—the office in charge of U.S. sanctions programs—to examine technical regulations and financial sanctions enforcement; experts from the Office of Terrorism and Financial Intelligence (TFI), including those from the Office of Terrorist Financing and Financial Crimes (TFFC) to focus on illicit finance; those from the Office of Intelligence and Analysis (OIA) to share financial intelligence; and the financial crimes experts from the Financial Crimes Enforcement Network (FinCEN); as well as professionals from Treasury's International Affairs office to consider economic warfare and its impact on global markets, financial trading, and other macroeconomic systems. As we have seen in the

application of sanctions on Russia, the intra-agency exchange can create valuable innovations in economic warfare tools. For example, Treasury economists working in international affairs understood the dependence of Russian corporations on external financing while Treasury's sanctions experts knew how to leverage the existing legal authorities to develop new targeted sanctions. The Office of Policy Planning would also build and expand on Treasury's relationship with Congress, which has been a key driver behind the secondary sanctions on Iran. The Office of Policy Planning would also work closely with economic and finance officials in Europe—who developed some of the most creative ideas regarding Russia sanctions because of their countries' own exposure and vulnerabilities—and with foreign ministries around the world.

In the creation of the Iran sanctions architecture, the private sector also played a vital role. The power of "smart sanctions" derived from deep cooperation and interaction between the government and private financial institutions. While TFI would continue to drive the implementation of tools of economic warfare, and its relationships in foreign banking capitals would remain paramount, the new Office of Policy Planning should develop long-range strategies on how to incentivize the private sector to build on the already extensive and effective collaboration and deepen its cooperation with the U.S. government. Treasury's tax, domestic finance, and trade experts, for example, have a valuable role to play in thinking through these strategies.

In today's environment, the creation of a new office would face budgetary challenges. However, Congress' willingness to provide funding for the Treasury Department, specifically TFI, is an exception. In the past, Congress played an important role by authorizing the formation of OIA and driving the creation of TFI, even ahead of White House wishes.[148] In April 2014, at the Senate Appropriations Financial Services Subcommittee hearing on TFI's budget, it was striking how many senators, from both sides of the aisle, asked Undersecretary David Cohen what other resources they could provide.[149] Building on that support, Treasury and Congress should work together to find the necessary budgetary flexibility and funding to create this new office. To create an Office of Policy Planning at Treasury, Congress again should be relied on to do some of the heavy lifting.

2. Set Up an Economic Coercion Directorate at the National Security Council

In addition to more resources within the Treasury Department, U.S. officials have told us that the White House itself needs more staff members who have in-depth understanding of economic tools and view economic coercion as a central component of national security policy making. As the institution that calls, sets the agenda for, and invites participants to inter-agency meetings, the National Security Council needs to play a role in strategic planning around the use of economic warfare tools. The NSC has a directorate of international economics, and thus from this directorate—as a subcomponent or as a reconfiguration of its priorities—a directorate of economic coercion ought to be created. This directorate would also need to interact and coordinate with the National Economic Council (NEC) within the White House because of the important role that the NEC plays in providing advice on domestic and global economic policies.

It is vital that Treasury officials are detailed to, and play a leading role in, this new directorate to ensure that Treasury's resources and expertise on economic suasion are used effectively in inter-agency settings. This directorate would focus broadly on economic coercion and would need to cooperate and perhaps have a permanent cross-directorate mechanism with other experts in the NSC to address specific cyber-enabled offensive and defensive economic warfare.

In addition to budgetary challenges, as we understand from our conversations with U.S. government officials, this new directorate may run up against the orthodoxy within the government that is pro-trade, pro-investment, pro-development, and pro-business. The U.S.

government has traditionally been more focused on how open markets can create political opportunity than on how countries should be isolated from the global economy. For example, rather than thinking about tools of economic coercion that might dissuade Russian aggression toward Ukraine, the U.S. government has focused on what support the International Monetary Fund might provide to Ukraine to help Kiev balance its budget. Despite the leading role that sanctions are playing in today's national security policy—Treasury is reportedly President Obama's "favorite noncombatant command"[150]—we are told that there remains a groupthink within the U.S. government that sanctions don't work and that they hurt innocent people. Tools that restrict economic and financial flows are dismissed and are traditionally sidelined in favor of tools that aid economic growth. A restructuring of the NSC directorate to also include those who have expertise in economic coercion may begin to change this way of thinking.

3. Create a Doctrine on the Use of Economic Coercion

Thus far, sanctions have merely been a tool. Economic coercion has not taken a central role in economic policy planning from an offensive or defensive position. While this is changing with the increasing profile of TFI's role in addressing national security crises,[151] we are told that too few officials outside TFI and select members of the NSC, State, Commerce, and threat finance specialists at the Defense Department truly understand these tools.

The new Office of Policy Planning and Economic Sanctions Directorate should develop and articulate a doctrine on the use of economic coercion. This doctrine could provide a framework for strategic evaluation of when, and how, economic coercion can be effective in policy relevant timeframes. The Defense Department has well-developed doctrines on the use of military force, and it is creating a cyberwarfare doctrine. There is also an increasing interest in developing an all-of-government "lawfare" doctrine to guide how legal tools can be used as instruments of offensive and defensive warfare. The Pentagon has created clear rules of engagement on the use of the tools at its disposal, and so should the Treasury Department and NSC.

For at least the first three years after the creation of CYBERCOM, the Command was reportedly still heavily focused on the development of policy and legal frameworks.[152] Although the Pentagon had issued its Strategy for Operating in Cyberspace in 2011, the 2010 National Security Strategy had stated that cyber threats are "one of the most serious national security, public safety, and economic challenges,"[153] and the 2010 Quadrennial Defense Review had noted that cyberspace is "as relevant a domain for DOD activities as" traditional arenas,[154] the creation of offensive and defensive doctrines of cyberwarfare was still a multiyear process. In 2012, President Obama signed "Presidential Policy Directive 20," establishing secret guidelines for offensive and defensive cyber action,[155] however statements from U.S. officials including President Obama in response to the North Korean hacking of Sony Pictures, reveals that there is not a clear definitions of cyberwarfare, cyberterrorism, or "cybervandalism."[156]

Recognizing that the creation (let alone implementation) of government-wide doctrines requires significant resources, coordination, and time, it is important that the process to develop a "Doctrine on the Use of Economic Coercion" begins immediately, as a precursor to the creation of an Economic Warfare Command, as discussed below.

The development of a doctrine may also help the United States in broader, international discussions about the application and legitimacy of economic warfare and to defend against the use of these tools in unacceptable ways by America's adversaries. In developing a system of rules and norms to govern the use of economic warfare, as it has for the use of force and is developing in the cyber realm, the U.S. can bolster its defenses against the unacceptable use of economic coercion.

4. Second Phase: The Creation of an Economic Warfare Command

In addition to mechanisms to address the use of economic warfare, a more system-wide change should be considered to develop an Economic Warfare Command, ECONCOM. This Command would become the locus for developing and leveraging offensive coercion and incentive tools and for devising and building proactive strategies of economic defense Housed at the Treasury Department and led by TFI with close coordination with the Treasury Office of Policy Planning, this new command would coordinate and draw assets from within Treasury and across the federal government. Placing ECONCOM at Treasury would be unique as even CYBERCOM, which is led by the director of the National Security Agency, is housed within the Department of Defense.

More so than perhaps any of the other commands, ECONCOM would depend on the participation of a wide range of officials, who would be detailed to the Command from throughout the government. ECONCOM would also depend on its ability to requisition additional assets from agencies and therefore must be given that authority. We recommend housing ECONCOM at the Treasury Department not because Treasury has exclusive expertise on tools of economic coercion but because the U.S. Treasury's mission includes protecting the integrity of the global financial system. The international community's, and specifically foreign financial institutions', understanding and acceptance of this particular component of Treasury's mission has been important for isolating illicit financial activity and rogue actors identified by Treasury. Building on Treasury's reputation will likely be important for ECONCOM's success.

With Treasury in the lead, ECONCOM would require the coordination of a number of key assets. The Commerce Department's Bureau of Industry and Security would provide expertise on export control issues and the U.S. Trade Representative on issues of U.S. trade relationships. Homeland Security Investigations (HSI) would provide assets related to illicit procurement and customs enforcement, and the Drug Enforcement Agency (DEA) would bring its significant investigatory and intelligence skills into illicit networks to ECONCOM. The State Department's Coordinator for Sanctions Policy and Office of Economic Sanctions Policy and Implementation would be central components of ECONCOM, and State's regional desks would be called upon on an ad hoc basis in order to provide country- and region-specific information and data.

As the Department of Defense continues to step up its Anti-Money Laundering (AML) and Counter Threat Financing programs, the Pentagon would be an ex-officio member of this new command. With the recognition of the financial independence of the Islamic State (also called ISIL), new conversations are developing about the interplay between kinetic options and economic assets. This discussion builds on the Pentagon's Counter Threat Finance (CTF) Policy, which states that DOD will engage in strategic planning around CTF and integrate interagency representatives into DOD planning as necessary.[157] As these conversations continue, the Defense Department's role in ECONCOM may grow such that DOD is no longer ex-officio but rather a full member of the command.

ECONCOM would need to work closely with federal banking regulators who not only set standards and policy but also can help develop creative defensive tools. Representatives of the Federal Reserve ought to be detailed to ECONCOM in order to coordinate with those in charge of monetary policy. There may also be requirements for the Fed to issue guidance to U.S. banks or to create work-arounds like the opening of accounts at federal institutions on behalf of allies who may find themselves under economic attack.

It would also be important for this command to develop strong working relationships with the enforcement team at the Justice Department and officials in New York. ECONCOM would need to build a close working relationship with the DOJ as well as closely coordinate with the Superintendent of Financial Services (New York's financial regulator), who has prosecuted

banks for sanctions violations,[158] and the Manhattan District Attorney's Office and the office of the U.S. Attorney for the Southern District of New York, which have also played leading roles in terrorism and sanctions-related cases.

The Economic Warfare Command would also require a large intelligence component, drawing on assets from across the intelligence community. Treasury's OIA has traditionally been a consumer and analyst rather than a collector of intelligence although it plays a leading role in the intelligence community's counter-threat finance efforts. While OIA would continue to play a leading role in the analysis of FININT, the Director of National Intelligence would need to coordinate across the CIA, DIA, and other intelligence agencies to ensure that their agents and analysts are collecting FININT and other useful intelligence for analysis by OIA and others. Conversations with former U.S. government officials in unclassified settings indicate that this coordination is already ongoing and effective.

In addition to offensive financial sanctions like those we have seen from Treasury in the past decade, the new Command would address the broad scope of U.S. economic persuasion and coercion—both offensive and defensive measures and tools of both isolation and inclusion. Coordination between financial and economic experts from Treasury with cyberwarfare experts at CYBERCOM would likely be necessary for the development and implementation of offensive and defensive cyber-enabled economic warfare tools. The two very different perspectives that these experts would bring to policy discussions would likely be a force multiplier of what each could develop and implement separately. Discussions about CYBERCOM's relationship with the private sector—as well as Treasury's experience working with SWIFT to create the Terrorist Finance Tracking Program—can also help inform ECONCOM's development of relationships with the private sector.

U.S. Cyber Command was initially created as a sub-command of the U.S. Strategic Command and is scheduled to become a full, unified command by the beginning of 2015.[159] Explaining the importance of this step, then-NSA Director and head of CYBERCOM Gen. Keith Alexander testified before a House Armed Services Committee hearing that the main reason is "command and control, directly from the President and the Secretary [of Defense], directly to that commander."[160] A similar lesson should be applied to ECONCOM—that it should be a full, unified command so that the leadership has direct chain of command to the president.

Unlike CYBERCOM, which was—in part at least—built on more than a decade of military engagement with cyber and information warfare against the United States,[161] ECONCOM has less precedent from which to draw; economic warfare has been overwhelmingly offensive not defensive.[162] The creation of this command, however, depends upon the creativity and innovation of policymakers to analyze and prepare for over-the-horizon threats.

Conclusion

Cyber-enabled economic warfare tools like the SWIFT financial messaging system have reshaped the mechanisms and levers of global statecraft. Economic sanctions had been dismissed for decades as ineffective until the debate shifted following the implementation of smart sanctions against Iran as a result of its illicit financial activities in support of its nuclear program and international terrorism. The ever-tightening financial isolation of Iran, including the first-ever expulsion of a country's banks from SWIFT, changed Tehran's tactics from nuclear defiance to international negotiations (whether or not this economic pressure however will change Iran's objective of a nuclear weapons capability still remains to be seen[163]). The use of sanctions against Iran, Russia, Syria, and non-state actors such as al-Qaeda, the Islamic State, Hezbollah, Hamas, and others demonstrated that economic warfare can be an important tool

but cannot work in isolation; it is one instrument to be wielded in conjunction with the full range of national power to address national security threats.

Over the past decade, the United States government—led by the U.S. Treasury with vital input and pressure from Congress—has developed its economic warfare offensive capabilities but neglected defensive planning. With the challenge by states such as China and Russia to the U.S.-led international order, including to the preeminence of the U.S. dollar, economic warfare against the United States and its allies is a growing threat. While U.S. legislators and British officials contemplate de-SWIFTing Russian banks, Russian officials are considering creating an alternative SWIFT system with Chinese cooperation, to create a financial network that is unlikely to meet high standards of financial integrity. Meanwhile, Palestinian activists are pressuring SWIFT, so far unsuccessfully, to expel Israeli banks, raising concerns that SWIFT may become a political football.

A whole-of-government approach to hardening defenses against economic warfare is required to protect America and its allies. If we can envision a hypothetical scenario involving the use of SWIFT in a crisis in the South China Sea, in which economic warfare becomes a threat to U.S. interests and allies, our enemies no doubt can as well.

---

[1] Jose W. Fernandez, "Smart Sanctions: Confronting Security Threats with Economic Statecraft," *Remarks at the San Francisco World Affairs Council*, July 25, 2012. (http://www.state.gov/e/eb/rls/rm/2012/196875.htm)

[2] Foundation for Defense of Democracies, Press Release, "New Report Reveals Iran's Terror Network in Latin America," May 30, 2013. (http://www.defenddemocracy.org/media-hit/new-report-reveals-irans-terror-network-in-latin-america/)

[3] "SWIFT Mission," *SWIFT Website,* accessed January 9, 2012. (http://www.swift.com/about_swift/company_information/swift_history.page?)

[4] "Company Information," *SWIFT Website*, accessed October 23, 2014. (http://www.swift.com/about_swift/company_information/company_information?rdct=t&lang=en)

[5] "Company Information," *SWIFT Website,* accessed January 9, 2012. (http://www.swift.com/info?lang=en)

[6] Josh Meyer and Greg Miller, "U.S. Secretly Tracks Global Bank Data," *Los Angeles Times*, June 23, 2006. (http://articles.latimes.com/2006/jun/23/nation/na-swift23)

[7] Leonard H. Schrank and Juan C. Zarate, "Data Mining, Without Big Brother," *The New York Times*, July 2, 2013. (http://www.nytimes.com/2013/07/03/opinion/data-mining-without-big-brother.html?ref=opinion&_r=0)

[8] Juan Zarate, *Treasury's War: The Unleashing of a New Era of Financial Warfare*, (New York: PublicAffairs, 2013), pages 51-60.

[9] Glenn Simpson, "Treasury Tracks Financial Data in Secret Program," *The Wall Street Journal*, June 23, 2006. (http://online.wsj.com/news/articles/SB115101988281688182)

[10] Eric Lichtblau and James Risen, "Bank Data Is Sifted by U.S. in Secret to Block Terror," *The New York Times*, June 23, 2006. (http://www.nytimes.com/2006/06/23/washington/23intel.html?pagewanted=all)

[11] "Hambali: 'Asia's Bin Ladin,'" *BBC News*, September 6, 2006. (http://news.bbc.co.uk/2/hi/asia-pacific/2346225.stm)

[12] Glenn Simpson, "Treasury Tracks Financial Data in Secret Program," *The Wall Street Journal*, June 23, 2006. (http://online.wsj.com/news/articles/SB115101988281688182)

[13] Ibid.

[14] Juan Zarate, *Treasury's War: The Unleashing of a New Era of Financial Warfare*, (New York: PublicAffairs, 2013), pages 270-274; Josh Meyer and Greg Miller, "U.S. Secretly Tracks Global Bank Data," *Los Angeles Times*, June 23, 2006. (http://articles.latimes.com/2006/jun/23/nation/na-swift23)

[15] Juan Zarate, *Treasury's War: The Unleashing of a New Era of Financial Warfare*, (New York: PublicAffairs, 2013), pages 269-270.

[16] Ibid, pages 279-280.

[17] "European Swift Bank Data Ban Angers U.S.," *BBC News*, February 11, 2010. (http://news.bbc.co.uk/2/hi/europe/8510471.stm)

[18] Robin Emmott, "EU Lawmakers Seek to Block U.S. Financial Spying," *Reuters*, October 23, 2013. (http://www.reuters.com/article/2013/10/23/us-eu-us-security-idUSBRE99M0OR20131023)

[19] "State Sponsors of Terrorism," *U.S. Department of State Website*, accessed June 13, 2014. (http://www.state.gov/j/ct/list/c14151.htm)

[20] Robin Wright, "Stuart Levey's War," *The New York Times*, November 2, 2008. (http://www.nytimes.com/2008/11/02/magazine/02IRAN-t.html?pagewanted=all&_r=0)

[21] Juan Zarate, *Treasury's War: The Unleashing of a New Era of Financial Warfare*, (New York: PublicAffairs, 2013), pages 300-302.

[22] Ibid, page 296.

[23] U.S. Department of the Treasury, Press Release, "Treasury Designates Major Iranian State-Owned Bank," January 23, 2012. (http://www.treasury.gov/press-center/press-releases/Pages/tg1397.aspx)

[24] Bank Sepah (Iran); Bank Melli (Iran); Arian Bank (Iran); Bank Kargoshaee (Iran), controlled by Bank Melli; Future Bank (Bahrain), controlled by Bank Melli; Post Bank of Iran (Iran), controlled by Bank Sepah; Ansar Bank (Iran); Mehr Bank (Iran).

[25] U.S. Department of the Treasury, Press Release, "Treasury Cuts Iran's Bank Saderat Off From U.S. Financial System," September 8, 2006. (http://www.treasury.gov/press-center/press-releases/Pages/hp87.aspx)

[26] "United Nations Sanctions," *Foundation for Defense of Democracies Website*, accessed October 28, 2014. (http://defenddemocracy.org/united-nations-sanctions)

[27] U.S. House of Representatives, 111th Congress, 2nd Session, P.L. 111-195, "Comprehensive Iran Sanctions, Accountability, and Divestment Act of 2010," *Government Printing Office*, 2010. (http://www.treasury.gov/resource-center/sanctions/Documents/hr2194.pdf)

[28] William Burns, "Implementing Tougher Sanctions on Iran: A Progress Report," *Testimony before the House Foreign Affairs Committee*, December 1, 2010. (http://www.state.gov/p/us/rm/2010/152222.htm).

[29] U.S. Department of State, "Country Reports on Terrorism 2013," April 2014, pages 228-230. (http://www.state.gov/j/ct/rls/crt/2013/224826.htm)

[30] Thomas Joscelyn, "Treasury 'Further Exposes' Iran-al Qaeda Relationship," *The Long War Journal*, October 18, 2012. (http://www.longwarjournal.org/archives/2012/10/treasury_further_exp.php)

[31] SWIFT, Press Release, "SWIFT Selects Sword FircoSoft to Support New Centralised Sanctions Screening Service," May 4, 2011. (http://www.swift.com/news/press_releases/sanctions_screening)

[32] "Sanctions Screening Over SWIFT - Details," *SWIFT Website,* accessed January 9, 2012. (http://www.swift.com/products/sanctions_screening/details?lang=en)

[33] "Sanctions Screening Over SWIFT," *SWIFT Website,* August 2011, page 2. (http://www.swift.com/dsp/resources/documents/ip_sanctions_screening.pdf)

[34] U.S. Department of the Treasury, Press Release, "Fact Sheet: New Sanctions on Iran," November 21, 2011. (http://www.treasury.gov/press-center/press-releases/Pages/tg1367.aspx)

[35] U.S. Department of the Treasury, Press Release, "Fact Sheet: Treasury Amends Iranian Financial Sanctions Regulations to Implement the National Defense Authorization Act," February 27, 2012. (http://www.treasury.gov/press-center/press-releases/Pages/tg1434.aspx)

[36] U.S. Energy Information Administration, "Sanctions Reduced Iran's Oil Exports and Revenues in 2012," April 26, 2013. (http://www.eia.gov/todayinenergy/detail.cfm?id=11011)

[37] "Annual Review 2010," *SWIFT Website,* accessed January 9, 2012, page 29. (http://www.swift.com/about_swift/publications/annual_reports/annual_review_2010/SWIFT_AR2010.pdf)

[38] Editorial, "Swift Sanctions on Iran," *The Wall Street Journal*, February 1, 2012. (http://online.wsj.com/news/articles/SB10001424052970203718504577178902535754464)

[39] "SWIFT Corporate Rules," *SWIFT Website*, accessed September 6, 2014. (http://www.swift.com/about_swift/legal/swift_corporate_rules?rdct=t)

[40] "Decision of the European Central Bank of 2 November 2010 Amending Decision ECB/2007/7 Concerning the Terms and Conditions of TARGET2-ECB," *Official Journal of the European Union*, November 2, 2010, page 2. (https://www.ecb.europa.eu/ecb/legal/pdf/l_29020101106en00530055.pdf)

[41] "Swift Sanctions on Iran," *The Wall Street Journal*, February 1, 2012. (http://online.wsj.com/news/articles/SB10001424052970203718504577178902535754464)

[42] Senator Robert Menendez, Press Release, "Menendez Hails Banking Committee Passage of Iran Sanctions Legislation," February 2, 2012. (http://www.menendez.senate.gov/newsroom/press/menendez-hails-banking-committee-passage-of-iran-sanctions-legislation)

[43] "Payments System SWIFT to Expel Iranian Banks Saturday," *Reuters*, March 15, 2012. (http://www.reuters.com/article/2012/03/15/us-nuclear-iran-idUSBRE82E15M20120315)

[44] Rick Gladstone and Stephen Castle, "Global Network Expels as Many as 30 of Iran's Banks in Move to Isolate Its Economy," *The New York Times*, March 16, 2012. (http://www.nytimes.com/2012/03/16/world/middleeast/crucial-communication-network-expelling-iranian-banks.html?_r=0)

[45] SWIFT, Press Release, "SWIFT Instructed to Disconnect Sanctioned Iranian Banks Following EU Council Decision," March 15, 2012. (http://www.swift.com/news/press_releases/SWIFT_disconnect_Iranian_banks)

[46] Rachelle Younglai and Roberta Rampton, "U.S. Pushes EU, SWIFT to Eject Iran Banks," *Reuters*, February 15, 2012. (http://www.reuters.com/article/2012/02/16/us-iran-usa-swiftidUSTRE81F00I20120216)

[47] The full text of the Turkish prosecutor's report can be accessed online. Istanbul Cumhuriyet Bassavciligi, "Sorusturma No: Istanbul CBS 2012/120653," December 18, 2013. (http://www.cumhuriyet.com.tr/haber/turkiye/50525/Fezlekeleri_indirmek_icin_tiklayin.html)

[48] Jonathan Schanzer and Emanuele Ottolenghi, "Turkey's Teflon Don," *Foreign Policy*, March 31, 2014. (http://www.foreignpolicy.com/articles/2014/03/31/turkey_teflon_don_erdogan_elections_corruption)

[49] "87 Billion Euros in Suspicious Transfers From Iran," *Today's Zaman* (Turkey), December 17, 2013. (http://www.todayszaman.com/news-334277-87-billion-euros-in-suspicious-transfers-from-iran.html)

[50] "Turkish Prosecutors Drop Corruption Case Against Ex-Ministers' Sons," *The Guardian* (U.K.), October 17, 2014; (http://www.theguardian.com/world/2014/oct/17/turkish-prosecutors-drop-corruption-case); Daniel Dombey, "Turkish Prosecutor Drops High-Level Corruption Probe," *The Financial Times*, October 18, 2014. (http://www.ft.com/intl/cms/s/0/63cf5042-56cb-11e4-a0b2-00144feab7de.html#axzz3H4OzdDSf)

[51] Daniel Dombey, "Turkish Prosecutor Drops High-Level Corruption Probe," *The Financial Times*, October 18, 2014. (http://www.ft.com/intl/cms/s/0/63cf5042-56cb-11e4-a0b2-00144feab7de.html#axzz3H4OzdDSf)

[52] "Turkey's Massive Corruption Case Dropped by Prosecutor," *Hurriyet Daily News* (Turkey), October 17, 2014. (http://www.hurriyetdailynews.com/turkeys-massive-corruption-case-dropped-by-prosecutor.aspx?pageID=238&nID=73149&NewsCatID=338)

[53] "Turkish Prosecutors Drop Corruption Investigation That Had Rocked the Government," *Associated Press*, October 18, 2014. (http://www.usnews.com/news/world/articles/2014/10/18/turkish-prosecutors-drop-corruption-probe)

[54] "Members and Partners," *Organization for Economic Co-operation and Development Website*, accessed October 24, 2014. (http://www.oecd.org/about/membersandpartners/)

[55] "OECD 'Seriously Concerned' About How Turkey Investigates Bribery," *Today's Zaman* (Turkey), October 23, 2014. (http://www.todayszaman.com/business_oecd-seriously-concerned-about-how-turkey-investigates-bribery_362465.html)

[56] For an overview of the AKP's response, see Merve Tahiroglu, "Turkey's War on Rule of Law: One Year On," *Foundation for Defense of Democracies*, December 17, 2014. (http://defenddemocracy.org/media-hit/merve-tahiroglu-turkeys-war-on-rule-of-law-one-year-on/)

[57] "Turkish Court Issues Media Ban on Inquiry Into Corruption," *Hurriyet Daily News* (Turkey), November 26, 2014. (http://www.hurriyetdailynews.com/turkish-court-issues-media-ban-on-inquiry-into-corruption.aspx?pageID=238&nID=74831&NewsCatID=338)

[58] Peter Foster, "U.S. Congress in Urgent Call to ECB to Tighten Sanctions on Iran," *The Telegraph* (U.K.), February 26, 2013. (http://www.telegraph.co.uk/news/worldnews/middleeast/iran/9894143/U.S.-Congress-in-urgent-call-to-ECB-to-tighten-sanctions-on-Iran.html)

[59] U.S. House of Representatives, 112th Congress, 2nd Session, H.R. 1905, "Iran Threat Reduction and Syria Human Rights Act of 2012," Sec. 220: Reports on, and Authorization of Imposition of Sanctions With Respect to, the Provision of Specialized Financial Messaging Services to the Central Bank of Iran and Other Sanctioned Iranian Financial Institutions," *Government Printing Office*, 2012, page 24. (http://www.gpo.gov/fdsys/pkg/BILLS-112hr1905enr/pdf/BILLS-112hr1905enr.pdf)

[60] U.S. House of Representatives, 113th Congress, 1st Session, H.R. 850, "Nuclear Iran Prevention Act of 2013," *Government Printing Office*, 2013, page 29. (https://beta.congress.gov/bill/113th-congress/house-bill/850)

[61] U.S. Senate, 113th Congress, 1st Session, S. 1881, "Nuclear Weapon Free Iran Act of 2013," *Government Printing Office*, 2013, page 29. (http://beta.congress.gov/bill/113th-congress/senate-bill/1881)

[62] "S.1881—Nuclear Weapon Free Iran Act of 2013," *Congress.Gov*, accessed July 3, 2014; (https://beta.congress.gov/bill/113th-congress/senate-bill/1881/cosponsors); Rosie Gray, "Senate Reaches Veto-Proof Majority on Iran Sanctions," *BuzzFeed*, January 10, 2014. (http://www.buzzfeed.com/rosiegray/senate-reaches-veto-proof-majority-on-iran-sanctions)

[63] Carol Lee and Jay Solomon, "Obama Issues Rare Veto Threat on Iran Bill," *The Wall Street Journal*, December 19, 2013. (http://online.wsj.com/news/articles/SB10001424052702304866904579268611658114286)

[64] Thomas Erdbrink and Mark Landler, "Iran Said to Seek a Nuclear Accord to End Sanctions," *The New York Times*, September 19, 2013; (http://www.nytimes.com/2013/09/20/world/middleeast/iran-said-to-seek-a-nuclear-accord-to-end-sanctions.html?pagewanted=all&_r=0) ; Christopher Harress, "Iran's Rouhani Faces Music as Sanctions Bite Harder, Is There a SWIFT Solution in the Works?," *International Business Times*, October 8, 2013. (http://www.ibtimes.com/irans-rouhani-faces-music-sanctions-bite-harder-there-swift-solution-works-1417768)

[65] Jeremy Binnie, "Russia Cancels Syrian S-300 Deal," *IHS Janes 360*, August 13, 2014; (http://www.janes.com/article/41819/russia-cancels-syrian-s-300-deal); "'First Shot': Iran Tests Bavar-373 System Aimed to Substitute Russian S-300," *RT* (Russia), August 30, 2014. (http://rt.com/news/183856-bavar373-missile-iran-s300/)

[66] Laurence Norman, "U.S. Warns on Potential Russia-Iran Oil Deal," *The Wall Street Journal*, April 4, 2014. (http://online.wsj.com/articles/SB10001424052702303847804579481683785277324)

[67] "Nuclear Power in Iran," *World Nuclear Association Website*, September 2014. (http://www.world-nuclear.org/info/Country-Profiles/Countries-G-N/Iran/)

[68] Paul Richter, "Russia Threatens to Halt Cooperation With U.S. on Iran, Syria," *Los Angeles Times*, December 30, 2014. (http://www.latimes.com/world/europe/la-fg-russia-us-iran-syria-20141230-story.html?elq=d8ef9b8af38d4fffa7f8fd858fce9790&elqCampaignId=3962)

[69] "Executive Order 13660—Blocking Property of Certain Persons Contributing to the Situation in Ukraine," *Federal Register*, March 10, 2014; (http://www.treasury.gov/resource-center/sanctions/Programs/Documents/ukraine_eo.pdf) "Executive Order 13661—Blocking Property of Additional Persons Contributing to the Situation in Ukraine," *Federal Register*, March 19, 2014; (http://www.treasury.gov/resource-center/sanctions/Programs/Documents/ukraine_eo2.pdf) "Executive Order 13662—Blocking Property of Additional Persons Contributing to the Situation in Ukraine," *Federal Register*, March 24, 2014; (http://www.treasury.gov/resource-center/sanctions/Programs/Documents/ukraine_eo3.pdf) ; "Executive Order 13685—Blocking Property of Certain Persons and Prohibiting Certain Transactions With Respect to the Crimea Region of Ukraine," *Federal Register*, December 19, 2014. (http://www.treasury.gov/resource-center/sanctions/Programs/Documents/ukraine_eo4.pdf)

[70] A group major industrial countries including Canada, France, Germany, Italy, Japan, the United Kingdom, and the United States formed to "monitor developments in the world economy." "A Guide to Committees, Groups, and Clubs," *International Monetary Fund Website*, October 3, 2014. (http://www.imf.org/external/np/exr/facts/groups.htm#G7)

[71] European Council, Press Release, "G7 The Hague Declaration," March 24, 2014. (http://www.consilium.europa.eu/uedocs/cms_data/docs/pressdata/en/ec/141855.pdf)

[72] Boris Groendahl and Irina Reznik, "Bank Rossiya Is First Russian Lender Under U.S. Sanctions," *Bloomberg News*, March 20, 2014. (http://www.bloomberg.com/news/2014-03-20/bank-rossiya-becomes-first-russian-lender-under-u-s-sanctions.html)

[73] Tim Fernholz, "The U.S. Crackdown on Russia's Oligarchs Begins in Earnest," *Quartz*, March 20, 2014. (http://qz.com/190465/the-us-crack-down-on-russias-oligarchs-begins-in-earnest/)

[74] Boris Groendahl and Irina Reznik, "Bank Rossiya Is First Russian Lender Under U.S. Sanctions," *Bloomberg News*, March 20, 2014. (http://www.bloomberg.com/news/2014-03-20/bank-rossiya-becomes-first-russian-lender-under-u-s-sanctions.html)

[75] U.S. Department of State, Press Statement, "United States Expands Export Restrictions on Russia," April 28, 2014; (http://www.state.gov/r/pa/prs/ps/2014/04/225241.htm); Council of the European Union, Press Release, "Reinforced Restrictive Measures Against Russia," September 11, 2014. (http://www.consilium.europa.eu/uedocs/cms_data/docs/pressdata/EN/foraff/144868.pdf)

[76] Department of Commerce, Bureau of Industry and Security, "Russian Oil Industry Sanctions and Addition of Persons to Entry List," August 1, 2014; (http://www.bis.doc.gov/index.php/forms-

documents/doc_download/1027-russian-oil-industry-sanctions-and-addition-of-person-to-the-entity-list) ; Maria Gallucci, "New Russia Sanctions: Latest EU Moves on Russian Oil Sector Would Hinder Drilling in Arctic Ocean and Shale Fields," *International Business Times*, July 29, 2014. (http://www.ibtimes.com/new-russia-sanctions-latest-eu-moves-russian-oil-sector-would-hinder-drilling-arctic-ocean-1642528)

77 Peter Baker, Alan Cowell, and James Kanter, "Coordinated Sanctions Aim at Russia's Ability to Tap Its Oil Reserves," *The New York Times*, July 29, 2014. (http://www.nytimes.com/2014/07/30/world/europe/european-sanctions-russia.html?gwh=C5894D30748D4BA5BCC7B326F137E9E2&gwt=pay&assetType=nyt_now&_r=0)

78 Victoria Butenko, Laura Smith-Spark and Diana Magnay, "U.S. Official Says 1,000 Russian Troops Have Entered Ukraine," *CNN*, August 29, 2014; (http://www.cnn.com/2014/08/28/world/europe/ukraine-crisis/); Adam Taylor, "Has Russia Invaded Ukraine? Here's What We Know," *The Washington Post*, August 28, 2014. (http://www.washingtonpost.com/blogs/worldviews/wp/2014/08/28/has-russia-invaded-ukraine-heres-what-we-know/)

79 Dan Roberts, "Sweeping New U.S. and EU Sanctions Target Russia's Banks and Oil Companies," *The Guardian* (U.K.), September 12, 2014. (http://www.theguardian.com/world/2014/sep/12/russia-sanctions-us-eu-banks-sberbank-oil-gazprom)

80 U.S. Department of the Treasury, Press Release, "Announcement of Expanded Treasury Sanctions Within the Russian Financial Services, Energy and Defense or Related Materiel Sectors," September 12, 2014. (http://www.treasury.gov/press-center/press-releases/Pages/jl2629.aspx)

81 Peter Baker and Andrew Higgins, "U.S. and European Sanctions Take Aim at Putin's Economic Efforts," *The New York Times*, September 12, 2014. (http://www.nytimes.com/2014/09/13/world/europe/european-union-details-tightened-sanctions-against-russia.html?emc=edit_th_20140913&nl=todaysheadlines&nlid=46684088)

82 "Nonproliferation Sanctions," *U.S. State Department Website*, September 16, 2014. (http://www.state.gov/t/isn/226423.htm)

83 Jay Solomon, "Ties to Russian Arms Supplier Snarl U.S. Sanctions Efforts," *The Wall Street Journal*, March 28, 2014. (http://online.wsj.com/news/articles/SB10001424052702304688104579467542674720908)

84 "FATF Members and Observers," *Financial Action Task Force Website*, accessed June 23, 2014. (http://www.fatf-gafi.org/pages/aboutus/membersandobservers/)

85 "Countries" *Financial Action Task Force Website*, accessed January 21, 2015. (http://www.fatf-gafi.org/countries/)

86 Eli Lake, "NATO Plans New Military Outposts to Stop Putin—Just Don't Call Them Bases," *The Daily Beast*, September 3, 2014. (http://www.thedailybeast.com/articles/2014/09/03/nato-plans-new-military-outposts-to-stop-putin-just-don-t-call-them-bases.html?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A+thedailybeast%2Farticles+%28The+Daily+Beast+-+Latest+Articles%29)

87 Brett Logiurato, "The UK Has a Plan to Cut Off Russian Businesses From the Rest of the World," *Business Insider*, August 29, 2014. (http://www.businessinsider.com/russian-sanctions-swift-banking-ban-ukraine-putin-2014-8)

88 Robert Hutton and Ian Wishart, "U.K. Wants EU to Block Russia From SWIFT Banking Network," *Bloomberg News*, August 29, 2014. (http://www.bloomberg.com/news/2014-08-29/u-k-wants-eu-to-block-russia-from-swift-banking-network.html)

[89] Laurence Norman. "European Union Considers Modest Increase in Sanctions on Russia," *The Wall Street Journal*, September 2, 2014. (http://online.wsj.com/articles/european-union-to-decide-on-russia-sanctions-by-friday-1409654982)

[90] Jack Farchy, "Russia's Central Bank to Help Companies Refinance Debts," *The Financial Times*, December 24, 2014. (http://www.ft.com/intl/cms/s/0/6ef85db6-8b6d-11e4-be89-00144feabdc0.html?siteedition=intl#axzz3PUtNKst1)

[91] Mikhail Klikushin, "Top Russian Banker and Putin Confidante Threatens U.S. with 'War,'" *New York Observer*, December 4, 2014. (http://observer.com/2014/12/top-russian-banker-and-putin-confidante-threatens-us-with-war/)

[92] Mikhail Klikushin, "Top Russian Banker and Putin Confidante Threatens U.S. with 'War,'" *New York Observer*, December 4, 2014. (http://observer.com/2014/12/top-russian-banker-and-putin-confidante-threatens-us-with-war/)

[93] U.S. Department of the Treasury, Press Release, "Announcement of Additional Treasury Sanctions on Russian Financial Institutions and on a Defense Technology Entity," July 29, 2014. (http://www.treasury.gov/press-center/press-releases/Pages/jl2590.aspx)

[94] Ambrose Evans-Pritchard, "The Week the Dam Broke in Russia and Ended Putin's Dreams," *The Telegraph* (U.K.), December 23, 2014. (http://www.telegraph.co.uk/finance/economics/11305146/The-week-the-dam-broke-in-Russia-and-ended-Putins-dreams.html)

[95] Michael Crowley, "Is Obama Destroying the Russian Economy?," *Politico*, December 16, 2014. (http://www.politico.com/story/2014/12/barack-obama-vladimir-putin-russian-economy-113626.html)

[96] "Russia Is Losing Up to $140 Billion Per Year From Western Sanctions and Oil Price Fall," *Agence France-Presse*, November 24, 2014. (http://www.businessinsider.com/afp-russia-to-lose-some-40-bn-a-year-due-to-sanctions-minister-2014-11)

[97] Anthony DiPaola, "Saudi Arabia Says Hard for OPEC to Give Up Market Share," *Bloomberg News*, December 18, 2014. (http://www.bloomberg.com/news/2014-12-18/saudi-arabia-s-naimi-says-difficult-for-opec-to-cut-oil-output.html)

[98] Michael Moran, "Is Saudi Arabia Trying to Cripple American Fracking?," *Foreign Policy*, December 23, 2014. (http://foreignpolicy.com/2014/12/23/is-saudi-arabia-trying-to-cripple-american-fracking-oil-iran/)

[99] Carol Matlack, "Swift Justice: One Way to Make Putin Howl," *Bloomberg*, September 4, 2014. (http://www.businessweek.com/articles/2014-09-04/ultimate-sanction-barring-russian-banks-from-swift-money-system)

[100] Gillian Tett, "The Hidden Cost of Freezing Russia Out of Finance," *The Financial Times*, October 2, 2014. (http://www.ft.com/intl/cms/s/0/2adebf9c-48c1-11e4-9f63-00144feab7de.html)

[101] Carol Matlack, "Swift Justice: One Way to Make Putin Howl," *Bloomberg*, September 4, 2014. (http://www.businessweek.com/articles/2014-09-04/ultimate-sanction-barring-russian-banks-from-swift-money-system)

[102] Gillian Tett, "The Hidden Cost of Freezing Russia Out of Finance," *The Financial Times*, October 2, 2014. (http://www.ft.com/intl/cms/s/0/2adebf9c-48c1-11e4-9f63-00144feab7de.html)

[103] "Money Laundering," *U.S. Immigration and Customs Enforcement Website*, accessed September 13, 2014. (http://www.ice.gov/money-laundering/)

[104] Jonathan Schanzer and Emanuele Ottolenghi, "Turkey's Teflon Don," *Foreign Policy*, March 31, 2014. (http://www.foreignpolicy.com/articles/2014/03/31/turkey_teflon_don_erdogan_elections_corruption)

[105] Rachelle Younglai, "U.S. Cracks Down on Iran's Oil Tanker Company, Exposes Fronts," *Reuters*, July 12, 2012. (http://www.reuters.com/article/2012/07/12/us-usa-iran-sanctions-idUSBRE86B12I20120712)

[106] Jonathan Saul, "Call Me Brawny: Iran Defends Tankers Alias Game," *Reuters*, August 2, 2012. (http://www.reuters.com/article/2012/08/02/iran-tankers-nitc-idUSL6E8IVD5D20120802)

[107] U.S. Department of the Treasury, Press Release, "Major Iranian Shipping Company Designated for Proliferation Activity," September 10, 2008. (http://www.treasury.gov/press-center/press-releases/Pages/hp1130.aspx)

[108] Peg Mackey, "Insight: Catch Me If You Can - Oil Sanctions Against Iran," *Reuters*, March 6, 2012. (http://www.reuters.com/article/2012/03/06/us-iran-oil-sanctions-idUSTRE8250UG20120306)

[109] For additional examples of sanction-busting schemes, see Mark Dubowitz, "So You Want to Be a Sanctions-Buster," *Foreign Policy*, August 10, 2012. (http://www.foreignpolicy.com/articles/2012/08/10/so_you_want_to_be_a_sanctions_buster)

[110] "Resource Center: Foreign Sanctions Evaders (FSE) list," *U.S. Department of the Treasury Website*, accessed September 13, 2014. (http://www.treasury.gov/resource-center/sanctions/SDN-List/Pages/fse_list.aspx)

[111] For a more in depth study on the "digital economy" and illicit activities, see The Digital Economy Task Force, "The Digital Economy: Potential, Perils, and Promises," Thomson Reuters and the International Centre for Missing and Exploited Children, March 2014. (http://thomsonreuters.com/business-unit/legal/digital-economy/digital-economy-task-force-report.pdf)

[112] U.S. Federal Bureau of Investigation, "Bitcoin Virtual Currency: Unique Features Present Distinct Challenges for Deterring Illicit Activity," *Intelligence Assessment*, April 24, 2012, page 1; (http://www.wired.com/images_blogs/threatlevel/2012/05/Bitcoin-FBI.pdf); New York Department of Financial Services, Press Release, "NY DFS Releases Proposed Bitlicense Regulatory Framework for Virtual Currency Firms," July 17, 2014. (http://www.dfs.ny.gov/about/press2014/pr1407171.html)

[113] Barak Ravid, "International Banking Giant Refuses to Cut Off Israel, Despite Boycott Calls," *Ha'aretz* (Israel), October 6, 2014. (http://www.haaretz.com/business/.premium-1.619514)

[114] "SWIFT Sanctions Statement," *SWIFT Website*, October 6, 2014. (http://www.swift.com/about_swift/shownews?param_dcr=news.data/en/swift_com/2014/PR_swift_sanctions_statement.xml#)

[115] Linda Gradstein, "Growing Concern in Israel Over BDS," *Ynet News*, March 3, 2014. (http://www.jta.org/1992/08/07/archive/arab-boycott-said-to-cost-israel-45-billion-over-the-past-40-years)

[116] Cutler J. Cleveland, *The Concise Encyclopedia of the History of Energy*, (San Diego: Elsevier Inc, 2009).

[117] "Palestinian Civil Society Call for BDS," *BDS Movement Website*, July 9, 2005. (http://www.bdsmovement.net/call).

[118] Barak Ravid, "EU Consuls Recommend Imposing Sanctions on Israeli Settlements," *Ha'aretz* (Israel), February 2, 2013. (http://www.haaretz.com/news/diplomacy-defense/eu-consuls-recommend-imposing-sanctions-on-israeli-settlements.premium-1.506043)

[119] "A Campaign that is Gathering Weight," *The Economist*, February 8, 2014. (http://www.economist.com/news/middle-east-and-africa/21595948-israels-politicians-sound-rattled-campaign-isolate-their-country)

[120] Barak Ravid, "Haaretz Obtains Full Document of EU-Proposed Sanctions Against Israel," *Ha'aretz* (Israel), November 17, 2014. (http://www.haaretz.com/news/diplomacy-defense/.premium-1.626946)

[121] U.S. Energy Information Administration, "South China Sea," *Analysis Briefs*, February 7, 2013. (http://www.eia.gov/countries/regions-topics.cfm?fips=scs)

[122] Eric Campbell, "Reef Madness," *ABC News* (Australia), May 20, 2014. (http://www.abc.net.au/foreign/content/2014/s4008035.htm)

[123] Leo Lewis, "Dredger Shores Up China's Claims to Disputed Islands," *The Australian,* September 12, 2014. (http://www.theaustralian.com.au/news/world/dredger-shores-up-chinas-claims-to-disputed-islands/story-fnb64oi6-1227056331695?nk=3c6fd1bcbff213fbbc039a166d09c68c)

[124] "Not the Usual Drill," *The Economist*, May 7, 2014. (http://www.economist.com/blogs/banyan/2014/05/china-v-vietnam)

[125] Dingding Chen, "No, China Did Not Blink by Removing Its Oil Rig," *The Diplomat*, July 30, 2014. (http://thediplomat.com/2014/07/no-china-did-not-blink-by-removing-its-oil-rig/)

[126] Eva Dou and Richard Paddock, "Behind Vietnam's Anti-China Riots, a Tinderbox of Wider Grievances," *The Wall Street Journal*, June 17, 2014. (http://online.wsj.com/articles/behind-vietnams-anti-china-riots-a-tinderbox-of-wider-grievances-1403058492)

[127] "Joint Statement by President Barack Obama of the United States of America and President Truong Tan Sang of the Socialist Republic of Vietnam," *Embassy of the United States, Hanoi, Vietnam Website*, July 25, 2013. (http://vietnam.usembassy.gov/joint_statement_072513.html)

[128] Joel Guinto, "China Builds Artificial Islands in South China Sea," *Bloomberg*, June 19, 2014. (http://www.businessweek.com/articles/2014-06-19/china-builds-artificial-islands-in-south-china-sea)

[129] Eric Campbell, "Reef Madness," *ABC News* (Australia), May 20, 2014. (http://www.abc.net.au/foreign/content/2014/s4008035.htm)

[130] "The Pressure on the Sierra Madre," *The Economist*, March 22, 2014. (http://www.economist.com/news/asia/21599402-beached-ship-risks-becoming-south-china-seas-latest-flashpoint-pressure-sierra)

[131] "Not the Usual Drill," *The Economist*, May 7, 2014. (http://www.economist.com/blogs/banyan/2014/05/china-v-vietnam)

[132] Liane Hansen, "Sanctions Turn Tables in U.S.–China Relations," *National Public Radio*, February 7, 2010. (www.npr.org/templates/story/story.php?storyId=123463748)

[133] Henry M. Paulson Jr., *On the Brink: Inside the Race to Stop the Collapse of the Global Financial System* (New York: Business Plus, 2010).

[134] "Asia/Pacific Group on Money Laundering (APG)," *Financial Action Task Force Website*, accessed January 21, 2015. (http://www.fatf-gafi.org/pages/asiapacificgrouponmoneylaunderingapg.html)

[135] Timothy O'Brien, "Move Seen to Press Banks to Deal With Embassies," *The New York Times*, June 9, 2004; (http://www.nytimes.com/2004/06/09/business/move-seen-to-press-banks-to-deal-with-embassies.html); Matthias Rieker, Joseph Palazzolo, and Victoria McGrane, "Banks Exit From Embassy Business," *The Wall Street Journal*, November 20, 2010. (http://online.wsj.com/articles/SB10001424052748703531504575625060985983720)

[136] "Banks Can Keep Embassy Accounts: U.S. Regulators," *Reuters*, March 25, 2011. (http://www.reuters.com/article/2011/03/25/us-financial-embassies-idUSTRE72O3ID20110325)

[137] "Countries and Regions: China," *European Commission Website*, accessed September 14, 2014. (http://ec.europa.eu/trade/policy/countries-and-regions/countries/china/)

[138] Michael Martina and Andreas Rinke, "China Says Willing to Buy EU Bonds Amid Worsening Crisis," *Reuters*, August 20, 2012; (http://www.reuters.com/article/2012/08/30/us-china-europe-

idUSBRE87T0BY20120830); Leigh Phillips, "Wen: China Will Continue to Buy European Debt," *EU Observer*, June 27, 2011. (http://euobserver.com/china/32554)

[139] "China Calls for Swift Movement on BRICS Development Bank," *Agence France-Presse*, November 14, 2014. (http://www.businessinsider.com/afp-china-calls-for-swift-movement-on-brics-development-bank-2014-11)

[140] John Mauldin, "China's Renminbi Is Well on Its Way to Becoming a Global Reserve Currency," *Business Insider*, September 29, 2013. (http://www.businessinsider.com/renminbi-soon-to-be-a-reserve-currency-2013-9)

[141] "Currency Composition of Official Foreign Exchange Reserves (COFER)," *International Monetary Fund Website*, September 30, 2014. (http://www.imf.org/external/np/sta/cofer/eng/)

[142] Zijing Wu, "UnionPay: Visa and MasterCard's Tough Chinese Rival," *Bloomberg*, December 20, 2012. (http://www.businessweek.com/articles/2012-12-20/unionpay-visa-and-mastercards-tough-chinese-rival)

[143] "Russia Launches China UnionPay Credit Card," *RT*, August 15, 2014. (http://rt.com/business/180696-china-russia-union-pay/)

[144] "About-U.S. Army Space and Missile Defense Command/Army Forces Strategic Command," *U.S. Army Space and Missile Defense Command Website*, accessed September 21, 2014. (http://www.smdc.army.mil/2008/about.asp)

[145] Siobhan Gorman and Yochi Dreazen, "Military Command Is Created for Cyber Security," *The Wall Street Journal*, June 24, 2009. (http://online.wsj.com/articles/SB124579956278644449)

[146] Department of Defense, "Department of Defense Strategy for Operating in Cyberspace," July 2011. (http://www.defense.gov/news/d20110714cyber.pdf)

[147] Ellen Nakashima, "Pentagon to Boost Cybersecurity Force," *The Washington Post*, January 27, 2013. (http://www.washingtonpost.com/world/national-security/pentagon-to-boost-cybersecurity-force/2013/01/27/d87d9dc2-5fec-11e2-b05a-605528f6b712_story.html)

[148] Juan Zarate, *Treasury's War: The Unleashing of a New Era of Financial Warfare*, (New York: PublicAffairs, 2013), pages 204-206.

[149] Senate Appropriations Subcommittee on Financial Services and General Government, "FY15 Department of the Treasury's Office of Terrorism and Financial Intelligence Budget," April 2, 2014. (http://www.cq.com/doc/congressionaltranscripts-4453825?5&search=Rz3w3nor)

[150] David Sanger, "Global Crises Put Obama's Strategy of Caution to the Test," *The New York Times*, March 17, 2014. (http://www.nytimes.com/2014/03/17/world/obamas-policy-is-put-to-the-test-as-crises-challenge-caution.html?_r=2&gwh=2AB4E35C86F3ECC785A68EB09C8DC6F8&gwt=pay)

[151] Julie Hirschfeld Davis, "Enforcer at Treasury Is First Line of Attack Against ISIS," *The New York Times*, October 22, 2014. (http://www.nytimes.com/2014/10/22/business/international/enforcer-at-treasury-is-first-line-of-attack-against-isis.html?_r=0)

[152] Ellen Nakashima, "Pentagon to Boost Cybersecurity Force," *The Washington Post*, January 27, 2013. (http://www.washingtonpost.com/world/national-security/pentagon-to-boost-cybersecurity-force/2013/01/27/d87d9dc2-5fec-11e2-b05a-605528f6b712_story.html)

[153] Department of Defense, "Department of Defense Strategy for Operating in Cyberspace," July 2011, page 1. (http://www.defense.gov/news/d20110714cyber.pdf)

[154] Department of Defense, "Department of Defense Strategy for Operating in Cyberspace," July 2011, page 5. (http://www.defense.gov/news/d20110714cyber.pdf)

[155] Ellen Nakashima, "Obama Signs Secret Directive to Help Thwart Cyberattacks," *The Washington Post*, November 14, 2012. (http://www.washingtonpost.com/world/national-security/obama-signs-secret-

cybersecurity-directive-allowing-more-aggressive-military-role/2012/11/14/7bf51512-2cde-11e2-9ac2-1c61452669c3_story.html)

[156] Eric Bradner, "Obama: North Korea's Hack Not War, but 'Cybervandalism,'" *CNN*, December 21, 2014. (http://www.cnn.com/2014/12/21/politics/obama-north-koreas-hack-not-war-but-cyber-vandalism/)

[157] Department of Defense, Directive, "DoD Counter Threat Finance (CTF) Policy," November 16, 2012, page 2. (http://www.dtic.mil/whs/directives/corres/pdf/520514p.pdf)

[158] Lynnley Browning, "Regulator Benjamin Lawsky Is the Man Banks Fear Most," *Newsweek*, June 30, 2014. (http://www.newsweek.com/regulator-benjamin-lawsky-man-banks-fear-most-256626)

[159] Ellen Nakashima "Alexander: Promote Cyber Command to Full Unified Command Status," *The Washington Post*, March 12, 2014. (http://www.washingtonpost.com/blogs/the-switch/wp/2014/03/12/alexander-promote-cyber-command-to-full-unified-command-status/)

[160] Jared Serbu, "Cyber Command Headed Toward Unified Command Status," *Federal News Radio*, March 14, 2014. (http://www.federalnewsradio.com/398/3581197/Cyber-Command-headed-toward-unified-command-status)

[161] Jason Healey, "The Future of U.S. Cyber Command," *The National Interest*, July 3, 2013. (http://nationalinterest.org/commentary/the-future-us-cyber-command-8688)

[162] During World War II, the United States and Britain had offices of economic warfare. Exploring lessons from this period as they apply in the modern context would likely provide fertile ground for additional analysis.

[163] Reuel Marc Gerecht and Mark Dubowitz, "Iran Wants the Bomb—And Sanctions Relief," *The Washington Post*, October 12, 2013; (http://www.washingtonpost.com/opinions/iran-wants-the-bomb--and-sanctions-relief/2013/10/11/201f0734-31e7-11e3-9c68-1cf643210300_story.html); Mark Dubowitz and Reuel Marc Gerecht, "Iran Ignores a Lucrative Deal Over Its Nuclear Activities," *The Washington Post*, August 10, 2014. (http://www.washingtonpost.com/opinions/iran-ignores-a-lucrative-deal-over-its-nuclear-activities/2014/08/08/32ef5c96-1ef0-11e4-ab7b-696c295ddfd1_story.html)

CHAPTER 2

Cyber-Enabled Economic Warfare and State Actors

By Abe Shulsky

What is "Economic Warfare"?

It is a commonplace notion that we live in an era of "globalization." This phenomenon has many aspects, but the most important one refers to the increasing economic integration of the different parts of the world in terms of cross-border trade and finance. In general, these economic relationships are not zero-sum; in the past 70 years, globalization has led to a vast increase in prosperity world-wide. The successful post-World War II economic integration of such countries as Germany and Japan, for example, into the global economic order, and their resulting prosperity, stands in marked contrast to their economic circumstances in the pre-war period. The economic development of China and India, as well as many smaller countries, has also been facilitated by the open world economic order that has prevailed since World War II.

Nevertheless, we have not reached an Adam Smithian utopia of global open markets free of government attempts to influence economic behavior in pursuit of various national objectives. As long as nations compete with each other politically and militarily, there will be scope for them to rely also on economic and financial means to further their goals. An effort to strengthen one's political-military situation by weakening an adversary's economic condition or otherwise causing him economic or financial difficulties has been called "economic warfare."

Economic warfare can be used to accomplish one or more of the following objectives:

- It can help reduce an adversary's (or potential adversary's) military and political power, thereby making it a less formidable opponent in an on-going or potential military or political conflict.
- It can, by causing the adversary's government domestic political difficulties, attempt to induce it to change its policies or behavior.
- It can attempt to cause sufficient popular dissatisfaction to bring about the overthrow of a regime.

Economic warfare methods can be used in "peacetime," i.e., in the absence of violent conflict or a state of war as ordinarily recognized under international law, or they can be part and parcel of a violent conflict or traditional war. Indeed, it may be that, in conjunction with the absence for almost seventy years of wars between the major powers, the very distinction

between war and peace has been blurred and economic warfare methods will be used by major powers in the context of relationships that combine both conflict and cooperation.

In this chapter, we will focus primarily on the use of economic warfare means in peacetime, while recognizing that some techniques (such as a blockade) would themselves constitute acts of war and hence would be incompatible with peace. The focus will be on the threat to the U.S. posed by the possible use of economic warfare means by state adversaries. The threat of economic warfare by non-state entities is discussed in chapter 3.

Although economic warfare has always been a possible factor in international relations (the Peloponnesian War finally ended when the Athenians lost control of the Dardanelles and could no longer import grain from the Black Sea area), the availability of cyber techniques has meant that certain kinds of economic warfare are easier and less costly to pursue and can have much greater impact than previously. Among the key differences are:

- Attacks can be conducted without having to operate on the victim's territory (e.g. cybersabotage can be conducted remotely, whereas traditional sabotage typically required an agent on the victim's territory).
- The victim may have a harder time attributing the attack, thus inhibiting any retaliation.
- The effects of an attack can be much greater. (For example, intellectual property can be stolen by the gigabyte by cyber means, as opposed to having to steal each physical document or piece of equipment. Cybersabotage can take down an entire network without having to attack each piece of equipment individually.)

In general, the more a victim relies on cyber capabilities to communicate, to conduct financial transactions, to control industrial processes and infrastructure, etc., the more vulnerable he is to cybersabotage. Given the economic benefits of digitization, we can expect this reliance to continue, especially with respect to advanced economies. Hence, cyber-enabled economic warfare is likely to loom larger and larger as a national security issue in the coming years.

In the remainder of this section, we will review briefly the various economic warfare techniques that have or could be used. Such techniques include:

Blockade or Embargo

A blockade or embargo curtails an adversary's trade, either to weaken his overall economic situation or to deny him key commodities (e.g., foodstuffs, rubber, oil, etc.), or manufactured products (e.g., high technology goods or components, especially those with military uses). The use of force to conduct such a blockade would itself constitute an act of war, which could lead to military retaliation. It would also require interfering physically with third nations' trade with the adversary; such a use of force would raise legal issues and carry a political cost. An embargo, on the other hand, may simply involve forbidding one's own nationals from doing business with the adversary, an action that does not raise international legal issues.

This technique was used in both World Wars. Using its naval supremacy, Britain blockaded Germany and German-held territory in both wars, while the Germans resorted to submarine warfare to interdict British sea-borne commerce. During the Napoleonic Wars, the French "continental system" prohibited any French-controlled or -allied country from trading with Britain, which responded with a series of "orders in council" under which the British Navy seized merchant ships trading with those countries.

Sanctions

Sanctions or boycotts of various sorts involve the refusal of one or more countries to conduct certain types of business with a target country. Obviously, the more countries that cooperate in imposing the sanctions, the more effective they are likely to be. The drafters of the UN Charter placed particular hopes in the ability of such measures to resolve major problems without resort to military force: Article 41 refers to the "complete or partial interruption of economic relations and of rail, sea, air, postal, telegraphic, radio, and other means of communication" as measures the Security Council may take "to maintain or restore international peace and security." These steps are intended to induce the target government to change its behavior, either by causing pain to the governing group itself, or by creating enough popular dissatisfaction to pressure the government to change, or to bring it down.

Sanctions are most likely to be imposed against smaller and/or weaker countries, especially those particularly dependent on international trade and access to the world financial system. In general, they have to be "quasi-universal" to have any hopes of succeeding, unless one nation or small group of nations is a major and hard-to-replace supplier of vital commodities or other items. Current examples include proliferation-related international sanctions against such "rogue" states as Iran and North Korea. In the past, sanctions against apartheid South Africa and Rhodesia were particularly effective, since these countries considered themselves, and wished to be, part of the West.

Unilateral sanctions are unlikely to be very effective unless a particular dependence can be exploited. The U.S. embargo against Japan in 1940-41 exploited that country's dependence on oil imported from the U.S. (The Dutch government, whose colony of what is now Indonesia was the main alternative source of oil for Japan, cooperated with the U.S.) It was effective in squeezing Japan's oil supply but may have been an important factor motivating the attack on Pearl Harbor. By contrast, the unilateral U.S. sanctions against Cuba, which have not been supported even by the closest allies of the United States, have been generally ineffective.

A particularly important type of sanction involves freezing financial assets (or the barring of financial transactions generally). The dollar's role as the world's major reserve currency—in which international payments are most often and most conveniently made—gives the U.S. particular leverage. Thus, the United States has been able to prevent non-U.S. banks from conducting any dollar transactions on behalf of an Iranian bank or business.

Given the importance of the U.S. (and the West generally) in world economic and financial activity, there is little opportunity for others to use sanctions against it effectively: in most cases, the unwillingness of a country to do business with the U.S. will not pose much of a threat. Therefore, use of sanctions against U.S. (or allied or friendly countries) will be infrequent and limited to specific dependencies that can be exploited:

- The most famous attempt to impose sanctions on the U.S. was the so-called "oil embargo" against the U.S., the UK and some other Western countries in 1973-74 in connection with U.S. support for Israel in the Yom Kippur War. However, the actual effect of the "embargo" was caused by the OPEC (mainly Saudi) cutbacks in oil production, which raised the world price of oil. In fact, the U.S. was not disadvantaged more than any other importer.[1]
- At various points, the Russians have tried to exploit the dependence of Western Europe on their natural gas, as could happen again in connection with the Ukrainian situation. (Given that most natural gas is transported via pipeline, there are greater opportunities for exploiting specific dependencies; the development of a robust global capability to handle ship-borne liquefied natural gas (LNG) would cause the natural gas market to resemble the oil market.)

- In 2010, the Chinese imposed strict limits on exports of rare earths to the U.S. and other countries, and, for a while, prohibited any exports to Japan. This step was designed primarily to pressure Japan with respect to the territorial dispute between the two countries concerning the Senkaku/Daiyu Islands in the East China Sea. The measure was effective since China is the preeminent source for rare earths globally.[2]

Manipulation of Prices for Critical Goods

The export limitations discussed above had the effect of manipulating the global market for various critical goods. As noted, the actual effect of the "embargo" imposed on the U.S. by Saudi Arabia and other oil producers in 1973 was not to deprive the U.S. of imported oil, but rather to raise the world price of oil, to the disadvantage of not only the U.S. but of other oil importers as well. Aside from limiting one's own exports, one could raise world prices by sabotaging the productive capacity of other countries. Cyber means could be particularly useful in this regard.[3]

Alternatively, one could seek to weaken a country economically by lowering the world price of one of its major exports. For example, the current decline in the price of oil (or, more precisely, Saudi Arabia's unwillingness to stabilize prices by cutting its own production) has been attributed to the Saudi interest in weakening Iran. (A similar scenario played out during the mid-1980s, during the Iran-Iraq war.) In general, however, lowering the world price of a product will be much more difficult than raising it, since lowering the price requires the ability to bring a large amount of the product (or some good substitute for it) to market at the low price, whereas raising the price can be accomplished by shutting down existing capacity, either by sabotage or political-military pressure.

Preclusive Purchasing

Various other economic warfare techniques have been used at various times. For example, preclusive purchasing – the buying up of critical commodities on the world market to prevent an adversary from obtaining them – was practiced by the Allies in World War II. The British sought to deny Nazi Germany access to Portuguese and Spanish wolframite by this means.[4] Similarly, toward the end of World War II, the British and Americans were able to buy up chromite ore from Turkey, thus precluding its shipment to Germany. This technique was also used by the United States against Japan in the period prior to the attack on Pearl Harbor, while the United States was officially neutral.[5]

Counterfeiting

Counterfeiting the adversary's currency goes at least as far back as the American Revolution, when the British counterfeited American bank notes.[6] More recently, the Germans planned to counterfeit British currency during World War II, and indeed produced very good fake notes in various denominations. However, they were never able to distribute them widely enough to reach the desired objective, i.e., to cause the general loss of confidence in the British currency.[7] During the war, the British debated the advisability of counterfeiting German currency; Sefton Delmer, a key British psychological warfare official, reports that the psychological warriors were prohibited by the Treasury from doing this, although they did produce counterfeit German ration cards, which the RAF dropped over Germany, in an attempt to disrupt the rationing system.[8]

In the case of currency counterfeiting, one should distinguish between its use as a technique of economic warfare and the (much more common) criminal motivation. Most counterfeiters wish to profit from their activity – the last thing they would want would be a general loss of confidence in the currency they are counterfeiting (which would render their product worthless.) Thus, North Korean counterfeiting of U.S. dollars should probably not be considered economic warfare; the North Koreans can have little hope of causing a loss of confidence in the dollar, but they do need the income their criminal activity produces. However, one could imagine other counterfeiting efforts where the goal would be to cause financial panic.

Disruption

Counterfeiting may be seen as a specific example of a more general tactic: attempting to cause a loss of confidence in the normal functioning of an adversary's economic system, so as to produce panic or a crisis. For example, toward the end of World War II, the U.S. disseminated propaganda leaflets over Japanese cities encouraging the Japanese to cash in their bonds and spend their money, arguing that goods would soon become scarce. The goal was to cause panic buying and to undermine the Japanese economy.[9] This type of activity, designed to destabilize economic and financial activity, may be particularly amenable to being conducted by cyber means.

Tariffs and Dumping

High (and especially discriminatory) tariffs may be designed not so much to produce revenues for the government or to protect domestic industry as to put pressure on a given country or group of countries. If the intent is to harm the economy of a given country or countries, it would be reasonable to include such actions under the "economic warfare" heading. Similarly, dumping – the selling of a product at an artificially low price – may be considered as economic warfare, although the precise definition of "artificial" in the circumstances may be tricky. Thus, many in the U.S. saw Japan as acting in a hostile manner in this way in the 1980s when Japanese manufacturers captured a substantial portion of the American automobile market. However, the Japanese advantage derived primarily from the inferior management of the U.S. automobile companies;[10] having been forced to clean up its act, the U.S. automobile industry is now able to compete. More recently, the Chinese made a major effort to dominate the world solar power industry by heavily subsidizing the expansion of production capacity of solar panels. The result was financial difficulty and even bankruptcy for solar companies throughout the world, including in China itself.[11] Was this an act of "economic warfare" against the U.S. and Europe?

Technology Theft

Another technique that raises the same issue is technology theft. This practice is at least as old as the industrial revolution. For example, in the early nineteenth century, Great Britain led the world in the production of textiles because of a series of major technological innovations. Chief among them was the power loom, which revolutionized cloth manufacturing. To protect this advantage, Great Britain had, since 1774, "enacted laws to forbid the export of its machines or even the plans." In 1811, a U.S. citizen, Francis Cabot Lowell, visited a number of textile factories and memorized the details of the power looms he saw. War had already broken out between the U.S. and Britain by the time he left for home in 1812, and his ship was intercepted by the Royal Navy and diverted to Halifax. "The British twice searched [the family's] baggage in Halifax, convinced that Francis had hidden drawings of the remarkable power looms and

spinning machines he had seen in Britain. But Francis had committed all to memory and no drawings or calculations were uncovered."[12] Lowell's daring act of technology theft is commemorated in the naming after him of the Massachusetts mill town.

In recent years, China has been engaged in the wholesale theft of intellectual property of all sorts from the U.S. and other Western countries, including most importantly technological information but also such items of intellectual property as software, movies, and books.[13] This type of theft is very much facilitated by cyber means. General Keith Alexander, former head of the National Security Agency, called the cyber-theft of intellectual property by China "the greatest transfer of wealth in history."[14]

While technology theft can have important consequences in the short run, it is hard to calculate its long-term effects. In any case, it is unlikely that any particular technology can remain the preserve of a given company or country for long. Aside from Coca-Cola's supposed "secret formula," this type of information generally spreads out in the world in one way or another. More importantly, technological innovation in the modern world is a rapid affair; thus, any technological "secret" is likely to be effectively obsolete in a decade or two. It is more important for a country that wishes to maintain its economic position to be constantly innovating than to be able to protect its technological secrets indefinitely. Nevertheless, the ability to maintain secrecy for a limited period of time remains important in order to enable the innovators to profit adequately from their innovation.

Techniques such as tariffs, dumping, and technology theft raise the interesting theoretical question of whether one can distinguish in a clear and convincing manner between economic warfare and the promotion of one's own economic development. Presumably, when the U.S. imposed high tariffs on manufactured goods in the early nineteenth century (and engaged, as noted above, in some technology theft on the side), it was interested primarily in its own economic development; while Britain was seen as a potential adversary, there isn't any evidence suggesting that weakening it economically was a goal of these policies. In any case, such a goal probably seemed far out of reach in the early part of the nineteenth century. Although eventually, as immigration to the U.S. and its westward expansion continued, surpassing Britain economically was probably inevitable. (For an alternative perspective on these issues, see Hsieh's treatment of them in chapter 3.)

Whether or not one should regard such steps as economic warfare may not be a question that can be answered definitively. However, one could look at distinctions such as the following in trying to understand the dimensions of the issue:

- State involvement in the economy: To what extent is the state involved in directing the development of the economy? To the extent that the state sees itself as responsible for developing the economy, what strategy has it adopted? What sorts of objectives does it set for itself and what tools does it have at its disposal?
    - For example, in the U.S. in the nineteenth century, the federal government was heavily involved in the internal development of the country (e.g., expansion of railroads, promotion of agriculture through homesteading, tariffs on manufactured goods). While more industrialized countries (such as Britain) no doubt regarded U.S. tariffs as burdensome, the absence of any intention of weakening those countries economically suggests that they were not economic warfare.
    - On the other hand, countries that adopt an export-oriented growth strategy, such as China, are necessarily involved in "capturing" markets that had previously been served by domestic producers (or by third

parties). This doesn't mean that such efforts should be regarded as economic warfare, but it increases the likelihood.

  - One important indicator could be the way in which the state bureaucracy is organized with respect to its promotion of economic development. What part of the economy is directly state-controlled? How much control does the state exercise with respect to non-state-owned enterprises? What is the nature of the (legal and practical) relationship between the state and these enterprises? How involved is the state in the collection of information for the benefit of economic entities? In short, has the state organized itself to be able to conduct economic warfare on behalf of its enterprises (including those not owned by the state)?

- State's grand strategy: To what extent does the country see itself as engaged in a zero-sum competition with its adversaries? Does the country see the relationship with the potential adversary as primarily economic (which would allow both countries to prosper) or as political-military (which is more inherently zero-sum in nature)? This goes beyond strictly economic questions to address the state's overall grand strategy: does it see the weakening of an adversary as a necessary component of its future success?
- State's attitude toward international norms: To what extent are "illegal" methods used? Methods might be illegal under customary international law or with respect to specific treaty obligations, e.g., obligations as a member of the World Trade Organization; or under domestic law, e.g., copyright or patent infringement, industrial espionage, computer hacking. (In some cases, a country might explicitly or implicitly permit an activity, such as copyright infringement, that most states regard as illegal.)[15]

Examination of these factors can be helpful in determining whether a given state is likely to engage in economic warfare against the U.S. They can provide a context in which to evaluate specific economic actions by the government in question to see whether it is likely that they are part of an overall economic warfare campaign.

Economic Warfare Threats to the U.S.

This section looks at potential economic warfare threats to the U.S. from state actors such as China, Russia, Iran, North Korea, and perhaps others; potential threats from non-state actors are discussed in the next chapter.

China still appears to be focused primarily on the development of its economic strength, which it is translating into military strength, thanks to double-digit percentage increases in its defense budget over a sustained period of years. To facilitate this, it has adopted a number of economic policies that have substantial impact on the U.S. and other advanced industrial countries.

Its pattern of heavy capital expenditures, often subsidized in one form or another, has produced overcapacity in a number of industries. Most recently, this effect has been evident in the case of solar power, with the result that Chinese dumping of solar panels has undercut producers in other countries, as discussed above. From the perspective of these countries, this can appear to be an attempt to kill off an entire industry.

In addition, as noted, China has engaged in the widespread theft of intellectual property, including by cyber means. China also forcefully pressures foreign firms to transfer technology to

it, for example, by making technology transfer a requirement for permission to invest in certain sectors of the economy.

Despite China's accession to the World Trade Organization, it has used various regulatory methods to hinder foreign companies' access to its markets. Similarly, restrictions on direct foreign investment have hampered the ability of foreign companies to penetrate the Chinese market and have protected their Chinese counterparts from competition.[16]

For many years, the yuan was systematically undervalued, thereby fostering Chinese exports and reducing imports. It would appear that this policy is continuing, although it is also possible that a thorough liberalization of financial markets would facilitate capital flight sufficient to cause the yuan to fall in value. (In any case, the huge size of Chinese reserves means that the government has a great deal of flexibility in setting the yuan exchange rate.) More recently, the Chinese government has been taking steps (e.g., making arrangements for trade with other countries to be denominated in Chinese yuan) that suggests it may be aiming at making the yuan a reserve currency alongside, or possibly eventually in replacement of, the U.S. dollar. However, making the yuan a reserve currency would require China to liberalize its financial regime considerably. This would be a long-term project, to say the least.

Until at least recently, China has followed a policy of export-led growth, which implies, among other things, that weakening the economies of the importers – of which the U.S. has been the most important one – would be counterproductive. In addition, China held vast amounts of U.S. Treasury bonds as part of its reserves; any weakening in the prices of those bonds would have been very costly. Thus, China had good reasons not to want to weaken the U.S. economy.

The 2008 financial crisis, which caused a sharp drop in Chinese exports, may have been something of a turning point in this regard. Going forward, we may see trends that will make China less dependent economically and financially on the U.S. For example, the Chinese are attempting to make their economy less dependent on exports, including to the U.S., and to increase domestic consumption as a percentage of GNP. Similarly, there is some evidence that China may be reducing its holdings of U.S. government debt. At the same time, China's more aggressive stance in the East and South China Seas with respect to various disputed islands and maritime areas increases the risk of U.S.-Chinese political, diplomatic, and even military conflict.[17]

Thus, we could see a China whose economic goals would include not only its own development but the weakening of the U.S. economic and financial position as well. Some of the same techniques – such as the theft of intellectual property, and the targeting of given U.S. industries by means of subsidies to domestic competitors – would serve the latter purpose as well. However, other methods might also be usable in this regard.

If the Chinese were to seriously seek to replace the dollar with the yuan as a global reserve currency,[18] they might have reason to take steps to decrease the general level of confidence in the dollar and in dollar-denominated markets. This could be done, for example, by causing instability and failures of trading platforms.

More generally, there are various means of cybersabotage that could have the effect of weakening the U.S. economy by attacking critical infrastructure. As these effects are likely to be relatively short-lived, they would presumably be done in conjunction with other acts of war, or as a prelude to them. Cyber means would likely be chosen to affect such sabotage because they offer plausible deniability and avoid the necessity of deploying personnel to the target country.

As noted, up until recently, at least, China has been focused on developing its economic strength and catching up with the advanced industrial world technologically and in terms of GDP. Since the economic crisis of 2008, Chinese policy with respect to the East and South

China Seas has become more aggressive; if this marks a strategic choice by China to begin to reap geopolitical benefits from its increased economic and military might, then it would have to see the U.S. as a potential obstacle. In this context, the actions discussed above, both those underway already (such as technology theft) and additional possible steps (such as cyberattacks on critical infrastructure, especially financial infrastructure) could be part of an overall strategy of weakening the U.S. economically so that it is less able to resist Chinese geopolitical initiatives.

The Ukraine crisis has focused attention on Russia's (or at least Vladimir Putin's) ambitions to reverse the outcome of the Cold War to the extent of re-creating a Russian "sphere of influence" in what it tellingly refers to as the "near abroad." Given overall economic and demographic trends, Russia may find it difficult to achieve its desired status as a global power, or even as a predominant regional one. Nevertheless, in addition to its nuclear arsenal, Russia has a major geopolitical asset, i.e., its large reserves of oil and natural gas and, in particular, its predominant position in the European market for the latter fuel.

Thus, Russia could have an incentive to resort to economic warfare techniques to maximize its revenues from oil and gas sales, and to maintain leverage over the rest of Europe via control of natural gas supplies. The goals would be to raise world oil prices (perhaps by disrupting oil production facilities elsewhere by sabotage or by stoking political instability) and to prevent other major sources of natural gas for Europe from coming on line (e.g., pipelines from the Eastern Mediterranean gas fields or elsewhere, such as Qatar and the Caucasus, or LNG from the United States).

For example, according to recent reporting, U.S. intelligence officials believe that Russia was responsible for the cybersabotage of the Baku-Tblisi-Ceyhan pipeline in 2008.[19] Construction of the pipeline was opposed by Russia since it would provide Azerbaijan with an export route for its oil that Russia could not control. The attack was very sophisticated; it involved taking control of the operational control systems to increase the pressure in the pipeline above safe levels, while at the same time blocking all the sensors that could have reported the dangerous situation back to the pipeline control room. The result was a spectacular explosion; its heat was felt a half mile away.

Depending on how U.S.-Russian relations evolve in the context of Russia's regional ambitions, Russia could have an incentive to weaken the U.S. economically by means of cybersabotage and other forms of criminality. At present, Russia appears to tolerate the use of its territory as a base for a large amount of cyber criminality against the West; it may see this as a potential useful capability depending on the evolution of inter-state relations.[20]

In the past, Russia has used a cyberattack as a means of pressuring smaller states on its border (such as against Estonia and Georgia in 2007 and 2008, respectively). Its preferred method is apparently the use of "patriot hackers" (hackers whose relationship with the state is kept deliberately vague) in the hope of retaining a certain degree of plausible deniability.[21]

The possibility of Russian involvement has been raised in connection with a major cyberattack on JPMorgan Chase,[22] perhaps in connection with the imposition of sanctions on Russia in connection with its activities in Ukraine. In October 2014, however, the FBI said that, "there was no evidence that the hack … was payback for western sanctions against Russia" and that "they still have not determined whether it was a foreign government … or criminals who were behind the network intrusions…"[23]

In either case, the goal appears to have been the theft of sensitive customer information; the operations of the bank were not interfered with. While the circumstances suggested a political motive, the activity could have a criminal motivation as well, although JPMorgan has not detected any fraudulent activity.[24] One possibility is that the attack involved collection of information that could be used to conduct a more devastating attack at a later date.

Finally, if the Russian government were ever to get serious about rebuilding its industrial base, pursuing new technologies, and diversifying away from natural resource extraction, it would have an incentive to engage in technology theft (as well as the other techniques practiced by China, as discussed above) to "jump start" its industries.[25]

As long as the U.S. is seen as "guarantor" of the global order, any "rogue state" that is concerned that the U.S. will try to enforce the rules against it will have an incentive to divert U.S. attention inwards towards its own domestic problems. One way to do this could be to create economic or financial problems in the United States; cybersabotage is an attractive way of doing it since it is generally a cheaper way of achieving a significant impact than more traditional methods (involving, e.g., the use of human saboteurs) and offers a certain amount of anonymity, or at least plausible deniability that can inhibit retribution.

Specific rogue states may also have other incentives for economic warfare against the U.S. For example, Iran shares Russia's interest in enhancing its oil revenues and could cooperate with it toward that end. More generally, Iran's views itself as leading a global "resistance" movement against the U.S. In 2012, Iran demonstrated rapid advances in its offensive cyber capability by attacking U.S. banks, the Qatari firm RasGas, and Saudi Aramco; the last-named attack erased data from 30,000 of the company's computers.[26]

From the Iranian perspective, the offensive cyber capability is probably viewed at present as an additional asymmetric capability (along with, for example, support for terrorism and naval "swarm" tactics in the Persian Gulf) with which to deter or retaliate against a U.S. or Israeli attack on its nuclear program. Attacking U.S. economic interests, either directly (as in the denial of service attacks against U.S. banks) or via attacks on Gulf oil producers that create major disruptions in the oil markets, could be an attractive use of this capability. In the future (especially if Iran succeeds in obtaining a nuclear capability that renders it, in its view, invulnerable to direct attack) Iran could use this cyber capability to pressure neighboring Sunni states into accepting Iranian positions on regional issues and eventually into acquiescing to Iranian regional hegemony.

The North Korean regime appears to have a major concern for regime survival. Given its lack of economic resources, one could expect it to continue its criminality in the form of currency counterfeiting and drug trafficking. Recently, the regime has shown some capability in the cyber arena[27] and it could try to harness that capability for money-making as well.

A recent report by Hewlett-Packard[28] provides a timeline of North Korean cyberattacks, mainly against South Korean financial and media organizations. These actions appear similar in intent to the North's occasional kinetic attacks against the South, i.e., to continue to exert pressure against the South Korean regime and to display the military and related capabilities that it claims to have. A key purpose of these pressure tactics appears to be to extort resources from South Korea to make up for the failings of its domestic economy, an approach that has had some success in the past.

In late 2014, North Korea conducted a massive cyberattack on Sony Pictures Entertainment in conjunction with its comedy *The Interview* (about a CIA plot to assassinate Kim Jung Un).[29] North Korea is extremely sensitive to anything that it sees as denigrating the stature of its leader, and, in June 2014, the North Korean news agency claimed that the movie "would not be tolerated."[30] Furthermore, although North Korea denied responsibility, it had applauded the attack, suggesting it might be the work of "supporters and sympathizers."[31]

North Korea's motive was likely "extra-economic," to protect the public image of its leader. The recent threats of physical violence against any theater screening the movie would support this interpretation.[32] However, the fact that the hackers had attempted privately to extort money from Sony before they went public suggests a possible economic motive as well.[33]

Potential New Methods of Cyber-Enabled Economic Warfare

This section explores and discusses the interest that the state actors mentioned above have, or might acquire, in developing new methods of cyber-enabled economic warfare against the U.S.

Benefiting Domestic Companies at the Expense of Foreign Companies

As we have discussed, cyberespionage is a useful, low-cost, and essentially risk-free method of stealing intellectual property; given that some state actors will continue to have an interest in benefiting domestic companies at the expense of U.S. and other foreign companies, we can expect that the basic methods of hacking into corporate computer systems will continue to be developed. As U.S. and other companies embrace the concept of cloud computing (which promises economic efficiency), the new opportunities to circumvent security measures and gain access to vast amounts of proprietary data that are thereby created will be exploited fully.

As China moves up the "value-added chain," i.e., shifts more of its economic activity from low-tech export industries exploiting low-cost labor (such as the manufacture of textiles and shoes, and the assembly of consumer electronics items) toward higher value added and higher information content items, its need for cutting-edge technological information will increase. If past experience is any guide, we should expect much of this need to be satisfied by technology theft. Other countries, as well, may use cyber means to steal technology.

Cyberespionage directed against foreign companies need not be limited to technology theft. It could also be profitably used to gain access to business-related information. For example, in cases where a domestic and a foreign company are competing for a contract, knowing the foreign company's strategy and proposal would be of great benefit to the domestic company. Similarly, understanding a competitor's strategic plans (e.g., in which business areas it intends to concentrate, which technologies it intends to pursue, etc.) would give a domestic company a clear advantage.

As the Internet becomes central to more and more business activity – especially retailing, but also service industries such as transportation (e.g., Uber) and business-to-business sales – countries may seek to benefit their domestic companies by interfering with the internet-based activities of foreign companies. This would be easiest to do in one's own country, especially in a country like China that exercises widespread control over the internet within its own "firewall," but it could be done via hacking outside one's own boundaries as well.

For example, in 2002, the Chinese government blocked access to Google.com by users in China. No reason was given, and the primary motivation may have been to enforce internet censorship more effectively. Nevertheless, the motivation may also have been – and the result certainly was – to benefit Google's Chinese competitors such as Baidu, which has since become a major player in Internet search, at the expense of Google.[34] In any case, as more and more economic activity shifts to the Internet, a government could use similar tactics to benefit its domestic companies at the expense of foreign ones.

Governments could use a wide range of methods, from the blatant and obvious – such as China's simply blocking all access from within the country to Google.com – to the more subtle and deniable. Instead of blocking all access to the website of a foreign retailer, steps could be taken to make access to the site intermittent and/or slow, in the hope that consumers would get frustrated and purchase from a domestic retailer instead. Web sites could be altered to indicate that certain products were not available, or that delivery times would be longer than they in fact

were, and so forth. Overall, the effect could be to suggest to consumers that a given retailer was not particularly reliable or efficient, thus leading them to prefer others.

More generally, any form of sabotage of a foreign competitor could also be undertaken to benefit domestic companies. Such sabotage could take various forms: attacks on a company's website so as to interfere with its ability to communicate with or sell to consumers; disruption of its intra-company communications; disruption of its computer-controlled manufacturing processes; interference with its communications with suppliers or with the logistics of its supply chain; and so forth. The goal would be to weaken the competitive capability of the foreign company thereby allowing a domestic competitor to gain at its expense.

This type of activity could be particularly effective in cases in which there are strong so-called "network effects," i.e., cases in which any format or standard that gains an initial advantage thereby achieves such a strong competitive position that it can crush its competitors. The classic case of such a "network effect" is that of the competition between the VHS and Beta videotape formats. Once one competitor (in this case, VHS) had an initial advantage in market share, it tended to become self-reinforcing: if consumers purchased more VHS players than Beta players, content providers had a greater incentive to make content available on VHS than on Beta; if more content was available on VHS, consumers had an incentive to purchase VHS players. Eventually, VHS won out and Beta disappeared.

In such circumstances, helping a domestic company gain an initial advantage for its format or standard via some sort of cybersabotage could have a big payoff. With any luck, once the cybersabotage was identified and attributed to a given government, and diplomatic or political pressure was applied to the government to cease the activity, the company for whose sake the sabotage was undertaken would be sufficiently far ahead that the "network effect" would ensure its eventual victory even after the sabotage on its behalf had stopped.

Disrupting the Adversary's Financial Infrastructure

Another possible area of economic warfare that could be developed in the future is the disruption of an adversary's financial or other infrastructure so as to weaken their economic situation or cause others to lose financial, political, or military confidence.

Financial markets could be a primary target of this type of operation, the purpose of which would be to weaken international confidence in an adversary's financial markets, thus diminishing his global economic presence and power. One method the U.S. has used to apply economic pressure on foreign countries is to deny them the ability to conduct international trade in dollars by sanctioning the banks through which the transactions would be carried out.[35] Thus, any country that was affected by such sanctions, or feared that it might be in the future, could have an incentive to reduce the role of the U.S. dollar in international trade and finance. Shaking international confidence in U.S. financial markets might appear to be a way to accomplish this goal. Similarly, if China or some other country were to wish to reduce the role of the U.S. dollar as a reserve currency in favor of its own currency, it might have an incentive to take similar action.[36]

There are, no doubt, many possible ways in which the stability of financial markets and infrastructure could be attacked. The ingenuity of man being what it is, it is likely that new methods of attack will be created all the time, and that, in many cases, their victims will not see them coming. Nevertheless, by examining ways in which the financial system has run into difficulties – due to accident or criminality, among other causes – we can get a sense of the ways in which an attack designed at destabilizing it might be conducted.

In the past decades, the stock and other financial markets have been transformed in various important ways: there has been a proliferation of marketplaces on which securities are traded, a proliferation of various derivative products (i.e., securities, such as options and index funds, whose value is keyed to the value of other securities) and the advent of high-frequency trading[37] (i.e., automated trading, directed by computer algorithms, which profits by reacting in milliseconds to minor price discrepancies across exchanges and securities), among other developments. As a result, financial markets are now much more complex organisms, whose reactions to atypical events can be difficult to predict and understand. They are also more vulnerable to various kinds of instability.

An event that highlighted this possibility was the "flash crash" of May 6, 2010. Within minutes, major equity indices plummeted 5-6%, before rebounding almost as quickly; in addition, shares in particular corporations also fluctuated wildly, with some issues trading more than 60% away from their values just minutes previously. The precipitating cause, according to the Commodities Futures Trading Commission/Security Exchange Commission investigation, was the clumsy execution by a mutual fund of a large sell order of a financial contract tied to the S&P index.[38]

Whatever the precipitating cause, however, the episode showed that certain underlying characteristics of the equities markets made them vulnerable to disruption and instability. These factors include various features of high-frequency trading, including the widespread reliance on computer algorithms to initiate trades without human intervention, and the vast amount of trading which creates the appearance of liquidity in the markets which, as the flash crash showed, isn't there when you need it.

Similarly, on April 23, 2013, the "Syrian Electronic Army" (a hacker group supporting Syrian President Bashir al-Assad) hacked into the Associated Press' twitter account and sent out a message saying that the White House had been attacked and President Obama injured. The reaction on the financial markets was immediate: the Dow Jones Industrial Average plunged 140 points before recovering within minutes. It appears that stock market traders' computer algorithms "read" the twitter feed of major news organizations such as the AP and initiate trades without any human intervention; in this case, the algorithms automatically entered "sell" orders. Thus, the markets reacted before any human traders had had the opportunity to consider whether the news was true, etc. The motivation for this hacking attack was presumably political revenge (or perhaps just a spirit of daring-do); there was no indication that the disruption of financial markets was the intended outcome.[39]

In both of these cases, the (unintentional) disruption was short-lived; however, they could suggest ways in which a malicious actor might cause more serious and longer lasting disruption. For example, if the erroneous twitter message had gone out during the "flash crash," it could have compounded the effect. Traders, having seen the market decline, would be more likely to accept the fake news report as authentic, since it would seem to explain what they were seeing on their screens. At the same time, it could have brought about a further wave of selling, thus depressing markets even more.

Fake news reports appearing to come from credible sources could also be used to target individual companies; banks and brokerage firms would be likely targets in this regard, since they depend on public confidence in their financial soundness in order to do business. If, for example, during a period of financial crisis (such as the latter days of 2008), fake reports had been circulated appearing to come from reputable news sources to the effect that a major bank was on the brink of failure, the report might seem sufficiently credible to cause a severe market reaction. In fact, one could even imagine – if the general situation were sufficiently tense – that market reactions (e.g., sale of the bank's stock, refusal of other banks to make overnight loans, etc.) would be enough to collapse the target institution.

Another approach might be to try to collapse the electronic payment system (credit and debit cards, on-line banking, automatic bank drafts, etc.) so as to bring commercial activity to a halt, or to at least impact it severely. This could be done either directly, by using cyber means to destroy records or interfere with transactions, or indirectly, by compromising the integrity of payment systems.

For example, it was publicly disclosed on April 7, 2014 that an "open source" (i.e., free) program widely used in connection with on-line retailing (as well as other activities) contained a security bug – named "heartbleed" – that could enable hackers to retrieve credit card information and passwords from companies using the software. This bug was introduced into the system in code written by a (volunteer) programmer, a German graduate student, after his proposed update was approved for incorporation into the program by a British consultant.[40] The disclosure of the security bug caused a great deal of consternation, as it suggested that criminals might have obtained access to a large number of passwords for bank accounts and e-commerce sites, among other things.

Despite some conspiracy theories, it appears that the incorporation in the widely-used software of the flawed additional code was an innocent mistake.[41] Nevertheless, the incident showed how a malicious actor might seek to introduce a vulnerability into critical software that could then be exploited to gather sensitive information. In this case, the hacker could have used the information he gathered to initiate a large number of unauthorized transactions involving credit cards, bank accounts, etc. If the scale were sufficiently large, it might not be possible to check the authenticity of each transaction (e.g., by attempting to contact the account holder in each case) and thus it might become necessary to close down entire segments of the payment system. This would have a major disruptive effect on commerce at the national level, and could serve to decrease confidence in U.S. economic strength.

Finally, an adversary could seek to cause a loss of confidence in the U.S. financial system by a widespread attack to destroy, encrypt or corrupt the stored financial records of banks, trust companies, stock exchanges, etc. Depending on the types of back-up systems that these institutions used, the objective of destroying or making unusable these essential records may be more or less attainable. In any case, the method of attack would have to be adjusted in the light of the back-up system in place. Thus, given a robust back-up system, it might be possible to recover relatively quickly from an attack that wiped out financial records in a bank's computer. A more sophisticated attack, however, that was able to corrupt records gradually on an on-going basis, so that the corrupted data themselves were copied into the back-up system, might be more successful.

Disrupting Other Critical Infrastructure

It might also be possible to disrupt other critical infrastructure by cyber means. In cases in which the internet is used to convey commands from system operators to the physical infrastructure components, there would be a possibility of malicious penetrations into the control system. Such remote electronic control is now common for many types of critical infrastructure, e.g., electrical grids, oil and gas pipelines, and railroads. In each case, there are great efficiencies that can be gained by enabling an operator in a control room to send commands to generators, transformers, pumping stations, compressors, signals, switches, etc. located throughout the country. Using the internet to convey these commands obviates the expense of creating a separate, dedicated communications system.

In 2009, President Obama noted that "cyber intruders have probed our electrical grid and … in other countries cyberattacks have plunged entire cities into darkness."[42] The country in question appears to have been Brazil, which suffered large-scale outages in 2005 and 2007.[43]

According to Richard Clarke, cybersecurity advisor to President George W. Bush, hackers were in fact responsible for bringing down power systems in Brazil. He further expressed the fear that the rapid adoption of "smart meters" (which report not only total electricity consumption, but also when the electricity is consumed) before adequate cybersecurity safeguards were devised suggests that something similar could happen in the U.S.[44] In 2014, the Department of Homeland Security announced that the control system network of a public utility had been compromised by hackers, but that there was no evidence the utility's operations were affected.[45] The fact that operations were not affected suggests the possibility that the hackers were implanting malware in the system to facilitate a future attack.

Such cybersabotage could be undertaken to weaken a country economically; however, the effects could be so widespread and damaging as to constitute, at least in the eyes of the victim, an act of war, against which it might feel compelled to retaliate. In any case, the damage, however severe, would likely be reparable in at most weeks, after which the victim's overall economic strength would recover. Thus, it is likely that action of this sort would be most likely undertaken as a prelude to all-out (kinetic) warfare. On the other hand, if the cybersabotage were able to do extensive physical damage to the infrastructure, then the victim might be weakened economically for a considerable period of time.

Another motive for cybersabotage against oil or gas infrastructure might be to disrupt markets in order to raise prices or damage confidence in a given energy supplier. Even temporarily damaging or shutting down of a major oil supplier's infrastructure would raise world prices, thus benefiting oil exporters and harming importers. Similarly, cybersabotage of a gas pipeline or liquid natural gas (LNG) facility could harm confidence in that victim's reliability as a gas supplier, to the benefit of alternative suppliers.

Actual preparations for such attacks have been detected. On June 30, 2014, the software company Symantec reported that:

> An ongoing cyberespionage campaign against a range of targets, mainly in the energy sector, gave attackers the ability to mount sabotage operations against their victims. The attackers … managed to compromise a number of strategically important organizations for spying purposes and, if they had used the sabotage capabilities open to them, could have caused damage or disruption to energy supplies in affected countries [including the United States, Spain, France, Italy, German, Turkey, and Poland.][46]

Symantec noted that the effort "bears the hallmarks of a state-sponsored operation, displaying a high degree of technical capability." Based on the time of day when actions were taken, "it is likely the attackers are based in Eastern Europe."[47]

Finally, one could imagine state actors resorting to criminal activity to raise funds. Much as the North Korean government currently engages in drug trafficking and counterfeiting as sources of revenue, a state in the future could engage in various forms of cyber criminality for the same purpose. Extortion, based on the threat of causing a disruption of the sorts discussed above, would be one possibility. There has been speculation that the attacks on the Brazilian electrical grid, as discussed above, were part of an extortion attempt. More generally, the research director of a cybersecurity institute has said that "Cyber extortion is a growing threat in the United States, and attackers have radically increased their take from online gambling sites, e-commerce sites, and banks, which pay the money to prevent sites from being shut down and to keep the public from knowing their sites have been penetrated."[48] Similarly, states could engage in other forms of cyber criminality, such as credit card fraud, in order to generate revenues.

It seems unlikely that any such criminal-type actions could be significant enough to cause overall instability in the target's financial system. Hence, one could argue that they should not be considered "economic warfare." Nevertheless, the cumulative effects of such activities could

help weaken the target's economic situation and confidence in his financial system. At the same time, the revenues would enable the attacking state to finance its destructive activities.

An adversary wishing to conduct economic warfare against the U.S. would presumably integrate many if not all of these tactics into its overall strategy. One could imagine at least two classes of overall strategies: a long-term one that aims at weakening U.S. economic power in favor of that of the attacker, and an "asymmetric" one that aims at inflicting a high degree of economic (and perhaps other) damage on the U.S. via a "cyber Pearl Harbor."

The first strategy would involve the systematic attack on a series of important U.S. industries through a mixture of cyber-enabled and other means, with the goal of promoting domestic companies at the expense of their U.S. competitors. The cyber-related tactics could include technology theft; cybersabotage of U.S. companies; and cybersabotage of critical infrastructure on which the U.S. companies depend. Companies that conduct business on the Internet could be vulnerable to denial-of-service and other forms of cyberattack that would impede their operations. These tactics would be used in parallel with non-cyber-related steps such as favorable tax, credit and other treatment of domestic competitors; manipulation of tariffs and non-tariffs barriers; and unfavorable regulatory treatment of U.S. operations in the attacker's country. The goal would be to seize global market share from U.S. companies in key industries, such as civilian aircraft production, where the U.S. now enjoys a leadership position. As leadership in major industrial areas is obtained, the overall economic position of the U.S. might be weakened to the point that it could no longer pursue global geo-political strategies of the sort that it has since the end of the World War II.

This strategy could also target the U.S. global financial position by using cyber means to disrupt U.S. financial and credit markets, thus reducing the attractiveness of U.S. markets to foreign businesses and investors and undermining, eventually, the dollar's global reserve currency status. This would contribute to the overall weakening of the U.S. global position.

The second overall strategy would focus more on using cyber as an asymmetric tactic, along the lines of terrorism. This strategy might be adopted by a weaker state that fears U.S. sanctions or other hostile U.S. action in response to the state's nuclear proliferation, support for terrorism or subversion against states friendly to the U.S., or other "rogue state"-type behavior. The goal would be to launch an attack so disruptive as to constrain the U.S. from taking action against the attacker and/or to deter any further U.S. action along those lines.

So far, states such as Iran or North Korea have engaged in some cyber activity of this sort, but the attacks have been of insufficient magnitude to achieve any significant effects. In the future, such attackers might develop more sophisticated campaigns that could produce vastly more disruption. Such a campaign might involve long-term preparations in which malware is inserted in the computer systems affecting critical infrastructure, government activities, and financial markets. The insertion of "Trojan horses" would allow the attacker to disrupt many critical systems at once, making it much harder to react to the attack. Similarly, the attacks could be synchronized in terms of their intended effects: for example, as noted above, an attack on financial systems designed to destabilize markets could be combined with the spread of false news reports that appear to come from reliable sources.[49] In addition, such cyberattacks could be coordinated with non-cyber terrorist attacks.

The synchronization of all these attacks would require sophistication on the part of the attacker that may not yet exist. Nonetheless, all the pieces are knowable and, in the case of many actual attacks, it often is not clear whether the attacker has left behind in the target system malware that he might be able to activate at a later date. Thus, the possibility of a "cyber Pearl Harbor" involving the synchronized use of a wide variety of cyber and other asymmetric tactics cannot be ruled out.

Future Research and Policy Issues

This section discusses where research and policy reforms may be needed to enable the U.S to deal with economic warfare threats from foreign states, and in particular with cyber-enabled economic warfare.

The highest priority is to enhance cybersecurity across the board. This goes beyond the specific issue of defending against cyber-enabled economic warfare, and deals with the whole range of cyber threats, including criminality, sabotage, vandalism, terrorism, and so forth. Responding to all of these adequately involves many highly technical issues that cannot be dealt with adequately here. Nevertheless, it is important to highlight a few of the approaches that can be taken, without which any attempt to deal with the economic warfare challenge would be woefully incomplete.

A first avenue of approach would be to seek ways to make the information technology user culture more security conscious overall. When the internet was developed, the goal was to make it as flexible and functional as possible: given that only presumably like-minded technology enthusiasts had it, it is not surprising that security considerations were minimal. Although conditions have since changed, the prioritizing of flexibility and functionality over security has remained: in addition, ease of use for the technologically unsophisticated has also become a desideratum.

Changing the culture will be difficult, especially since there are strong financial incentives on the part of software and hardware producers to push the technological frontier as quickly as possible.[50] This raises, among other things, important policy issues concerning the role of government in influencing the technological culture.

There are several policy approaches for enhancing security consciousness. The government can encourage and facilitate greater sharing of information among the companies that are potential cyber targets. Liability laws can be updated to ensure that the cost incurred because of careless security practices fall on those responsible for them.[51] Stricter liability standards would presumably lead to a greater demand for liability insurance on the part of vulnerable companies; the insurance companies would then become the promulgator and enforcer of security standards as part of the underwriting process.

Alternatively, the government can promulgate more precise regulations on required security practices and enforce them more energetically. At present, the Federal Trade Commission (FTC) appears to be ramping up enforcement actions against companies it regards as deficient in this area.[52]

In either case, there would be an important trade-off to be considered: the dynamism of the IT world could be endangered if security requirements were made too onerous or inflexible. Clearly, the "open" architecture and culture of the Internet has been a major factor in its growth, and one would not want to sacrifice that unduly in the name of security. Overly hampering innovation and growth in the IT sector could do as much damage to the U.S. economy as most forms of economic warfare.

Along with steps to improve cybersecurity, more research is required on the possible effects of cybersabotage, and of steps that can be taken to mitigate them. As a technologically advanced country, the U.S. is more vulnerable to various forms of cybersabotage than are countries that do not rely as much on electronic systems to handle basic economic and industrial functions. Cases in which a country's reliance on cyber capabilities and connections has been successfully attacked need to be studied and fully understand.[53]

Research on instances of both man-made and natural disruptions to critical infrastructure can shed light on ways to increase the survivability of essential functions. This would involve

such approaches as increasing redundancy and resiliency, stockpiling assets to allow for more rapid reconstitution, and others ways of making systems more robust. This is likely to raise costs and to derogate from the efficiency of systems, so attention must be paid to the legal or regulatory regimes that would either set standards to be met or allocate the costs for system failure.

Given the difficulty of preventing and defending against cyberattacks, it is not surprising that much attention has been paid to the possibility of deterring them. The discussion has been vitiated by the analogy to theorizing about nuclear deterrence; this kind of deterrence, however, depends on factors that are not present in the case of cyber. Briefly, if cyber deterrence is to be constructed on the nuclear analogy, it stumbles over the following five differences:

- Attribution of the attack: Nuclear deterrence in the Cold War assumed that it would be easy to attribute an attack to a specific country; in the case of cyber, attribution can be very difficult.
- Establishing credibility: The U.S. was never subject to nuclear attack; on the other hand, it is continuously subject to cyberattack and has not retaliated. Why should a future attacker believe that it will?
- Specifying the threshold for retaliation: It was assumed during the Cold War that an attack with one nuclear weapon would be sufficient to trigger retaliation. Since cyberattacks of various magnitudes go on continuously, it would be difficult to establish a clear threshold for retaliation.
- Demonstrating capability: Tests of nuclear weapons and missiles demonstrated capability. In the case of cyber, one would not want to alert potential adversaries to how one might launch an attack, for fear that the adversary would fix the vulnerability on which the attack depends.
- Providing reassurance: Deterrence requires that the potential attacker believe that, if he does not attack, he will be left alone. This was easy to believe in the nuclear context. But in the cyber context, all sorts of activities (e.g., espionage via cyber means) are going on all the time, making it harder to convey the necessary reassurance.

Nevertheless, deterrence does have a role to play but it has to be understood differently from the nuclear case. Nuclear deterrence was understood in a binary manner: it failed if one nuclear weapon was launched. Cyber deterrence, by contrast, has to be thought about on the analogy of gang life in a bad neighborhood: there is no possibility of absolute deterrence (bad stuff is happening all the time), and it is often difficult to attribute any particular bit of mischief to a given adversary. Nevertheless, if one gang's reputation for an ability and willingness to deal fiercely with adversaries is strong enough, other gangs will tend to leave it alone and think twice before engaging in particularly egregious conduct toward it.[54]

A second major area where research is required is the nature and future of economic warfare as it might be conducted by a nation that wishes to strengthen itself economically relative to us. In particular, from the perspective of the United States the question is, how does the leading country in terms of its economy, financial system and technological prowess maintain its lead?[55] Furthermore, again from the perspective of the United States, this question must be addressed in the context of its free market traditions, which preserve the initiative in most economic, financial and technological matters to private actors and limit the acceptable role of the government.

More understanding of the economic development strategies of major competitors is required to provide the context for assessing the likelihood and importance of any potential

economic warfare steps. For example, China's Five-Year Plan lists a number of "new strategic industries" for priority development; this might provide some indication of what areas might be most likely to see economic warfare activity such as technology theft.[56]

Given the importance of technological advance in modern economies, the key question is how best to foster technological innovation across all sectors of the economy. Much of the answer – having to do with patent law, government regulation, education, availability of venture capital, and so forth – will have little to do with economic warfare. In the course of such work, however, one particular question would have importance for our subject: what is the relative importance of protecting current technology from transfer to other countries versus out-innovating them? In general, one would have to expect that technological knowledge will spread throughout the world, just as the designs for the power loom spread from early nineteenth century Britain to America. So, the question becomes for how long one can hope to protect such secrets, and for how long is it important to do so? The more dynamic the field, the more quickly any technological secret will lose its value. A general understanding of these relationships could inform policy on preventing technology theft. Some sort of trade-off is likely involved here, in that steps that might be taken to prevent the diffusion of technology to other countries (e.g., restrictions on international communication on certain topics) could also hamper its development.

Similarly, a serious study of the factors that support a currency's status or as the global reserve currency is a necessary backdrop for understanding what steps an adversary could take, including cyber-enabled steps, to undermine the dollar.

As the country with the largest GDP and the most advanced technological base, the U.S. is in some ways the most vulnerable to certain kinds of economic warfare. Furthermore, as one of the least *dirigiste* of the major advanced economies, the U.S. is in some ways least able to benefit its own companies in international competition. In any case, the multinational nature of many if not most major U.S. corporations makes it unclear whether a policy of attempting to benefit them would make sense in terms of overall U.S. interests.

While many of the economic warfare tactics that might be used may have been identified, further investigation is required concerning how that might be used together as part of an overall strategy. Given that this area is quite speculative, approaches such as scenario-building and economic "war gaming" might be the best ways to investigate these interrelationships. Gaming also allows for an integrated investigation of possible U.S. retaliatory steps.

The unique situation of the United States may require that it look for asymmetric responses to various forms of economic warfare. For example, the U.S. has spent a lot of diplomatic effort aimed at convincing the Chinese to cease cyber-enabled technology theft. This approach is unlikely to bear fruit; the Chinese are aware that the U.S. is unlikely to engage in similar economic espionage and, in any case, the Chinese have more to gain from technology theft than they have to lose to it. As a result, the Chinese were unwilling to engage seriously on the issue (and in the aftermath of the indictment of Chinese military personnel, [57] they have called off the talks.)

Thus, if the U.S. wishes to make progress on the diplomatic front on this issue, it must demonstrate a willingness to engage in asymmetric responses of sufficient gravity to force the Chinese to the negotiating table. One possibility might to be to exploit the Chinese sensitivity to the free flow of information, both from the outside world to the citizens of China, and concerning key members of its leadership, such as the great wealth accumulated by high officials and members of their families. Thus, an information campaign that rendered part of the censorship apparatus ineffective might create sufficient pressure. Similarly, the collection and judicious leaking of information about the assets of the key officials could serve the same

purpose.[58] A thorough study of possible U.S. asymmetric responses to technology theft could assess the value of these approaches and suggest others.

---

[1] The domestic disruption – the gasoline "shortage" which caused long lines at gas stations – was due to U.S. price control policies; if the U.S. had allowed gasoline prices to rise to market-clearing levels, there wouldn't have been any "crisis" other than the hardships caused by the increase in price.

[2] In 2014, the World Trade Organization ruled that the Chinese limitations on exports were in violation of their obligations. Tom Miles and Krista Hughes, "China loses trade dispute over rare earth exports," Reuters, March 26, 2014. Available at http://www.reuters.com/article/2014/03/26/us-china-wto-rareearths-idUSBREA2P0ZK20140326 (accessed June 28, 2014). Not surprisingly, the Chinese action led to the development (or revival) of rare earth mining activities in the U.S. and elsewhere.

[3] See below for a discussion of apparent Russian sabotage of an oil pipeline linking Azerbaijan and Turkey in 2008.

[4] Gerhard Weinberg, *A World at Arms*, p. 396

[5] For example, the U.S. began to preclusively purchase Chilean copper in mid-1941. Jonathan G. Utley, *Going to War with Japan, 1937-1941* (New York: Fordham University Press, 2005), p. 122.

[6] Steven Mihm, "Outfoxing the Counterfeiters," *Wall Street Journal*, April 23, 2010. Available at http://online.wsj.com/news/articles/SB10001424052748703876404575200093609290372 (accessed June 30, 2014).

[7] "Nazi fake banknote 'part of plan to ruin British economy,'" *The Telegraph*, September 29, 2010. Available at http://www.telegraph.co.uk/history/world-war-two/8029844/Nazi-fake-banknote-part-of-plan-to-ruin-British-economy.html (accessed June 30, 2014).

[8] Sefton Delmer, *Black Boomerang* (New York: Viking Press, 1962), pp. 156-57.

[9] This operation is discussed on a blog devoted to the history of psychological operations. http://www.psywarrior.com/WWIIAlliedBanknotes.html (accessed July 1, 2014). This site states that the Office of War Information described the goal of the leaflet as follows: "To disrupt the civilian economy in Japan by encouraging demand for commodities in excess of supply. Skepticism regarding the worth of Japanese war bonds is known to exist in Japan."

[10] A whole literature developed to argue that the Japanese had an "unfair" advantage, due to the fanaticism of Japanese workers, currency manipulation, hidden government subsidies, or whatever. It turned out, however, that the Japanese had simply developed much better ways to manufacture cars. See Frank Fukuyama and Abram Shulsky, *Virtual Corporation*, RAND Corporation, MR-863-A, 1997.

[11] See, for example, Keith Bradsher, "China Benefits as U.S. Solar Industry Withers," *New York Times,* September 1, 2011, available at http://www.nytimes.com/2011/09/02/business/global/us-solar-company-bankruptcies-a-boon-for-china.html (accessed August 22, 2014). When the U.S. and the European Union imposed countervailing tariffs against Chinese solar cells on the ground of "dumping," China complained to the WTO. The panel established to investigate the Chinese complaint ruled on July 14, 2014 that the countervailing duties imposed by the U.S. were inconsistent with WTO rules in certain respects. Both China and the U.S. have filed appeals concerning parts of the panel's report. World Trade Organization, Dispute Settlement DS437, available at http://www.wto.org/english/tratop_e/dispu_e/cases_e/ds437_e.htm (accessed October 21, 2014).

[12] Chaim M. Rosenberg, *Life and times of Francis Cabot Lowell, 1775-1817* (Lanham MD: Lexington Books, 2011), pp. 178, 214.

[13] See the 2013 Report to Congress of the U.S.-China Economic and Security Review Commission, November 2013, pp. 243-65.

[14] Interview with George Stephanopoulos, "This Week," ABC, July 23, 2013, available at http://icontherecord.tumblr.com/post/57804700833/general-keith-alexander-director-national (accessed October 21, 2014).

[15] See Andrew C. Mertha, *Politics of Piracy:Intellectual Property in Contemporary China* (Ithaca NY: Cornell University Press, 2007)

[16] A summary of Chinese adherence to WTO provisions in various industries was published by Reuters on the tenth anniversary of China's accession. "Factbox: China's decade in the WTO," November 29, 2011, available at http://www.reuters.com/article/2011/11/29/us-china-wto-factbox-idUSTRE7AS0BY20111129 (accessed July 1, 2014).

[17] At present, China's disputes with Japan, the Philippines and Vietnam have eclipsed the Taiwan issue in terms of escalatory risk. However, the relative quiescence of the Taiwan issue may reflect the fact that the KMT is in power; a future victory by the DPP, historically more concerned with maintaining Taiwan's *de facto* independence, could change that.

[18] Despite the costs that this would entail, as discussed above.

[19] Jordan Robertson and Michael Riley, "Mysterious '08 Turkey Pipeline Blast Opened New Cyberwar Era," Bloomberg, December 10, 2014, available at http://www.bloomberg.com/news/2014-12-10/mysterious-08-turkey-pipeline-blast-opened-new-cyberwar.html (accessed December 15, 2014).

[20] The threat from non-state actors themselves is discussed in the next chapter.

[21] This hope is not in vain: despite the circumstances of the Estonian attack, which clearly pointed at Russia, an NDU report referred to the incident as follows: "[t]he cyberattack that was launched on Estonia in spring 2007, which *allegedly* originated in Russia (*which its government denied)…*" Richard L. Kugler, "Deterrence of Cyberattacks," in *Cyberpower and National Security*, Franklin D. Kramer *et al.*, *eds*. (Washington: National Defense University Press, 2009), p. 313, emphasis supplied.

[22] Michael Riley and Jordan Robertson, "FBI Examining Whether Russia Is Tied to JPMorgan Hacking, *Bloomberg*, August 27, 2014.

[23] Ellen Nakashima, "FBI: 'No indication' JPMorgan was hacked because of sanctions against Russia," *Washington Post*, October 20, 2014, available at http://www.washingtonpost.com/business/economy/fbi-no-indication-jpmorgan-was-hacked-because-of-sanctions-against-russia/2014/10/20/66031f16-58af-11e4-b812-38518ae74c67_story.html (accessed December 23, 2014).

[24] "JPMorgan says no cyberattack-related customer fraud seen," *Reuters*, September 12, 2014.

[25] In one case, at least, Russia has resorted to cyber means to benefit a domestic producer at the expense of a U.S. company. (Discussion with cybersecurity expert, April 25, 2014)

[26] The discussion of Iran draws on James Andrew Lewis, "Cybersecurity and Stability in the Gulf," Center for Strategic and International Studies, *Gulf Analysis Paper,* January 2014, and Shane Harris, "Forget China: Iran's Hackers Are America's Newest Cyber Threat," *Foreign Policy*, February 18, 2014. Available at http://complex.foreignpolicy.com/posts/2014/02/18/forget_china_iran_s_hackers_are_america_s_newest_cyber_threat (accessed September 15, 2014)

[27] See, for example, "North Korea 'behind cyberattack' on South websites," BBC News Asia, July 16, 2013, available at http://www.bbc.com/news/world-asia-23324172 (accessed September 15, 2014).

[28] HP Security Briefing 16, August 2014, "Profiling an enigma: The mystery of North Korea's cyber threat landscape" available at http://h30499.www3.hp.com/t5/HP-Security-Research-Blog/HP-Security-Briefing-episode-16-Profiling-an-enigma-North-Korea/ba-p/6588592 (accessed September 15, 2014).

[29] According to the press release, "…the FBI now has enough information to conclude that the North Korean government is responsible for the [cyberattack on Sony]." FBI Statement, *Update on Sony*

Investigation, December 19, 2014, available at http://www.fbi.gov/news/pressrel/press-releases/update-on-sony-investigation (accessed January 5, 2015). While some private cybersecurity experts have questioned the FBI's attribution, it does not appear that any of them had access to all the information on which the FBI relied.

[30] "In June, the North Korean state KCNA news agency said, 'making and releasing a movie on a plot to hurt our top-level leadership is the most blatant act of terrorism and war and will absolutely not be tolerated.' North Korea has tried pressuring Sony Pictures, the White House and the United Nations to halt release of this film' Bruce W. Bennet, "Did North Korea Hack Sony?" Newsweek, December 15, 2015, available at http://www.newsweek.com/did-north-korea-hack-sony-292050 (accessed January 7, 2015).

[31] Jeremy Bender, "North Korea: 'Supporters and Sympathizers' May Have Hacked Sony," *Business Insider*, December 8, 2014, available at http://www.businessinsider.com/north-korea-supporters-may-have-hacked-sony-2014-12 (accessed January 6, 2015).

[32] Michael Cieply and Brooks Barnes, "Quandary for Sony in Terror Threats Over 'The Interview,'" *New York Times,* December 16, 2014, available at http://www.nytimes.com/2014/12/17/business/media/sony-weighs-terrorism-threat-against-opening-of-the-interview.html?ref=world (accessed January 7, 2015).

[33] Brandan Blevins, "Sony data breach update: Executives received extortion emails," TechTarget, December 10, 2014, available at http://searchsecurity.techtarget.com/news/2240236439/Sony-data-breach-update-Executives-received-extortion-emails (accessed January 9, 2015).

[34] According to Clive Thomson, writing in the *New York Times Magazine* ("Google's China Problem (and China's Google Problem)," April 23, 2006), "various American Internet executives … believe that Baidu has at times benefited from covert government intervention."

[35] According to the U.S. Treasury fact sheet, "Iran: What You Need To Know About U.S. Economic Sanctions " dated January 23, 2102: "Effective November 10, 2008, the authorization for 'U-turn' transfers involving Iran was revoked. As of that date, U.S. depository institutions are no longer authorized to process such transfers, thereby precluding transfers designed to dollarize transactions through the U.S. financial system for the direct or indirect benefit of Iranian banks or other persons in Iran or the Government of Iran." Available at http://www.treasury.gov/resource-center/sanctions/programs/documents/iran.pdf (accessed May 16, 2014).

[36] As noted above, the emergence of the yuan as a, or perhaps the, reserve currency would have costs, as well as benefits, for China. Nevertheless, it is possible that at some point in the future China will decide that the latter outweigh the former.

[37] See, for example, Michael Lewis, *Flash Boys* (New York: W. W. Norton and Co., 2014) for a fascinating discussion of high-frequency trading.

[38] *Findings Regarding the Market Events of May 6, 2010*, Report of the Staffs of the CFTC and SEC to the Joint Advisory Committee on Emerging Regulatory Issues, September 30, 2010.

[39] Patti Domm, "False Rumor of Explosion at White House Causes Stocks to Briefly Plunge; AP Confirms Its Twitter Feed Was Hacked," CNBC, April 23, 2013. Available at http://www.cnbc.com/id/100646197 (accessed May 19, 2014). On the other hand, a hostile intelligence service that was able to create an effect like this would presumably not be above profiting from it.

[40] Tu Thanh Ha, "Meet the man who created the bug that almost broke the Internet," *The Globe and Mail (Toronto)*, April 11, 2014, available at http://www.theglobeandmail.com/news/national/meet-the-man-that-created-the-bug-that-almost-broke-the-internet/article17941003/ (accessed May20, 2014).

[41] The conspiracy theories may have arisen from a Bloomberg News report alleging that NSA had been aware of the flaw, and had in fact exploited it to gather intelligence. Michael Riley, "NSA Said to Exploit Heartbleed Bug for Intelligence for Years," Bloomberg, April 12, 2014, available at

http://www.bloomberg.com/news/print/2014-04-11/nsa-said-to-have-used-heartbleed-bug-exposing-consumers.html (accessed May 20, 2014). The allegation was denied immediately by the Office of the Director of National Intelligence. The ODNI statement is available at http://icontherecord.tumblr.com/post/82416436703/statement-on-bloomberg-news-story-that-nsa-knew (accessed May 20, 2014).

[42] "Remarks by the President on Securing Our Nation's Cyber Infrastructure," The White House, May 29, 2009. http://www.whitehouse.gov/the-press-office/remarks-president-securing-our-nations-cyber-infrastructure (accessed May 29, 2014).

[43] The Brazilian government, however, denied that the blackouts were caused by cyberattacks. Michael Mylrae, *Foreign Policy Journal (Tufts University)*, November 15, 2009, available at http://fletcher.tufts.edu/News-and-Media/2009/11/15/Brazils-Next-Battlefield-Cyberspace (accessed May 29, 2014).

[44] Kin Zetter, "Feds' Smart Grid Race Leaves Cybersecurity in the Dust," Threat Level, *Wired*, October 28, 2009. Available at http://www.wired.com/2009/10/smartgrid/ (accessed May 29, 2014).

[45] Jim Finkle, "U.S. utility's control system was hacked, says Homeland Security," *Reuters*, May 20, 2014 available at http://www.reuters.com/article/2014/05/21/us-usa-cybercrime-infrastructure-idUSBREA4J10D20140521 (accessed May 29, 2014).

[46] "Dragonfly: Western Energy Companies Under Sabotage Threat," Symantec Security Response, available at http://www.symantec.com/connect/blogs/dragonfly-western-energy-companies-under-sabotage-threat?inid=us_ghp_thumbnail2_dragonfly (accessed July 1, 2014).

[47] *Ibid.*

[48] Ellen Nakashima and Steve Mufson, "Hackers Have Attacked Foreign Utilities, CIA Analyst Says," *Washington Post*, January 19, 2008. http://www.washingtonpost.com/wp-dyn/content/article/2008/01/18/AR2008011803277_pf.html (accessed May 29, 2014).

[49] See the discussion of the "flash crash," above.

[50] On the other hand, the recent departure of the CEO of Target in the wake of its massive loss of sensitive customer information may be seen as a positive sign. Although other factors may have been involved, the financial press saw a connection. "Nearly five months after Target first revealed that millions of customers' credit and debit card information was compromised in a data breach, the company is adding one more victim to its list." Samantha Sharf, "Target Shares Drop After CEO Gregg Steinhafel's Resignation," *Forbes*, May 5, 2014. Available at http://www.forbes.com/sites/samanthasharf/2014/05/05/target-shares-drop-after-ceo-gregg-steinhafels-resignation/ (accessed June 2, 2014).

[51] The Target case may be an important milestone here as well, given that the company may ultimately be found liable for a large amount of money. On December 2014, a federal judge refused to dismiss a suit brought by a group of banks against Target to recover losses they suffered as a result of the penetration of Target's computers. The judge said that Target's "key role" in allowing hackers to infiltrate its systems justified letting the banks pursue millions of dollars in damages. Jonathan Stempel, "Target fails to end banks' lawsuit over data breach," *Reuters*, December 2, 2014. Available at http://www.reuters.com/article/2014/12/03/us-target-breach-lawsuit-idUSKCN0JH04120141203 (accessed December 19, 2014).

[52] Paul Rosenzweig, "Which Federal Agency Controls Cybersecurity? The Answer May Surprise You," *The New Republic*, April 16, 2014.

[53] The case of Estonia, a highly "wired" country that came under massive cyberattack in 2007, seems to provide one good example.

[54] *How* the U.S. might retaliate in the cyber realm is another question: while the U.S. is unlikely, and would lack the incentive, to engage in theft of intellectual property on behalf of U.S. corporations, its

adversaries may have other vulnerabilities that could be exploited. For example, the U.S. could disable the "firewalls" that adversaries erect to prevent their citizens from having unfiltered access to news and information, or could publicize information about misbehavior by government officials that those governments wish to keep secret.

[55] A serious discussion of this issue would have to focus not on year-to-year growth rates but on the underlying strengths and weaknesses of the U.S. and its competitors, in particular, China.

[56] Of course, one cannot take documents such as the Five-Year Plan at face value; more detailed study might indicate however to what extent they can be relied on as guides to future action.

[57] Recently, five Chinese army personnel were indicted for computer hacking and economic espionage. "U.S. Charges Five Chinese Military Hackers for Cyber Espionage Against U.S. Corporations and a Labor Organization for Commercial Advantage," *Justice News*, Department of Justice press statement, May 19, 2014. Available at http://www.justice.gov/opa/pr/2014/May/14-ag-528.html (accessed June 5, 2014).

[58] For example, the Chinese leadership reacted strongly to a New York Times story describing the wealth accumulated by the family of former leader Hu Juntao, by, among other things, denying visas to New York Times reporters. Thomas L. Friedman, "Dear President of China," *New York Times,* December 14, 2013. Available at http://www.nytimes.com/2013/12/15/opinion/sunday/friedman-dear-president-of-china.html (accessed June 5, 2014).

CHAPTER 3

Intellectual Property Piracy as Economic Privateering

By Michael Hsieh

Intellectual Property Defense as an Indispensable National Interest

Suppose They Gave an Economic War and Everyone Came?

As a thought experiment of national strategy, one may imagine a United States stripped of its economic edge in production and innovation over its geopolitical competitors. Visualizing such a world, it would be difficult to imagine that the balance of strategic power would not realign in some proportion to this shift in the balance of economic power, which is increasingly determined by the relative ability of nations to create and implement commercially valuable ideas. Well before today's information age, that part of capital best described as "intellectual property" drove not only the quantitative dimensions of an economy – expanding output through ideas that lowered cost or increased value – but also qualitative ones, by spawning fundamentally new products and services. The notion of intellectual "property" evolved over centuries as an enshrinement of the system of economic reward to the inventors of such ideas.[1] The United States economy is particularly sensitive to the climate in which such rewards are protected. In a 2012 report by the U.S. Patent and Trademark Office, 75 of 313 U.S. industries are categorized as IP-intensive, accounting for 27.1 million jobs and 18.8% of all employment in the U.S. in 2010.[2] Furthermore, IP-intensive industries contributed $5.06T in value added (34.8% of U.S. GDP) in 2010. IP piracy denies IP innovators fair remuneration for the usage of their property, unlawfully extracting value from a large part of the U.S. economy. Technologically-advanced nations that can defend the rights of their inventors safeguard their economic preeminence, while those that do not cede a strategic edge afforded by their most ingenious denizens. A major security challenge for the United States in the twenty-first century is the protection of its IP rights.

Conversely, the unlawful acquisition of IP through espionage and other criminality can be a potent strategy for weak states to change the geopolitical status quo in their favor. Even though they may not be able to do so through armed force, weak states may strike asymmetrically at hegemonic states through the economic dimensions of national power. Weak states generally cannot expropriate land or labor from stronger states, but in the age of (1) the information economy and (2) near-ubiquitous global interconnectivity of informational infrastructure, they have potent options for asymmetric economic strikes against the capital stock of the economy of a hegemonic power. One historically-proven method of strike is the unlawful, large-scale extraction of intellectual property (IP) to increase the productive capacity

of the home economy while freeriding on the research and development investments of the target economy.

Economic warfare through IP theft, both in history and in present times, is ideally suited for the mass participation of non-state actors because of the natural alignment of the private commercial interests of thieves and pirates with the strategic interests of states seeking to increase the productive power of their economies with stolen technological know-how. These non-state actors are *economic privateers* in almost every sense of the term, short of formal letters of marque.[3] We explore this privateering model here from three perspectives: historical, contemporary, and technological. We examine how the advent of modern information and cyber technologies has quantitatively and qualitatively changed the dynamic between IP privateers and their victims. While a mature arsenal of technologies that assist the privateer in the theft of IP at larger scale and with broader scope exists, there is also an emerging class of technologies that may empower the protection of IP in fundamentally new ways.

In Section II, we explore the historical experience of the United Kingdom during the early Industrial Revolution, with deep analogies with the present challenge that confronts the United States: a strategically strong technological-leader beset by aggressive economic espionage and large-scale IP theft from an emerging strategic competitor. An exploration of the causes and effects of the inefficacy of the British official response in stanching the loss of the most economically-important categories of IP sets the stage for an exploration in Section III of the present American response, which has deep structural parallels to the essential features of British policy. Against the background of this historical analogue, we explore how the revolution in information and cyber technologies has profoundly empowered IP thieves by giving them tools with latencies, scope, and cost undreamt of in past epochs of IP theft.

In Section IV, we reimagine the problem of defending an entire economy against IP theft—not as a problem of legal or diplomatic action—but as a problem of technology. We explore qualitatively new options for the defense of IP for two historically difficult problems of defense: (1) preventing reverse-engineering of (often legitimately-acquired) product specimens, and (2) effective pooling of information between victim firms about cyber-espionage threats and incidents that traditionally could not be done because such information is often convolved with sensitive corporate information. Such a re-imagination of the problem may be useful today because history already provides us with a full account of a decades-long struggle between an emerging regional power seeking to transform its security landscape through an economic self-strengthening campaign based on large-scale IP theft against an established global power seemingly powerless to stop the hemorrhaging of its most sensitive industrial IP with the force of legal and diplomatic institutions alone.

The Strategic Privateer Campaign against British Intellectual Property

The Coxe Report

Shortly after winning political independence in the Revolutionary War, the national leadership of the young American republic viewed with alarm the precarious strategic position of the United States. In 1791, Treasury Secretary Alexander Hamilton, with his Assistant Secretary of the Treasury Tench Coxe, authored the "Report on Manufactures" addressed to the House of Representatives, which began with a call for a second national campaign to achieve manufacturing independence from the Old World:

> The Secretary of the Treasury…has applied his attention, at as early a period as his other duties would permit, to the subject of Manufactures; and particularly to the means of promoting such as well tend to render the United States, independent on foreign nations, for military and essential supplies.[4]

The recently concluded war with the United Kingdom revealed the backwardness of the American industrial base to be a major national security vulnerability:

> Not only the wealth; but the independence and security of a Country, appear to be materially connected with the prosperity of manufactures. Every nation, with a view to those great objects, ought to endeavor to possess within itself all the essentials of national supply. These comprise the means of Subsistence, habitation, clothing and defence. [...] [I]n the various crises which await a state, it must severely feel the effects of any such [industrial] deficiency. The extreme embarrassments of the United States during the late War, from an incapacity of supplying themselves, are still matter of keen recollection: A future war might be expected again to exemplify the mischiefs and dangers of a situation, to which that incapacity is still in too great a degree applicable, unless changed by timely and vigorous exertion.[5]

The retardation of American industry was a direct objective and the result of British imperial policy to maintain the dependency of the periphery for manufactured goods on the industrialized metropole. British policy sought to stifle manufacturing in the American colonies by limiting the flow of critical intellectual property imprinted in minds and machines. Export bans included silk and woolen manufacturing tools in 1749 and cotton and linen in 1774, and emigration bans included skilled manufacturing labor in 1749 and mechanics in 1774.[6] Hamilton and Coxe explicitly declared this drive for industrial independence to be an urgent national mission, asserting that, "To effect this change as fast as shall be prudent, merits all the attention and all the Zeal of our Public Councils; 'tis the next great work to be accomplished."[7]

As the United Kingdom was then the world leader in industrial technology, it was naturally the prime target for IP extraction by technologically laggard states. Against a background of doctrinal support from such national personages as Hamilton and various civic societies of American industrialists, this campaign of IP extraction was largely undertaken by persons and entities with no official relation with the United States government.[8] The illegality of such activities, from the perspective of British law, was well understood by the American proponents of such large-scale intellectual property acquisition as a national self-strengthening strategy. Hamilton acknowledged that most nations " ... prohibit, under severe penalties the exportation of implements and machines which they have either invented or improved."[9]

The American IP Privateering Campaign

Against the background of an aggressive doctrine of "procur[ing] all such machines as are known in any part of Europe can only require a proper provision and due pains,"[10] the official institutions of the United States government kept a cautious distance from the non-state actors that directly engaged in the unlawful IP acquisition. However, in certain situations, the line between official strategic doctrine and commercially-motivated private piracy was blurred. In this space, a phenomenon of *economic privateering* emerged, in which national strategic interests were advanced by (i) the officially unrecognized but (ii) doctrinally encouraged IP exfiltration activities undertaken by non-state actors motivated by private gain.

This model of economic privateering is exemplified by the case of Joseph Hague, who smuggled a cotton carding machine out of the UK. It was a non-governmental consortium of American industrialists, the Pennsylvania Society for the Encouragement of Manufactures and the Useful Arts, who lauded "...the ingenious artisan, who counterfeited the Carding and Spinning Machine, though not the original inventor... is likely to receive a premium from the Manufacturing Society, besides a generous prize for his machines."[11]

However, the public-private alignment of interest became more evident when they continued to surmise:

> ...it is highly probable our patriotic legislature will not let his merit pass unrewarded by them. Such liberality must have the happy effect of bringing into Philadelphia other useful artizans, Machines, and Manufacturing Secrets which will abundantly repay the little advance of the present moment.[12]

The desire of American officialdom to privatize as much of this activity as possible was exemplified in a technique Coxe proposed to the Society:

> It might answer an useful purpose, if a committee of this society should have it in charge to visit every ship arriving with passengers from any foreign country, in order to enquire what persons they may have on board, capable of constructing useful machines, qualified to carry on manufactures, or coming among us with a view to that kind of employment.[13]

In certain cases, direct official action was undertaken, albeit quietly. Coxe[14] in 1787-1788 reportedly contracted with an English expatriate to return to Britain to acquire brass models of Arkwright machinery, and pass them along to Thomas Jefferson, then serving as American Minister in Paris.[15] Apart from occasional direct action or personal interventions, the American IP privateering campaign never required much direct official material support. A permissive environment, created by (i) encouragements provided by official doctrine, (ii) financial inducements from industry and (iii) a lax legal environment, was sufficient.

The British Defensive Strategy

The British response to this IP privateering campaign was driven by a combination of industry and government action. The first British minister to the U.S. George Hammond declared to Foreign Secretary Lord Grenville: "No small degree of vigilance will be required in Great Britain to prevent emigration of artists and the export of models of machines."[16]

The British designated six government departments to the execution of the IP defense strategy. The function and interrelationships of these departments foreshadow many of the official responses to similar national campaigns of IP privateering in the twenty-first century. The Board of Trade was a kind of bureaucratic center, establishing policy on customs and international commercial relations. The Customs Commissioners performed the physical inspections at the ports and coasts. The Privy Council and the Treasury issued permits for skilled emigration and export licenses for machinery. The Foreign Office integrated into their regular diplomatic ambit the collection of local consular reports of smuggled artisans and machines. The Home Office developed domestic intelligence by receiving information from informants about the activities of foreign recruiters or the plans of artisans seeking to emigrate illegally.[17]

In the period before the 1820s, the design, construction, and processes of manufacturing was largely retained in the memories and know-how of artisans and mechanics rather than in blueprints and written manuals.[18] From the 1780s-1824, there was a particular legislative focus on the problem of curtailing skilled emigration. Skilled artisans or manufacturers from Britain or Ireland were limited strictly to the Crown dominions, and textile workers were altogether forbidden to leave the British Isles. Recruitment of artisans and manufacturers was expressly forbidden.[19] Heavy fines were imposed for smuggling machinery or skilled persons. Recruiters were fined £500 for each worker, shipmasters £100 fine for each smuggled passenger.[20]

Controls were imposed on the flow of machinery as well. There were broad bans for exporting or preparing to export pre-industrial or industrial textile, metal-working, clock-making, leather-working, paper-making, or glass manufacturing equipment.[21] Textile manufacturing IP was viewed as particularly sensitive, and was protected with specific legislation. In 1781, an export ban was passed on any "Machine, Engine, Tool Press, Paper, Utensil or Implement" and any "Model or Plan...Part or Parts thereof" used in the

manufacturing of cotton, linen, woolen or silk textiles. In 1782, an export ban was passed on engraved copper plates for calico printing, punishable with £500 fine and forfeiture of equipment. Shipmasters faced fines of £200 for machine smuggling, and an extra heavy fine of £500 for textile machines.[22]

The Etiology of Failure

The British response was largely ineffective in stopping the skilled emigration flows and machine export controls. Here again, six major failure modes of the British strategy[23] foreshadow many of the fundamental difficulties of managing broad and complex swathes of human activity that bedevil responses to such campaigns of IP privateering in the twenty-first century.

Poor Detection and Interdiction Capabilities. The British Customs authorities openly acknowledged their inability to identify skilled workers when artisans obfuscated themselves through perjury, brought falsified identification documents, or left behind the badge of their professions (commonly, bags of tools). Furthermore, some illegal emigrants could merely join ships after they had cleared Customs on small boats.

Proliferation from Intermediate States. In a report on unlawful machinery exports made by the Board of Trade in 1799, Ireland was identified as a favored hub for the unrestricted export of British machinery to multiple foreign destinations. Even the Union with Ireland Act of 1800 proved to be more of an administrative reconfiguration of the problem, rather than a solution to it.

Open Nature of Relevant Scholarship. Various drawings and specifications of manufacturing equipment and their operating rules were publicly available through such publications as Rees' *Cyclopaedia* and Montgomery's *Carding and Spinning Master's Assistant*. The British policy was to devolve the responsibility of censorship of sensitive IP to the individual authors.

Unfiltered Communications. Personal mail was not censored to any substantive degree by British authorities, and detailed plans and industrial information could be passed through private correspondence.

Non-Secrecy of Patent Information. Secret patents were generally not issued in Britain. Out of 5000 patents issued before 1824, only two were secret. In contrast, secret patents were commonly issued in contemporary France.

Domestic Resistance. Resistance to British official policy arose both from the British public and British industry. The informants used by the Home Office were socially reviled. The Privy Council commonly received complaints from shipmasters subject to Customs inspections. In 1785-1786, the wool card manufacturers of Essex and London pled with the Board of Trade for permission to export to the United States to alleviate unemployment among the poor in their textile districts.

With the rise of Tory power in the early part of the nineteenth century came the more popular acceptance of the ideologies of free trade and freedom of movement.[24] However, the British capitulation may have been more of an acknowledgment of realities rather than an act of surrender. In 1824, restrictions on skilled emigration were rescinded and in 1825, prohibitions on machinery exports were supplanted by a substantially more permissive licensing system.[25] As early as 1794, British clothier Henry Wansey found all of the state-of-the-art British textile manufacturing technology operating in United States.[26] A lower bound on the efficacy of the skilled emigration bans might be found in the Returns of Enemy Aliens made during the War of 1812, which record some 1300 British workers in the American textile trades out of about 7500

Britons residing in the United States.[27] On a more aggregated level, New England textile manufacturing output increased 50-fold between 1805 and 1815.[28]

The British response to the American IP privateering campaign failed to stanch the diffusion of its sensitive industrial IP to strategic rivals such as the United States. In using the British experience to frame modern national responses to present-day IP privateering, it is useful to consider the question of whether any British response strategy would have been successful. Historical experience reveals that government policy and action are rarely able to obstruct the diffusion of ideas and intellectual property when sufficiently strong economic inducements exist. Such cases include the smuggling of *Hevea brasiliensis* rubber tree seeds from Brazil to Malaya by British agent Henry Wickham,[29] or two Eastern Syriac monks smuggling silkworms to Byzantium from China in the sixth century,[30] export bans and strict punishments notwithstanding. As the United States of the present day itself contends with a constant and global onslaught of IP privateering emanating from multiple geopolitical competitors, the question arises: is the U.S. fated to lose today's IP privateering war?

The United States on Defense Against Intellectual Property Privateering

Industrial Age Defenses against an Information Age Adversary

In this section, we explore the similarities and differences between the British effort to resist American IP privateering, and the present-day effort by the United States to defend against an IP privateering threat that has been greatly empowered by modern information and cyber technologies. The greatest similarities lie in the legal and diplomatic dimensions. In style and substance, the present-day American defensive response against IP privateering deeply parallels that of the British during the late eighteenth and early nineteenth centuries against American IP privateers. This should not be surprising, because both British and American defensive options were limited by the same kinds of fundamental constraints. Then, as now, credible threats of IP enforcement action are infeasible when the aggressor entities are foreign nationals, often operating beyond the national jurisdiction of the victims. Where the two scenarios differ fundamentally is in the new advantages provided to the attacker by informational and cyber technologies. Such technologies enable the attacker to engage (i) a scope of victims and (ii) extract value at scales and latencies limited only by the physics of the global information infrastructure. Moreover, the technical challenges in attack attribution provide another advantage to the attacker. First, it is technically difficult to attribute attacks to specific actors, state- or non-state – smoking guns are rarely found. Furthermore, the defender's ability to definitively distinguish state and non-state actors can be severely limited against a sufficiently careful adversary. This is where adversary states not only passively benefit from the inflow of stolen IP into their economy, but can hypothetically exploit the difficulty of attribution to fight an information age equivalent of an irregular warfare campaign where regular forces fight without their identifying insignia. We conclude with an assessment of how the present U.S. national response could be augmented with new defensive technologies that assume that (i) perpetrators remain out of reach for legal remediation and (ii) exact attribution remains a technically challenging problem. These are not intended to be comprehensive solutions that address every dimension of IP theft, piracy, and economic espionage – cyber or otherwise.

Quantification and Attribution

The discussion of the threat to the modern American economy from IP theft usually begins with an attempt to quantify the problem by estimating the economic loss at a national scale. The difficulty of this problem is at least indirectly reflected in the widely divergent estimates from a

variety of analyses for both the U.S. and world economies, performed by government entities, cybersecurity firms and think tanks.

Exhibit 1

Article Title	Source	Date	Target of Cybercrime	Annual Losses	Link
Stolen Intellectual Property Harms American Businesses Says Acting Deputy Secretary Blank	United States Department of Commerce	11/29/11	U.S. economy	**$200 billion - $250 billion**	http://www.commerce.gov/blog/2011/11/29/stolen-intellectual-property-harms-american-businesses-says-acting-deputy-secretary-
NSA Chief: Cybercrime constitutes the "greatest transfer of wealth in history"	National Security Agency	7/1/12	U.S. economy, IP theft	**$250 billion**	http://foreignpolicy.com/2012/07/09/nsa-chief-cybercrime-constitutes-the-greatest-transfer-of-wealth-in-history/
			U.S. economy, cybercrime	**$114 billion**	
The Economic Impact of Cybercrime and Cyber Espionage	McAfee and the Center for Strategic and International Studies (CSIS)	7/1/13	World economy (p 16)	**$100 billion - $500 billion**	https://csis.org/files/publication/60396rpt_cybercrime-cost_0713_ph4_0.pdf
			U.S. economy (p 16)	**$70 billion - $140 billion**	
Cyber Espionage and the Theft of U.S. Intellectual Property and Technology	House Committee on Energy and Commerce, Oversight and Investigations Subcommittee	7/9/13	U.S. economy (5th paragraph of Rep. Murphy's remarks)	**$300 billion**	http://www.gpo.gov/fdsys/pkg/CHRG-113hhrg86391/html/CHRG-113hhrg86391.htm
Economic Impact of Cyber Espionage and IP Theft Hits U.S. Businesses Hard	Committee on the Theft of American Intellectual Property	7/10/13	U.S. economy	**$300 billion**	http://www.cio.com/article/2384269/cybercrime/economic-impact-of-cyber-espionage-and-ip-theft-hits-u-s--businesses-hard.html
Economic Impact of Trade Secret Theft: A framework for companies to safeguard trade secrets and mitigate potential threats	Center for Responsible Enterprise And Trade (CREATe.org), Pricewaterhouse Coopers LLP (PwC)	2/1/14	U.S. economy (p 3)	**1% - 3% of U.S. GDP**	http://www.pwc.com/en_U.S./us/forensic-services/publications/assets/economic-impact.pdf
Net Losses: Estimating the Global Cost of Cybercrime	McAfee and the Center for Strategic and International Studies (CSIS)	6/1/14	Global economy (p 2)	**$375 billion - $575 billion**	http://www.mcafee.com/us/resources/reports/rp-economic-impact-cybercrime2.pdf
Report: Cybercrime and espionage costs $445 billion annually	CSIS	6/9/14	World economy	**$445 billion**	http://www.washingtonpost.com/world/national-security/report-cybercrime-and-espionage-costs-445-billion-annually/2014/06/08/8995291c-ecce-11e3-9f5c-9075d5508f0a_story.html
			U.S. economy	**$100 billion**	

Attribution is challenging in other ways. While the targets can be well-defined and enumerated, the perpetrators are not always so easily identifiable. In the well-publicized "APT-1" report by security firm Mandiant in 2013, a range of cyber and non-cyber documentary

evidence was presented, linking a range of hacking activities associated with a specific military unit of the People's Liberation Army. Such reports, with comprehensively-documented evidence suggesting a specific state actor, are remarkable in their scarcity. In other cases, such as described in the "Nitro Attacks" report by Symantec in 2005, only a rough geographic location could be determined for one of the attackers (Hebei, China), but the directness/indirectness of his role and his affiliation with any broader group (state or non-state) could not be determined. Some cases are yet more challenging, as described in the "Energetic Bear / Crouching Yeti" report in 2014, for which only rather minimal inferences can be made. Certain catalogued threat actors have been ruled out as suspected participants in the attack, and the absence of, for instance, Cyrillic word content and the inclusion of some French and Swedish word content provides partial insight into the provenance of the malware code.

Exhibit 2

Report Title	Source	Date	Target Company or Companies	Perpetrator	Link
The Nitro Attacks: Stealing Secrets from the Chemical Industry	Symantec	7/3/05	Multiple Fortune 100 companies involved in R&D of chemical compounds and advanced materials; companies developing advanced materials for military vehicles; companies involved in developing manufacturing infrastructure for chemical and advanced materials industry	Covert Grove - 20 something male located in Hebei, China	http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/the_nitro_attacks.pdf
Hackers Linked to China's Army Seen From EU to D.C.	Bloomberg	7/1/12	European Union Council, Halliburton Co., Wiley Rein LLP, ITC (India based cigarette maker), British American Tobacco, Diablo Canyon nuclear plant, Pacific Gas & Electric Co., Business Executives for National Security, International Republican Institute, Immigration and Refugee Board of Canada, Pietro's Restaurant	Byzantine Candor (aka Comment) affiliated with the Chinese military, one member apparently goes by "Ugly Gorilla"	http://www.bloomberg.com/news/articles/2012-07-26/china-hackers-hit-eu-point-man-and-d-c-with-byzantine-candor
APT 1: Exposing One of China's Cyber Espionage Units	Mandiant	2/18/13	International cooperation and development agencies, foreign governments in which English is one of the multiple official languages, and multinational conglomerates that primarily conduct business in English	People's Liberation Army Unit 61398; Wang Dong "Ugly Gorilla; DOTA; Mei Qiang "SuperHard"	http://intelreport.mandiant.com/Mandiant_APT1_Report.pdf
Energetic Bear — Crouching Yeti	Kaspersky Labs	7/1/14	2,800 victims worldwide from the following industries: industrial/machinery, manufacturing, pharmaceutical, construction, education, and information technology	Energetic Bear/Crouching Yeti	https://securelist.com/files/2014/07/EB-YetiJuly2014-Public.pdf
APT 28: A Window Into Russia's Cyber Espionage Operations?	FireEye	10/27/14	Political and military targets including: government of Georgia, Eastern European Governments and militaries, and the European security organizations	"While we don't have pictures of a building, personas to reveal, or a government agency to name, what we do have is evidence of long-standing, focused operations that indicate a government sponsor – specifically, a government based in Moscow."	https://www2.fireeye.com/rs/fireye/images/rpt-apt28.pdf

Operation SMN: Axiom Threat Actor Group Report	Novetta	10/28/14	Fortune 500 companies, journalists, environmental groups, pro-democracy groups, software companies, academic institutions, and government agencies	"Novetta has moderate to high confidence that the organization-tasking Axiom is a part of the Chinese Intelligence Apparatus. This belief has been partially confirmed by a recent FBI flash released to Infragard stating the actors are affiliated with the Chinese government."	http://www.novetta.com/wp-content/uploads/2014/11/Executive_Summary-Final_1.pdf
The DarkHotel APT: A Story of Unusual Hospitality	Kaspersky Labs	11/1/14	Hotel guests - corporate executives and high-tech entrepreneurs	DarkHotel	https://securelist.com/files/2014/11/darkhotel_kl_07.11.pdf
The Regin Platform: Nation-State Ownage of GSM Networks	Kaspersky Labs	11/24/14	Victims fall into the following categories: telecom operators, government institutions, multinational political bodies, financial institutions, research institutions, individuals involved in advanced mathematical/cryptographic research	Regin - possibly supported by a nation state	https://securelist.com/files/2014/11/Kaspersky_Lab_whitepaper_Regin_platform_eng.pdf
Operation Cleaver	Cylance	12/1/14	Victims fall into the following industries: military, oil and gas, airlines, energy producers, utilities, transportation, healthcare, telecommunications, technology, manufacturing, education, aerospace, defense industrial base, chemical companies, and governments	Iran	http://www.cylance.com/assets/Cleaver/Cylance_Operation_Cleaver_Report.pdf
The Waterbug attack group	Symantec	1/26/15	Government related entities worldwide. Likely targeted U.S. CENTCOM in 2008	Waterbug	http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/waterbug-attack-group.pdf

In the present age of privateering, the sociology of the privateer has changed fundamentally. First, there is stronger empirical evidence compiled by the cybersecurity community that there are state actors playing as non-state actors. Second, the privateer has a quieter and murkier relationship with the state. In the age of American IP privateering against the UK, privateers were sometimes openly feted and celebrated by the most senior industrial and political leaders in the United States; there are no such publicly-visible mechanisms of reward to non-state actors in present times. Beyond the increased scale of the economic pain that can be imposed by IP privateers in the modern age, the qualitative difficulty of detecting and identifying bad actors has been exacerbated by the ease with which state actors now can convincingly conduct operations in the guise of non-state actors, augmenting the manpower already supplied by private criminal elements.

The Present U.S. Defensive Strategy: Juridical Punishments, Commercial Controls and Diplomatic Suasion

The blurry lines between state actors and non-state privateers in this realm of espionage and criminality is to some degree reflected in the hybrid response of the U.S. government to date: a combination of legal penalties structured to deter and punish non-state privateers, and efforts at diplomatic suasion calculated to rectify the behavior of state entities. Echoing the forceful British legislative response some two centuries earlier, harsh juridical deterrents based on fines and imprisonment, typified by legislation such as the Economic Espionage Act of 1996 (EEA), have been championed with the public diplomacy of the most senior national leadership. After the signing of EEA 1996 into law, President Clinton declared in his signing statement: "[It] will help us crack down on acts like software piracy and copyright infringement that cost American businesses billions of dollars in lost revenues. And it will advance our national security."[31]

The juridical deterrents were bolstered in 2012 with the enactment of the Foreign Economic Espionage Penalty Enhancement Act, which raised the maximum penalty for the transfer of trade secrets to a foreign government, permitting penalties up to $5 million for individuals and treble damages for the value of the stolen trade secret for enterprises.[32]

Commercial controls have been posed as a possible defensive strategy as well. The 2013 IP Commission Report issued by the Commission on the Theft of American Intellectual Property recommends the "…[enforcement] of strict supply-chain accountability for acquisitions by U.S. government departments and agencies…and [working] to enhance corporate accountability for the IP integrity of the supply chain."[33]

And to prevent latter-day equivalents of the machinists and artisans of the industrial revolution from voyaging back to their homelands with minds full of intellectual property wealth, another recommendation in the Plan is to "…greatly expand the number of green cards available to foreign students who earn science, technology, engineering, and mathematics (STEM) graduate degrees in American universities."[34]

Beyond the range of deterrents and punishments calculated to constrain the behavior of non-state actors, the U.S. government has also tried to directly address the murky nexus between state espionage activities and non-state privateering through public diplomacy. Max Baucus, U.S. Ambassador to China, explicitly underscored in his confirmation hearing the role that foreign governments have in IP theft, which sometimes crosses from the privateering approach to direct assaults with state resources: "It's also critical for the United States and China to work together to develop a shared understanding of acceptable norms and behavior in cyberspace, including a cessation of government-sponsored cyber-enabled theft of intellectual property."[35]

Director of National Intelligence James Clapper, in prepared testimony to the Senate Select Committee on Intelligence in 2014, indicates the strategic complementarity of national economic development with such privateering activities:

> China's cyber operations reflect its leadership's priorities of economic growth, domestic political stability and military preparedness. Chinese leaders continue to pursue dual tracks of facilitating Internet access for economic development and commerce and policing online behaviors deemed threatening to social order and regime survival. Internationally, China also seeks to revise the multi-stakeholder model Internet governance while continuing its expansive worldwide program of network exploitation and intellectual property theft.[36]

Beyond such juridical, commercial, and diplomatic responses, the IP Commission Report even considers the option of "…Congress and the administration [authorizing] aggressive cyber actions against cyber IP thieves," a notion that has historical parallels with the patriotic re-

purchase and return and of British manufacturing equipment by British industrialists or retaliatory acts of arson against American factories based on pirated technologies.[37] Short of that, other, more purely defensive tactics are explored by the report, which includes the recommendation:

> Support efforts by American private entities both to identify and to recover or render inoperable intellectual property stolen through cyber means. Some information or data developed by companies must remain exposed to the Internet and thus may not be physically isolated from it. In these cases, protection must be undertaken for the files themselves and not just the network, which always has the ability to be compromised. Companies should consider marking their electronic files through techniques such as "meta-tagging," "beaconing," and "watermarking." Such tools allow for awareness of whether protected information has left an authorized network and can potentially identify the location of files in the event that they are stolen.[38]

In the age of Hamilton and Coxe, such defensive technologies that can reach across oceans or make their presence felt long after they have left the workshop would have been fantasy. In the present day, however, they may not be. In the next section, we explore some potentially transformative technologies that may make the vision of the IP Commission Report a reality, if only partially. Specifically, we consider (i) cryptographically-secure program obfuscation methods to render the IP in a software product specimen intrinsically more resistant to reverse-engineering attacks by pirates and (ii) using secure multiparty communication (SMPC) to enable more adaptive cyber and network defenses against attackers through deep informational pooling by victims. *The primary value of a technological solution to IP piracy is its non-reliance on the adversary's compliance*. Defensive strategies based on legal and diplomatic force are fundamentally limited in efficacy, owing to the difficulties of enforcement and remediation in the lax legal environments in which privateers commonly operate,[39] and the plausible deniability of resource-poor governments in their unserious attempts to enforce foreign IP rights.

Defensive Technologies to Defeat IP Piracy and Economic Espionage

Raising the Cost of Piracy. The technological defense strategies discussed in this section do not seek to modify behavior through the fear of punishment or censure; they seek to fundamentally change the economics of IP theft. Roughly stated, obfuscation technology makes stolen goods harder to exploit, while the SMPC makes victims more expensive to victimize. Obfuscation can hypothetically render the IP in commercial software source code fundamentally more difficult to reverse-engineer, raising the cost of theft to unprofitable levels. SMPC allows victims comprehensively to share information about past and present attacks without revealing commercially-sensitive internal information about themselves, reducing the re-usability of the attacker's toolbox. This raises the cost for attackers in another way, by requiring them to reconfigure their tactics and tools against a pool of victims that are now equipped to learn and adapt to their attacks in a rapidly co-evolutionary manner.

Protecting Software against Reverse Engineering with Program Obfuscation. In the economies of the information age, software is uniquely important as both a quantitative and qualitative multiplier of productivity. As much as they enhance existing processes of production and other value-generating activity, they create qualitatively new ones as well. Among the IP-intensive American industries, software stands out as the largest by export value. In 2007, U.S. exports in software were valued at $22.3 billion, with the next largest being motion pictures and video industries at $15.3 billion and financial investment activities at $12.3 billion.[40] Software may be regarded as a special category of IP that is historically comparable to the role of textile-centric IP coveted by early American industry. Criminal

expropriation of commercial and industrial software IP creates an American-subsidized productivity multiplier at negligible cost to the aggressor nation.

The general landscape of global software piracy is bleak. According to a BSA study, the global piracy rate for PC software is around 42% (unlicensed software units / total software units installed). At the user level, 57% of the world's software users admit they pirate software, with 31% doing it "all the time" or "occasionally," and 26% doing it "rarely." Moreover, business decision makers self-report as "occasionally" pirating software at a higher rate (20%) than regular users (17%). The business decision maker piracy rate worsens substantially in emerging economies, where it is 22%, in contrast to 11% in developed economies.[41] The emerging economies are a particularly active locus for this kind of economic privateering. As a baseline, 2011 U.S. annual sales of legal software are about $42 billion, while the commercial value of piracy is about $10 billion, with a piracy rate around 19%. In contrast, China annual sales of legal software are about $3 billion, with the illegal market around $9 billion, with a piracy rate of 77%. Even among BRICS peers, China stands out as an anomalously low-compensator of producers of software IP. The average value of remuneration to software IP producers per computer in the USA is $120.22, whereas it is $41.18 in Russia, $36.38 in Brazil, $33.79 in India and $8.89 in China.[42]

Defending IP in software appears as two problems. One is access control: preventing unauthorized use of the functionality of the software. Another is algorithm control: preventing an unauthorized extraction of the proprietary mechanism underlying software's functionality. Traditionally, some combination of two solutions has been used to address these problems. Encryption entails converting the bits that comprise the compiled executable form of the software into a ciphertext, which can be decrypted temporarily when the program is run. Encryption is regarded as an approach appropriate to the access control problem, whose security depends on the security of a secret key. This is seen as a fundamentally unwieldy approach, because theft or discovery of the secret key is commonly achievable with key loggers and other system-resident malware, as well as more advanced attacks (such as the decompilation of the software and the search for high-entropy strings of key length, etc.). Beyond key-based vulnerabilities, attacks against the computer memory can also extract the plaintext version of the software as well. To keep the pirate out of the software, the defender must keep him almost completely out of the system.

Obfuscation is seen as a fundamentally more elegant solution. With obfuscation, the defender assumes that the pirate can access the system, and can even obtain a fully-functioning copy of the software, which he can copy and decompile at will. The idea of obfuscation is to write software source code in such a way that it runs and compiles normally, but is incomprehensible to a pirate seeking to understand the mechanism of the information processing functionality of the software.[43] Because software is stateless, obfuscation generally is not regarded as an approach appropriate to access control, as unbounded numbers of copies can be generated and run. However, it is the natural solution to the algorithm control problem, which in a broader sense may be the more important problem as it relates to the most valuable dimension of software IP – the proprietary ideas and innovations embedded within it.

The reason obfuscation is not an effective practical defense today is that it is based on "security through obscurity"—an approach that plainly does not work. State-of-the-art obfuscation entails methods that inject passive junk code to confuse a software pirate, or generate contorted control flows in the program to slow his understanding. With a decompiler, a debugger, and some basic visualization tools, a pirate can typically defeat codes obfuscated by the best known obfuscation utilities in about a day. The approximately one-day *adversary work factor* for de-obfuscation in the present state of technology renders it an effectively trivial barrier to the theft of the deepest aspects of software IP.

Practical Considerations. Recent breakthroughs in cryptographic theory open the possibility of a fundamentally new way to obfuscate software. Such methods, based not on "security through obscurity" but rather cryptographically-sound security assurances founded in rigorous mathematics, can raise the adversary work factor to unprecedented levels. With today's junk-code based obfuscation techniques, an adversary with commodity hardware can de-obfuscate most any software in a day; with the new obfuscation methods based on cryptographic security models, an adversary could in principle be confronted with a mathematical puzzle that would require on the order of years or centuries to de-obfuscate, even with the most powerful supercomputers available.

These security benefits do not come without cost. Obfuscating software in this way adds a degree of runtime overhead to the program, so that legitimate users will likely see their programs running more slowly in comparison to the same program that does not have the obfuscation-based protections. Because of the nascent state of the theory, absolute numbers for the runtime slowdown factors for practical software are not presently known to precision by the theoretical cryptography community. What is known with some exactness is the scaling of the runtime slowdown versus the cost imposed on the adversary. Encouragingly, the theory indicates that for a polynomial increase in runtime slowdown for the legitimate user, the attacker suffers an exponential increase in the time required to de-obfuscate.[44] The technological challenge is to get the runtime slowdowns to practically acceptable levels, while raising the adversary work factors to time lengths that make the economics of the piracy unfavorable for the pirate – either because of the resource expenditures for such long extraction processes, or because the software IP essentially becomes obsolete by the time he is able to extract successfully.

Certainly, the algorithm control problem can be potentially solved by such obfuscation technology. But to return to the vision of the IP Commission Report – such technology can be used to address the access control problem as well. Today, it is common for commercial software producers to try to control access to their software by obfuscating security features into their products. Such methods are very much "security through obscurity" methods as well – in which expiration dates, passwords and secret keys are "hidden" in the software. However, if the software can be de-obfuscated and reverse-engineered, the expiration date may simply be extended (or eliminated), while passwords and secret keys can be found and freely used afterwards. With the development of cryptographically-sound obfuscation technology, however, such security protocols could be made to work. Further, more active counter-measures can be obfuscated into software as well, such as (1) digital watermarks, which provide an indelible mark of provenance on digital goods or (2) distress beacons that cannot be shut off or removed by the pirate.

There are fundamental limitations to obfuscation-based defenses. Problems of piracy and espionage can never be fully solved by technology as the elements of the human dimension remain beyond its reach. For instance, human espionage against the research lab that produced the ideas and innovation that go into software can directly expropriate them in that manner. There also remain major technical obstacles to be overcome in the technology as well. The present state of the new obfuscation theory is in its earliest, most primitive stages. There are no known prototypes of this kind of obfuscation technology. The major open questions in this area are centered on how to practically reduce these runtime overheads to reasonable levels such that a practical balance between usefulness and security against IP piracy can be achieved. If such technical problems can be overcome, however, that major category of IP-intensive economic output represented by software can be defended in a way that can fundamentally change the cost equation for would be software pirates and reverse-engineers.

Safe Sharing of Economic Espionage Threat Data with Secure Multiparty Computation. Even perfect product-level defenses as exemplified by cryptographic software obfuscation would fail to stop cyber and traditional espionage threats against the laboratories and research centers from which sensitive information can be directly stolen in its raw form. To address this problem, the victims can be empowered by turning, to some degree, the tactics and tools of the attackers against the attackers themselves. As discussed in the prior section, the catalogue of, for instance, cyber bad actors is finite, as is the corpus of the cyber tools and methods which they use. The tools and methods are developed at cost. By enabling better information-sharing about threat actor identities, tools, and methods between victims, we can increase the economic cost of attack by diminishing the re-usability of tools and methods, and at a broader level, facilitate the identification of attacker groups and networks.

At present, the most comprehensive structure for the sharing of cyber (and human and physical) threats information in U.S. industry is the Information Sharing and Analysis Center (ISAC) system. Formed in 1998 by a Presidential Decision Directive (NSC-63), the original ISACs were focused on critical-infrastructure industries:

> The National Coordinator, working with Sector Coordinators, Sector Liaison Officials and the National Economic Council, shall consult with owners and operators of the critical infrastructures to strongly encourage the creation of a private sector information sharing and analysis center. The actual design and functions of the center and its relation to the NIPC [National Infrastructure Protection Center] will be determined by the private sector, in consultation with and with assistance from the Federal Government. Such a center could serve as the mechanism for gathering, analyzing, appropriately sanitizing and disseminating private sector information to both industry and the NIPC. The center could also gather, analyze and disseminate information from the NIPC for further distribution to the private sector. While crucial to a successful government-industry partnership, this mechanism for sharing important information about vulnerabilities, threats, intrusions, and anomalies is not to interfere with direct information exchanges between companies and the government.[45]

Since then, the ISAC system has expanded to a broader range of other industries, many of which are IP-intensive industries. ISACs have been formed for aviation, the defense industry base, the electric sector, information technology, the maritime industry, communications, national health, nuclear, oil and gas, and research and education.[46] The National Council of ISACs, formed in 2003, indicates the objectives of information sharing:

> Get information and data to the widest audience of recipients, either people or systems that need to: (i) analyze the data, (ii) make decisions based on that data, (iii) take action as a result of that data. Get information and data disseminated in the most timely manner appropriate. At the same time, the information sharing processes must prevent providing information and data to individuals or organizations that would likely: (i) use the data to commit malicious acts as a result of direct knowledge of that data, (ii) accumulate the data to commit future malicious acts, (iii) re-distribute, post, or otherwise indiscriminately or publicly disseminate information without permission of the information owner/provider.[47]

However, the objectives of information sharing need to be balanced with the requirements of discretion and careful judgment in the control and dissemination of the data: "Providing information that has not been sufficiently analyzed and therefore results in: (i) inappropriate or unnecessary actions that waste resources, (ii) harm to individuals, corporations, or organizations because the information is inaccurate."[48]

The dual technical and institutional challenge in good information integration is the seemingly incompatible objective of (i) maximizing information sharing about threats while (ii) minimizing the exposure of commercially-sensitive information whose dissemination may be damaging in its own right, for reasons of commercial competitiveness, civil liability or reputational damage.

To strike a balance between the objective of information sharing and the requirements of discretion, the National Council of ISACs has proposed protocols that are similar to the system of controlling classified information within the U.S. government:

> To lower these barriers, the following tasks must be accomplished: Categorize information [by]: (i) Sensitivity level (controls distribution), (ii) Target audience (helps determine appropriate distribution), (iii) Confidence level (helps determine appropriate response and timing), (iv) Severity level (helps determine appropriate response and timing).[49]

In addition, the vetting of individuals and entities privileged to access this data is similar to the security clearance system for classified information within the U.S. government:

> Vet organizations, including information providers, recipients, partners, and their relationships with other entities with whom they might share. Vet individuals thru personal contact and/or background checks. Establish guidelines/procedures/expectations for dealing with information… [and] establish consequences for not abiding by guidelines.[50]

Whatever advantages may exist in emulating U.S. government practices in controlling access to sensitive information, the costs and organizational difficulties in developing a security clearance system are likely not to be trivial. The challenges in maintaining an efficient pipeline of clearance provision was discussed in a 2011 report by the Intelligence and National Security Alliance (INSA):

> Over the past six years, timelines and backlogs in national security clearances have decreased substantially, particularly for government employees. Improvements for private contractors providing specialized services have not been as significant.[51]

Beyond the difficulty of operating efficient systems for managing clearances and accesses, the costs of denying clearances to trustworthy individuals or granting clearances to rogue individuals are also very much real, although difficult to quantify. Finally, the model ultimately relies on (i) making accurate judgments about individuals during the clearance assignment process and (ii) ensuring that individuals granted clearances continue to conduct themselves properly while possessing access to sensitive data. Errors introduced in these processes can evolve into system breakdowns where sensitive corporate information is either mistakenly or maliciously distributed beyond its authorized channels, causing immediate harm to the injured party and diminishing the trust of all participants in such a system, and returning all victim entities to a state of informational isolation that favors the attackers.

Implementation. With modern privacy-preserving information processing techniques, this unwieldy inter-organizational clearance system can be obviated. A class of techniques relevant to this problem is known as secure multiparty computation (SMPC). The general concept is that there are multiple parties who possess private information, who wish to perform a joint computation which (i) requires the input of the information from all parties and (ii) whose outcome is visible to all parties. However, each party wishes to keep their information private, and not allow any other party to gain any insight into their information through the joint computation process. As a classic example: two millionaires may wish to determine which one of them is wealthier, without revealing their wealth value to the other. [52]

Such methods have already been generalized to much more sophisticated problems. Today, there are estimated to be over 1000 satellites in Earth orbit, half of which are maintained by countries other than the U.S. Because of the nontrivial probability of collision, this poses the well-known "conjunction analysis problem" – in which various national agencies wish to perform joint computations of satellite trajectories to avoid collisions, but wish to keep the trajectory information of their own satellites completely private. The primary challenge of implementing such SMPC methods for nontrivial calculations is that large computational overheads that are incurred. Recent work in this area has demonstrated the viability of a model in which a large number of participants can perform joint computations of a highly sophisticated

variety in a pairwise manner.[53] The sophistication of the dynamical calculations performed in this work suggests that information synthesis at a deep level – encompassing the full range of threat scenarios emanating from cyber and human economic espionage threats – is within reach.

The institutional infrastructure for such privacy-preserving information sharing already exists through the ISACs, which cover a broad swathe of industries critical to national security. Beyond the safe sharing of information between private sector entities, such information exchange systems can hypothetically enable information exchanges between governments and private firms to bolster industrial defense against cyber and other economic espionage threats. The appeal of such methods is that the assurance of privacy-preservation does not depend on the good behavior or the non-failure of human security protocols, but rather the mathematically well-defined cryptographic hard problems that would have to be solved to violate the privacy of a participant. Whereas the CSPO technologies do not rely on laws but hard mathematics to protect the IP in software, SMPC relies not on good conduct by the members of the information-sharing pools, but also on hard mathematics to protect the privacy of the members.

Battles Without Strategy, and a War Without Tactics

Changing the Economics of the Attacker-Defender Dynamic Through Technology

Our present national struggle against IP theft, piracy, and espionage is simultaneously (i) a string of battles fought without strategy, and (ii) a war fought without tactics. When the occasional bad actor – cyber or traditional, state or non-state – is interdicted[54] or at least identified,[55] there is a sense that battles have been won – but there is no sense as to how any configuration of such victories translate into a desirable strategic end state – or even what a realistic strategic end state could be. On the other hand, broad doctrinal pronouncements calling for the marshaling and reorganization of national resources – public and private – to meet the great existential threat of IP theft to the foundation of our economy – are invariably appended to tactical playbooks that reprise almost exactly the methods that completely failed the British in the late eighteenth century. IP theft at its core is an economic phenomenon. The solutions to it, wherever they may exist, will be driven by economics, not laws or diplomacy. Future strategy for the defense of the U.S. intellectual property base should be built on techno-economic foundations, not just juridical or diplomatic ones. The tactics that support this strategy should have technical bite, rather than just legal or diplomatic bark.

The economics of the status quo greatly favor the attacker. The risks of IP theft in today's world are low. The beginnings of any juridical or diplomatic remedy begin with attribution, and flat denial is a consistently effective rhetorical strategy when incontrovertible, evidence-based attribution is the exception rather than the rule. The rewards are greater than ever, as the force multiplier of cyber and informational technologies allows the attacker to reach more victims and extract more from each victim. The juridical punishments and diplomatic censure relied upon in the present day, echoing the British analogues two centuries ago, are calculated to alter the economics of would-be attackers by introducing an element of deterrence: lengthy prison sentences and fines for non-state actors, and diplomatic consequences for states. But history indicates that such methods do not work, and if a latter day Henry Wansey were to tour the industrial districts of some of America's major geopolitical rivals today, he would be hard pressed to find something that is manufactured by U.S. industry that cannot be made, with very much the same methods, overseas.

The economics must be transformed by technology. If, for instance, a class of technologies analogous to the obfuscation technologies for software or hardware can be expanded to broader categories of economically-important IP—materials, chemicals, hardware, industrial processes,

media, to consider a few—the technical difficulty of IP theft can be raised to sufficiently high levels that it no longer becomes a cost-effective activity. Tactics based on juridical punishments catch perpetrators one at a time. But what is not known—and may be unknowable—is the number of perpetrators that may never be caught. With such juridical tactics, we win battles while not only losing the war, but also not even having the metrics to understand how rapidly and how devastating our losses are. Tactics based on technology are fundamentally different. When, for instance, a piece of commercial software is distributed to the open market, where it falls into the hands of legitimate customers and IP reverse engineers alike, cryptographic obfuscation assures that all who seek to steal the IP—seen by us or not—face exactly the same technical challenges in extracting the IP. If a would-be pirate cannot crack the cryptographic puzzles required to reverse engineer the software, it does not help him that he operates beyond our ability to attribute or arrest; the laws of mathematics are limitless in their jurisdiction.

Where such IP cannot be protected technologically at the product level, as with cryptographic obfuscation, more robust information pooling among victims of traditional economic espionage, enabled with privacy-preserving information processing technologies could also substantially raise the costs of economic espionage in their own right. Cybercrime is a rare kind in which the victims have strong economic incentives to cover up their own victimhood, because of the various legal, fiduciary, and public relations consequences of the disclosure of such incidents. The current ISAC infrastructure is only as effective as its participants are willing to trust. However, with new SMPC technologies, participants need not trust each other—only the cryptographic assurances of privacy established by hard mathematics. As much as SMPC is another technological tactic to raise the costs of the attacker by diminishing the reusability of his cyber toolbox, it also has a positive effect on the economics of the victim's decision making process, which can now reap a far greater return on sensitive information sharing about attackers, for a lower degree of risk that is furthermore quantified by the mathematical protocols particular to a specific implementation of SMPC—in contrast to the presently unquantifiable risk of insiders and other participants acting in bad faith.

Conclusion

The history of the American IP privateering campaign against the UK not only offers a troubling vision for the future state of a world in which the United States loses its present-day defensive struggle against IP privateering, but also demonstrates the limitations of law and diplomacy as a means of stanching IP theft. What potentially changes the dynamic in the twenty-first century is that technology makes possible technological tactics for IP defense that may fundamentally transform the strategic landscape of the struggle to protect the ideas that form the foundation of our economic prosperity and strategic security. It is fitting that the technological ingenuity of the American system that has produced so many value-creating, world-changing ideas can be the source of defenses to protect those very ideas.

---

[1] Ben-Atar, Doron. *Trade Secrets: Intellectual Piracy and the Origins of American Industrial Power*. (New Haven: Yale University Press, 2004). Print.

[2] Bureau of Economic Affairs. "Intellectial Property and the U.S. Economy: Industries in Focus." April 13, 2012. *United States Patent and Trademark Office*. Report accessed via Web, March 9, 2015.

[3] A letter of marque is: "written authority granted to a private person by a government to seize the subjects of a foreign state or their goods; specifically**:** a license granted to a private person to fit out an armed ship to plunder the enemy," *Miriam-Webster Dictionary (*Encyclopædia Britannica*)*. <http://www.merriam-webster.com/dictionary/letters%20of%20marque>

[4] Hamilton, Alexander. "Report on Manufactures." *Annals of Congress*. December 5, 1791.

[5] Ibid.

[6] Jeremy, David. "British Textile Technology Transmission to the United States: The Philadelphia Region Experience, 1770-1820." *Business History Review* (1973): 51-2. Print.

[7] Op cit at # 4.

[8] This American campaign to acquire sensitive British IP is described synoptically in Peter Andreas' *Smuggler Nation: How Illicit Trade Made America*. New York: Oxford University Press, 2013. Print.

[9] Op cit at # 4.

[10] Ibid.

[11] Op cit at # 8.

[12] Ibid.

[13] Op cit at # 6.

[14] Coxe often blurred the line between private and official interests by personally investing in various enterprises to personally profit from the extraction of IP from British industry. [Andreas 2013, op cit. at # 8.]

[15] Op cit at # 6.

[16] Op cit at # 8.

[17] Jeremy, David. "Damming the Flood: British Government Efforts to Check the Outflow of Technicans and Machinery, 1780-1843." *Business History Review* (1977): 1-34. Print.

[18] Op cit at # 6.

[19] Op cit at # 17.

[20] Ibid.

[21] Ibid.

[22] Op cit at # 6.

[23] Op cit at # 17.

[24] Op cit at # 8.

[25] Op cit at # 17.

[26] Ibid.

[27] Ibid.

[28] Op cit at # 8.

[29] Resor, Randolph. "Rubber in Brazil: Dominance and Collapse, 1876-1945." *Business History Review* (1977): 341-366. Print.

[30] Li, Lillian. *China's Silk Trade: Traditional Industry in the Modern World, 1842-1937*. Cambridge, MA: Harvard University Asia Center, 1981. Print.

[31] Clinton, William. *Statement on Signing the Economic Espionage Act of 1996*. October 11 , 1996. Accessed on Web, March 9. 2015. <http://www.gpo.gov/fdsys/pkg/PPP-1996-book2/html/PPP-1996-book2-doc-pg1814.htm>.

[32] United States Cong. House. *Foreign and Economic Espionage Penalty Enhancement Act of 2012*. Washington, DC: U.S. Government Printing Office, 2012. Print.

[33] The Commission on the Theft of American Intellectual Property. *The IP Commission Report: The Report of the Commission on the Theft of American Intellectual Property*. Research Report. Washington, DC: The National Bureau of Asian Research, 2013. Report via Web.

[34] Ibid.

[35] Baucus, Max. "Nomination Hearing, To Be Ambassador To China." 28 January 2014. *United States Senate Committee on Foreign Relations*. Accessed on Web, March 9, 2015.

[36] Clapper, James. "Worldwide Threat Assessment of the U.S. Intelligence Community." 29 January 2014. *United States Senate Select Committee on Intelligence*. Report accessed via Web, March 9, 2015.

[37] Op cit at # 8.

[38] Op cit at # 33.

[39] Ibid.

[40] Op cit at # 2.

[41] Business Software Alliance. "Shadow Market: 2011 BSA Global Software Piracy Study." 15 May 2012. *BSA Global Piracy Study*. Report accessed via Web, March 9, 2015.

[42] Ibid.

[43] Collberg, Christian and Jasvir Nagra. *Surreptitious Software: Obfuscation, Watermarking, and Tamperproofing for Software Protection*. Ann Arbor: Addison-Wesley/Pearson Education, 2009. Print.

[44] Garg, Sanjam et al. "Candidate Indistinguishability Obfuscation and Functional Encryption for all circuits." *IEEE 54th Annual Symposium on Foundations of Computer Science*. Berkeley, CA: IEEE, 2013. 40-49. Web.

[45] Op cit at # 31.

[46] NCI. *National Council of ISACs*. 2014. Accessed via Web, March 9. 2015 .

[47] "Vetting and Trust for Communication among ISACs and Government Entities," ISAC Council White Paper, January 31, 2004; p. 2. Report via Web.

[48] Ibid, p. 2.

[49] Ibid, p. 2.

[50] Ibid, p. 2.

[51] INSA Security Clearance Reform Task Force. *Next Steps for Security Reform: Industry Proposals to Enhance Efficiency and Reduce Costs in National Security Contracts*. White Paper. Arlington, VA:Intelligence and National Security Alliance, 2011. Report via Web.

[52] Yao, Andrew. "Protocols for secure computations." *DFCS 23rd Annual Symposium on Foundations of Computer Science*. Chicago: IEEE, 1982. 160-164. Print.

[53] Hemenway, Brett, William Welser IV, and Dave Baiocchi. *Achieving Higher-Fidelity Conjunction Analyses Using Cryptography to Improve Information Sharing*. Research Report. Washington, DC: RAND Corporation, 2014. Report via Web.

[54] Office of Public Affairs. "Sinovel Corporation and Three Individuals Charged in Wisconsin with Theft of Amsc Trade Secrets." June 27, 2013. *United States Department of Justice*. Web. 9 March 2015.

[55] United States of America v. Wang Dong, Sun Kailang, Wen Xinyu, Huang Zhengyu, Gu Chunhui. No. 14-118. U.S. District Court, Western District of Pennsylvania. May 1, 2014. Web.

Chapter 4

The Cyber Financial Wars on the Horizon: The Convergence of Financial and Cyber Warfare and the Need for a 21st Century National Security Response

By Juan C. Zarate[1]

Introduction

Cyberattacks and intrusions threaten U.S. private sector institutions on a daily basis. From cyber fraud to sophisticated intrusions into sensitive systems, the Western private sector has been under direct assault for years from myriad sources: low-level criminals and major state actors alike. Over the years, these attacks have cost the private sector billions of dollars of intellectual property and years of research and development and cast doubt on the ability of companies to secure customers' data and their systems. And now, the financial industry—namely major Western banks—finds itself at the center of this cyber storm.

On Thursday, October 2, 2014, JPMorgan Chase & Co., the largest American bank by assets, announced that a cyberattack it had detected in mid-August 2014 had compromised the accounts of 76 million households and seven million small businesses. The JPMorgan attack—which began in June and is believed to have originated from Russia—went unnoticed for two months, despite the $250m in cybersecurity that the bank expected to spend by year's end. Hackers had gained access to the bank's servers containing the names, email addresses, phone numbers, and addresses of both current and former customers. The same group of overseas hackers appears to have attempted to infiltrate at least twelve other financial institutions, including Fidelity Investments.[2]

JPMorgan maintains that the hackers were unable to gather detailed information that would be particularly damaging to consumers and that no fraudulent activity has been reported.

Passwords, account numbers, social security numbers, dates of birth, and other information valuable to any cyberattacker looking for financial gain remain unperturbed. In a statement to its customers, the bank insisted that customer money was "safe."[3]

Some have rightly noted that if the attackers were good enough to compromise JPMorgan's network, they may have left themselves backdoors into their servers that remain undetected. Cybersecurity experts have opined that there is a possibility that "ghost" or undetected intrusions may still be of concern.[4] It remains unclear exactly how much information the hackers accessed, but the number of those affected makes the breach one of the largest ever. Indeed, the hackers may have also been sending a message to the bank, industry, and U.S. government about their capabilities with the extent and reach of their intrusion.

The Treasury Department, Secret Service, Federal Bureau of Investigation (FBI), and other U.S. intelligence agencies have worked directly with JPMorgan following the intrusion, but identifying the exact identities and motivations of these hackers has been slow, grinding work. JPMorgan's size, its complex IT environment, and numerous third-party suppliers make it particularly vulnerable and an appealing target to attackers. Determining whether the hacking group was after notoriety or financial gain – or more likely some combination of both – could have major implications for our understanding of the attack – including whether this was a new form of state-sponsored cyberwarfare.

The U.S. government understood the potential significance of this attack and watched the forensics unfold over the summer – concerned this could be a new stealth attack from a state actor. When briefed by national security officials on the ongoing JPMorgan breach, President Obama reportedly asked his team whether this could be Putin's retaliation for Western sanctions. The U.S. government could not provide a definitive answer.[5] Joel Brenner, a former inspector general and senior counsel of the National Security Agency, wrote that Russia's likely use of proxies in the JPMorgan case "is what the gray space between war and peace looks like."[6]

Despite the range and years of cybersecurity initiatives and investments within government and the private sector, the scope of the attack on JPMorgan and other private sector companies over the years demonstrates the ease with which bad actors are able to infiltrate well-defended systems and potentially our most critical resources at home.

The attack on JPMorgan is perhaps the new face of cybercrime. Although organized criminals' ultimate goals are familiar, their methods are constantly evolving with escalating attempts to exploit cyber vulnerabilities for profit. This may also represent the new arena of asymmetric state warfare, with less powerful states able to send clear messages and threats to the United States and its allies by enlisting cyber actors. With the North Korean hack of Sony systems in December 2014, including the destruction of data, publication of sensitive internal communications, and threats of violence for production of the film, "The Interview," this new era is plainly upon us.

Nation states unable to compete in open markets are increasingly turning to illicit tools for financial gain. Enabling shadow proxy forces to do the dirty work of infiltrations and data collection, these rogue actors exploit trade secrets, critical infrastructure, and – increasingly – financial information for their own gain.

The frequency and sophistication of attacks on banks are increasing, with each attack representing a more dangerous intrusion and demonstration of systemic vulnerabilities. CitiBank reports ten million cyberattacks on its system a month.[7] Banks are prime targets for sophisticated, organized cyber criminals. Banks hold not just money and customer accounts, but also collect and centralize sensitive customer data and some clients' intellectual property.

More importantly, banks have been pulled into a more serious and sustained cyber financial battle. Nation states and their proxies realize that banks serve as both key systemic

actors important for the functioning of the global economy and as chief protagonists in the isolation of rogue regimes and actors from the financial system. Thus, the financial community finds itself drawn into combined financial and cyber battles—neither of which it controls. This has led cybersecurity experts in the banking community to admit openly, "We are at war."[8]

In some cases, the threat may stem from within. In late November 2014, the security firm FireEye released a special report on a group it had dubbed "FIN4." Operating since at least mid-2013, FIN4 targeted individuals at over 100 companies with access to sensitive, not-yet-public information regarding merger and acquisition (M&A) deals and announcements with major ramifications for markets.[9] With native-English language skills and nuanced knowledge of corporate practices, the group used spear-phishing techniques to manipulate financial markets to its advantage using insider information. In a December 25, 2014 op-ed in *The Wall Street Journal*, Congressman Mike Rogers, the Chairman of the House Intelligence Committee, warned that FIN4 was a harbinger of the kind of cyber and financial threat to come.[10]

Western banks and the financial system are now encountering the convergence between economic and cyberwarfare. We have entered a new era of financial influence where financial and economic tools have taken pride of place as instruments of national security. The conflicts of this age are likely to be fought with markets, not just militaries, and in boardrooms, not just battlefields. Geopolitics is now a game best played with financial and commercial weapons.[11]

And those weapons now include cyber tools, used by non-state and state actors alike to attack banks and financial systems. The new geo-economic game may be more efficient and subtle than past geopolitical competitions, but it is no less ruthless and destructive. Major and minor state powers, along with super-empowered individuals and networks, can harness economic interdependence and cyber weapons to increase their global power status at the expense of their geopolitical rivals. The danger emerging is the coalition of actors—perhaps states using non-state proxies in cyberspace—launching financial and cyber assaults.

So far, the United States has been at the cutting edge of this competition. But the fact that it was first to develop innovative and powerful financial and cyber tools to pursue its interests is no guarantee of continued success. Indeed, there is the potential for greater U.S. vulnerability and decreased financial and economic leverage. Although the United States has had a near monopoly on the use of targeted financial pressure over the past decade, this edge is likely to erode, leaving the United States both more vulnerable to external financial pressure and less able to use financial suasion as a lever of foreign policy.[12]

The need for urgent attention to this convergence within the financial community and among Washington policymakers is clear. Benjamin Lawsky, superintendent for New York's Department of Financial Services, the city's top banking regulator, said, "The cyber threat has to become urgent, one of the most important issues facing financial sector chief executives. It's got to be at the chief executive level. It is not an IT problem. It is a bank problem."[13] The failure of Washington lawmakers to innovate and enable relationships and cyber capabilities between the private sector and government – long understood to be essential to cybersecurity – has become even more problematic.

The current level of interaction between stakeholders is not sufficient to address the growing threat from cyber financial attacks. There needs to be a more aggressive approach to private sector defense of its systems and public-private collaboration to defend critical financial systems. This approach would borrow in part from the post 9/11 anti-money laundering and sanctions model to leverage financial suasion against rogue capital and actors as a way of protecting the financial system. This would also entail a more aggressive "cyber privateering" model to empower and enlist the private sector to better defend its systems in coordination with the government.

This paper will explore the growing cyber-financial threat, the actors and vectors involved, the way in which the U.S. government and private sector are currently addressing this vulnerability, and the need for a revolutionary approach that empowers and enlists the private sector as key actors in this domain.

The Evolution of the Cyber Financial Threat

The United States today faces unique systemic vulnerabilities and internal weaknesses that adversaries could exploit. The United States has been the driver of a globalized financial and commercial order, but it is also more dependent than other countries upon the economic and digital systems for trade, financing, and information on which that order has been built. As such, although the United States is well-equipped to fight kinetic wars, it remains uniquely vulnerable to financial warfare.

Perhaps the biggest source of U.S. vulnerability is not in terms of physical resources, but rather in virtual systems. As former director of national intelligence Mike McConnell noted before the Senate, "If we were in a cyberwar today, the United States would lose. This is not because we do not have talented people or cutting-edge technology; it is because we are simply the most dependent and the most vulnerable."[14] The Internet contributed an estimated 15 percent to the U.S. GDP between 2004 and 2009, and U.S. companies captured 35 percent of total Internet revenues earned by the top 250 Internet-related companies in the world.

In a 2013 speech, General Keith Alexander, the former head of the National Security Agency and Cyber Command, pointed to a seventeen-fold increase in attacks against U.S. infrastructure between 2009 and 2011, and graded U.S. preparedness to withstand a cyber-attack against its critical network infrastructure as "around a 3" on a 10-point scale.[15]

The cyber domain is the newest "final" frontier of geopolitical competition. The early, low-grade cyber battle in which Google and China have engaged, with Google fighting off mass penetrations and theft of its data (including proprietary information as well as information tied to the identities of Chinese dissidents), shows that this is a realm in which state and non-state actors can intermingle and do battle anonymously or via proxy. In addition, the cyber-realm is one in which infrastructure can be disrupted remotely. The globalized cyber supply chain can be easily manipulated. Since hard drives, chips, and the backbone of the cyber-infrastructure (including the increasing reliance on cloud computing) come from overseas, especially from East Asia, this is a particular concern for the United States.

Given the criminal opportunities that abound globally, it is no surprise that cyber-intrusions and attacks are increasing at a devastating rate—with billions of dollars' worth of intellectual property and value stolen digitally every year. It is estimated that the cost of cyber-crime to the global economy could be more than $500 billion annually.[16] Over the past few years, economic cyber-intrusions and targeted searches and attacks have hit the International Monetary Fund, Lockheed Martin's information systems (via stolen SecurID data), Google's mainframes, Sony's Playstation data, Bank of America, and Citibank.

In the words of General Keith Alexander, cyberattacks on the United States are resulting in the "greatest transfer of wealth in history." The blending of financial and cyberwarfare represents the new frontier.

On August 3, 2011, the computer security firm McAfee issued a report revealing the largest "cyberattack to date," which had targeted the data and systems of seventy-two organizations and companies around the world for over five years—enabled by an unidentified state actor presumed to be China. According to McAfee's former vice president of threat research, Dmitri Alperovitch, "what is happening to all this data is still largely an open question. However, if

even a fraction of it is used to build better competing products or beat a competitor at a key negotiation (due to having stolen the other team's playbook), the loss represents a massive economic threat."

This McAfee report was preceded by a February 8, 2011, report, also by McAfee, detailing the hacking of several U.S. oil companies from 2008 to 2010—with the cyber-intruders likely coming from China and having found their way into sensitive research and development files. This was the first time that such a massive intrusion and economic espionage operation had been reportedly directed at U.S. oil company computers. U.S. state secrets were not at risk, but valuable economic and oil resource research was. This research was vital to bidding by U.S. oil companies on oil-field rights in Iraq, Sudan, Ghana, and other lucrative sites around the world.

The Chinese government – likely in coordination with the People's Liberation Army – continues to pose a threat to U.S. industry. As recently as October 15, 2014, the FBI issued a private warning to American companies that "a group of highly skilled government hackers is in the midst of a long-running campaign to steal valuable data from U.S. companies and government agencies."[17] This latest announcement is just one in an ongoing series of cyberattacks against U.S. industry; however, the source of the threat appears to have evolved since security firm Mandiant revealed in February 2013 that the People's Liberation Army Unit 61398 was stealing corporate and government secrets. The FBI warning said that the state-sponsored group was "exceedingly stealthy and agile by comparison with PLA unit 61398."[18]

The United States is not alone in experiencing attacks from China's Advanced Persistent Threat (APT1) malware. According to an October 13, 2014 blog post from technology security firm FireEye, China has also taken advantage of its new bilateral economic partnerships with Australia to threaten key sectors, including data theft from its mining and natural resource firms.[19] The group's patience and ability to identify four "zero-day" vulnerabilities in Microsoft's Windows operating system while maintaining a low profile point directly to a state-sponsored entity.

It should come as no surprise that the bulk of cyberattacks today come from China, Russia, Iran, and North Korea. As James A. Lewis, a cybersecurity expert at the Center for Strategic and International Studies, has written, "These countries are our military rivals. Cyberspace creates opportunities to exercise national power, and these nations have seized these opportunities."[20] Yet cyberwarfare is not "war" in the Clausewitzian sense, although hacking is often conducted as "the continuation of politics by other means." Our opponents rely on the reliable functioning of international economic infrastructure, and therefore – to date – appear constrained to conduct systemic or catastrophic attacks on the United States that might collapse international systems or prompt a massive retaliation.

Evidence suggests that state-sponsored cyberwarfare is intensifying as part of a growing "cyber arms race." The most prominent cyber-battle to date was the use of the Stuxnet virus—believed to have been jointly developed by the United States and Israel—to sabotage Iranian nuclear facilities, and its subsequent "escape" on the Internet. But interestingly, the cyber-battles of today are beginning to meld with the strategies and tactics of financial warfare. This is also a theater of battle in which multiple actors can align for a common purpose, combining state and non-state proxies in the cyber-domain. A recently deployed cyber-weapon clearly illustrates the players, payoffs, and perils of cyber-espionage and warfare through economic and digital means.

On August 9, 2012, the Moscow-based security firm Kaspersky Lab announced that it had discovered a new "Gauss" virus (named after a file name in its codebase). Kaspersky Lab has historical connections to Russian intelligence and has made a practice of outing and analyzing computer viruses—often using crowdsourcing to help break codes. The Gauss virus had infected

approximately 2,500 computers, the majority of which—1,660, to be exact, including 483 in Israel and 261 in the Palestinian territories—are tied to Lebanese banks, with the first attacks going back to at least September 2011. Once the infection took hold, Gauss was capable of capturing and transmitting detailed records of information, such as browser histories, cookies, profiles, and system configurations. Once the virus was discovered, its communications were shut down, but not disabled. Apparently, they are still lying dormant, awaiting activation by an unknown controlling source.

Gauss's complexity and sophistication have led Kaspersky's experts to conclude that the virus is a state-sponsored descendant of Stuxnet, coming from the same "factory." It is able to track flows of money and tap into infected computers. But it also carries an encrypted "payload" that targets specific systems, much like the Stuxnet virus. Perhaps most revealing is that Gauss shares critical coding and platform features with the Flame virus, another data-mining virus and Stuxnet family member capable of extensive surveillance of infected computers that was discovered on Iranian computers in May 2012. But whereas Flame, which infected only seven hundred computers, cast a wide net toward all types of data, Gauss's focus is more attenuated, capturing primarily transaction data from a handful of specific Lebanese banks. Indeed, unlike typical non-state cyber-criminal malware, which tends to target a large number of small banks, Gauss targets a small number of large banks.

Gauss is so complex that Kaspersky has not been able to determine the function of its payload (what it has designated "resource 100"), though the firm suspects that it could trigger the destruction of critical infrastructure or some other high-profile target. For more details, Kaspersky crowd-sourced the solution on August 12, 2012, asking freelance hackers to crack the payload encryption and publishing the first 32 bytes of each encrypted section in Gauss to facilitate the process. By December 27, just a few months later and responding to Kaspersky's call, a well-known hacker posted open-source software he called "Gauss cracker," which represented a "major breakthrough" toward solving the encrypted Gauss payload.[21] Previously, Kaspersky successfully used crowd-sourcing to identify the programming language used in the state-sponsored DuQu malware.[22]

In light of the target, the claim of state sponsorship makes sense. Lebanon is "something like the Switzerland of the modern Middle East," wrote Katherine Maher, a digital rights security expert, in *The Atlantic*. "More than 60 banks manage nearly $120 billion in private deposits in a country of 4.3 million people, and account for roughly 35 percent of the country's economic activity."[23] Lebanese banks have been among the most secretive in the world, and their opacity has long been a concern for U.S. and international financial regulators seeking to disrupt money launderers and terrorist financiers. The Lebanese banking system has come under direct fire as a financial way station for Iran, Syria, Hezbollah, and illicit financial flows.

With Stuxnet and Flame, the target was a rogue regime's nuclear program. With Gauss, the target seems to be the banks of an important financial center in the Middle East, where rogue elements leverage the banking facilities. Western states' interest in Lebanon's private sector has traditionally focused on "know your customer" and transaction data rules. Gauss now ups the ante with aggressive information collection and destructive payload delivery.[24]

All of this suggests that states are willing to use cyber-weapons to impact the banking system and to engage in open cyber financial warfare. If Stuxnet and Flame represent the more "conventional" forms of cyberwarfare, then Gauss is akin to financial counterinsurgency: long-term, low-grade, persistent conflict rather than quick, high-profile battles with decisive results. This is a messy process, one with no clear line between enemies and friends or between private and public interests.

The process also raises a host of questions about the ethics of cyberwarfare and about the overall stability of the global financial system. How does such a financial system go about its business in the shadow of an indecipherable payload that could potentially sabotage the system's entire infrastructure? Perhaps the very existence and broader awareness of the virus is good enough—with the intended goal simply to engender a loss of faith and confidence in the Beirut financial system. Without trust, no financial center can last.

Gauss seems to represent the leading edge of cyber financial warfare. This is a type of conflict in which there are no clear rules, no ceasefires, and no uniforms or banners to identify the combatants. What is more, despite the fact that the United States starts with an enormous technological advantage, its size, relative transparency, and legal constraints may place it at a disadvantage on this type of cyber battlefield.

Indeed, this is a battlefield defined by potential asymmetric power disparities. An individual hacker can emerge as a cyberpower, one whose relative isolation, anonymity, and small footprint is a source of strength.

The Iranian government has entered the fray in response to the financial assault on its economy and currency. In September 2012, a Middle Eastern hacker group identifying itself as Izz ad-Din al-Qassam Cyber Fighters conducted a massive denial-of-service attack against the electronic banking operations of JPMorgan Chase, Citigroup, PNC Bank, Wells Fargo, U.S. Bancorp, and Bank of America. By increasing fake demands on the banks' sites at a rate some ten to twenty times higher than average denial-of-service attacks, the new group was able temporarily to suspend access to checking accounts, mortgages, and other bank services.[25] Perhaps more troubling is that the mysterious group warned these financial institutions that an attack was imminent, but the banks proved unable to stop it.

Though Izz ad-Din al-Qassam is also the name of the military wing of Hamas, Senator Joseph Lieberman, then chairman of the Homeland Security Committee, argued that the attacks were connected to the Iranian Islamic Revolutionary Guard Corps–Qods Force.[26] Major banks, including non-U.S. banks, continue to be attacked by intense denial-of-service operations.

At the same time, hackers calling themselves the "Cutting Sword of Justice" attacked the computers and control systems of Saudi Arabia's national oil company, Aramco—which produces a tenth of the world's oil supply—for weeks. In December 2012, the Saudi government admitted that the virus, dubbed "Shamoon," had destroyed 30,000 computers and wiped out hard drives, but did not succeed in disrupting production or operations.

The methods of cyberwar will continue to evolve rapidly in sophistication. We can also expect the pace of cyberattacks to pick up. The technology of cyberwarfare is evolving at an exponential rate. Also, unlike traditional combat, cyberwarfare has few normative restraints to limit its escalation and few controls to counter its proliferation to non-state actors.

The Gauss incident highlights the vulnerability that is found in fragile financial markets. Regulators cannot keep up with the pace of growth taking place in the speed, level of anonymity, and volume of trading.

In what is described as a "race to zero," trading is moving faster and faster—and further away from the gaze and capacity of national regulators. According to trade negotiator Harald Malmgren and Mark Stys, it has gone "from trading in milliseconds (thousandths of a second) a couple of years ago to trading in microseconds (millionths of a second) now, and for cutting edge traders, pursuit in trading in picoseconds (trillionths of a second)."[27] High-frequency trading firms "represent approximately 2 percent of the 20,000 or so trading firms operating in the U.S. markets . . . [but] account for 73 percent of all U.S. equity trading volume," according to one trading technology consultant.[28]

During the "Flash Crash" episode of 2010, a trading algorithm dumped 75,000 futures contracts valued at $4.1 billion on the market in a twenty-minute period. The losses were staggering, causing a 600-point fall in the Dow and erasing $862 billion from the value of equities before an automatic circuit breaker paused trading.[29] Though the mass volume of such trading provides a buffer against manipulation, the sheer speed and anonymity of the cross-border trading across asset classes increase the risks and the potential for markets to be manipulated and cornered by savvy criminal and nefarious actors—for profit or other purposes.

According to the World Economic Forum's Global Risks 2015 Report, cyberspace will be increasingly at the center of both our geopolitical and economic worlds, representing a new frontier that will pose unprecedented challenges. This new variable in the geopolitical equation, the report says, "will [make] it difficult for decision-makers to predict the development of such situations as sanctions and other instruments of economic coercion, thus raising the risk of unintended consequences."[30] As cyberattacks threaten the financial system with greater frequency, the threat to the financial order and traditional geopolitical relationships increases.

The very nature and speed of electronic trading, the instant flow of information, and the financial system's reliance on the Internet creates vulnerabilities, and is amplified by the twenty-four-hour business news cycle and social media. The emergence of a sophisticated cyber financial market manipulation scheme by the group FIN4 is the most problematic and poignant example of this threat. The anonymity and speed of trade, combined with lax U.S. laws and regulatory oversight on beneficial ownership of companies and controlling interests of offshore investment funds, adds to the potential that criminals and nefarious actors could use the U.S. financial system not only to launder proceeds but to manipulate, corner, or extort via market control or penetration. The estimated amount of laundered funds that make their way through U.S. banks ranges conservatively between $250 billion and $500 billion a year.

Thus, strategies to manipulate markets could focus principally on shaping the perception of the markets and then leveraging the market swings to profit or destroy value. It is in part for this reason that the Securities and Exchange Commission (SEC) put new regulations in place to prevent uncovered short selling such as that seen during the financial crisis of 2008.

The coming financial battles may find their most serious theater and articulation in cyberspace, with the vulnerability of the financial sector and the international system of trading and commerce potentially at risk.

The Cyber Financial Battles Underway

Cybersecurity experts today identify four kinds of primary threat to the financial sector. First, sophisticated cyber actors – usually states – use espionage to steal intellectual capital and data from banks and destabilize them. Second, banks can be targeted for systemic disruption by a range of cyber actors who view them as symbols of Western capitalism or have reason to threaten the financial system. Third, "hacktivists" take advantage of vulnerabilities to break into banks' IT networks, usually in order to gain publicity for their cause. Finally, organized criminal organizations and cyber fraudsters have shifted from stealing money through traditional bank heists to using other means (online, telephone, card fraud) that are harder to detect.[31]

As recent attacks have made clear, no business, critical infrastructure, or private consumer – big or small, poorly or well protected – is completely immune to cyber threat. While the Syrian Electronic Army defaced prominent American media websites, a group of hackers known as "Dragonfly" inserted malware into the legitimate software of three industrial control systems manufacturers. 2013 saw a 91 percent increase in targeted attack campaigns. A co-authored report from the Center for Strategic and International Studies (CSIS), a prominent Washington think tank, and security firm McAfee, estimated the annual global cost of digital crime and

intellectual property theft at $445 billion.[32] On nearly every front, the number, creativity, and effectiveness of attacks continue to go up.

There is evidence, however, that gaining notoriety in the cyber realm for its own sake is losing appeal. In its place, there is a growing desire for investment in hacking to pay dividends with financial reward. As such, both state and non-state actors are increasingly training their sights on banks, whose defenses – though strong – contain by far the most lucrative and easily exploited data. Banks have long been a target for criminals, simply because they hold money; numerous small-scale attacks on large banks like JPMorgan Chase are a daily occurrence.

The most recent Office of the Comptroller of the Currency's Semi-Annual Risk Perspective shows alarming accelerated risk of cyberattacks in financial institutions. The problem is that criminals seeking information are getting better at accessing bank information as technology becomes cheaper and the barriers for entry to cybercrime drop.[33] Those historically rejected by the international financial system find themselves increasingly embraced by unscrupulous nation states willing to use their expertise to exploit weaknesses, and the line between state and non-state actors further blurs. Online markets for cyber hacking expertise allow for states and non-state actors to recruit front-line cyber proxies. Like never before, state-sponsored cyberattacks pose a threat to financial institutions.

The nexus between the financial sector and cybercrime is growing as never before. In July 2014, Bloomberg's *Businessweek* magazine reported that Russian hackers had "stolen the Nasdaq" back in October 2010.[34] An FBI internet traffic monitor had picked up signals indicating that malware had infiltrated the company's central servers. The event quickly prompted both the National Security Agency (NSA) and the National Cybersecurity and Communications Integration Center (NCCIC) – the latter one of the Department of Homeland Security's many information sharing and coordination centers – to get involved. Over a period of five months, an array of government agencies struggled to characterize and counter the state-sponsored cyberattack. For weeks, it remained unclear whether the attackers had compromised the trading platform, whether the breach was part of a larger attack, and which government agency was responsible for addressing which weakness.

Ultimately, the hack was disrupted, and there was no evidence that the hackers stole any valuable financial information. The "Nasdaq Hack" is nevertheless symptomatic of today's increased alignment of financial assets and cyber threats. Groups that target the U.S. stock market demonstrate not only their potential desire for financial gain, but also the desire to cripple an internationally recognizable symbol of Western power. Moreover, the confused and lethargic response of private and government entities illustrated the gridlock that continues to plague information-sharing and legislation in the cybersecurity realm.

State-sponsored attacks are not limited to a particular region or type. The Advanced Persistent Threat 1 (APT1) was described by Mandiant in a 2013 report as "one of the most prolific cyberespionage groups in terms of the sheer quantity of information stolen" and stated that the group had stolen terabytes of data from at least 141 organizations in 20 major industries, estimating that it was an organization with at least dozens, potentially hundreds, of human operators.[35] In its report, Mandiant claimed that APT1 is Unit 61398 of the Chinese People's Liberation Army, though China's Ministry of Defense has previously stated that it is "unprofessional and groundless to accuse the Chinese military of launching cyberattacks without any conclusive evidence."[36] Still, in over 97 percent of the 1,905 times Mandiant observed APT1 intruders connecting to their attack infrastructure, APT1 used IP addresses registered in Shanghai and systems set to use the Simplified Chinese language.

In March 2013, the "Dark Seoul" attacks targeted South Korean banks and other institutions. Believed to be part of a larger espionage campaign conducted by North Korea, Dark

Seoul deleted data from hard drives, targeted ATMs and mobile payment platforms, overloaded bank servers, and shut down computers at several South Korean media stations.

On August 5th, 2014, Hold Security reported that a Russian crime ring had amassed the largest known collection of stolen Internet credentials, including 1.2 billion user name and password combinations and more than 500 million email addresses.[37] The attack was not specifically targeted. The hackers targeted any website they could get, ranging from Fortune 500 companies to very small websites. On September 10th, the passwords and email addresses for close to 5 million Gmail accounts were posted to a Russian Bitcoin forum in a text file. While forum administrators were quick to remove all passwords from the file, there is no doubt some accounts are now compromised.

Cyber Tools and Actors

There are an array of cyber tools and methods used by a range of actors to attack and infiltrate financial and commercial systems. The breadth of international actors engaging in cyberattacks has complicated and accelerated the threat environment. In this context, there is a new risk of strategic cybersabotage, enabled by new cyber tools and cloaked by the vagaries of attribution. Terrorists or agents of hostile powers could mount attacks on companies and systems that control vital parts of an economy, including power stations, electrical grids and communications networks. Such attacks are hard to pull off, but not impossible.

Online underground markets for cybercrime remain prevalent and barriers to launching cybercriminal operations are fewer than ever. Toolkits are becoming cheaper and more available; some are even free of charge. Underground forums are thriving worldwide, particularly in China, Russia, and Brazil.

Financial Trojans represent one of the newest and fastest-growing threats to banks. Financial institutions have dealt with targeted malware for more than a decade, evolving their security measures to stay one step ahead of fraudsters. Security firm Symantec reports that these security solutions—often customized—were ineffective in protecting banks from the threat they faced, as cybercriminals "motivated by financial reward" outpaced them.[38] In 2013 alone, attackers using financial Trojans targeted over 1,400 financial institutions and the top 15 most targeted financial institutions were targeted by over 50 percent of known Trojans. The number of unique financial Trojans has quadrupled since January 2013, and unfortunately, the adoption rate of strong countermeasures has been too slow.[39]

State-sponsored malware and distributed denial-of-service (DDoS) attacks remain only one small but growing piece of the larger picture vulnerable to cyber threats. In 2013, over 552 million identities were exposed, web-based attacks went up 23 percent from 2012, and 23 zero-day vulnerabilities were discovered (up 61 percent from 2012). Healthcare and retail industries remain among the most targeted and most under-protected in cybersecurity. Attackers added watering-hole attacks to their arsenal, in which threat actors compromise a carefully selected website by inserting an exploit resulting in malware infection.

Reports of the death of spear-phishing – in which an attacker disguises himself as a friend or known entity and asks for sensitive financial information – were greatly exaggerated. Such campaigns increased a dramatic 91 percent in 2013.[40] Attacks now, however, use a "low and slow" approach, with both the total number of emails used per campaign and the number of those targeted decreasing. Ransomware scams – in which the attacker pretends to be local law enforcement, demanding a fake fine of between $100 and $500 – escalated in 2013 and grew by 500 percent over the course of the year. These attacks are highly profitable and attackers have adapted them to ensure they remain so. Related "Cryptolocker" scams are even more vicious.

An attacker drops any pretense of being law enforcement and will spontaneously encrypt a user's files and request a ransom for the files to be unencrypted.[41]

While the prevalence of mobile malware is still comparatively low, 2013 showed that the environment for an explosive growth of scams and malware attacks is here. The Norton Report 2014, a global survey of end-users, showed that 38 percent of mobile users had already experienced mobile cybercrime.[42] Although lost or stolen devices remain the biggest risk, mobile users continue to engage in dangerous habits – such as storing sensitive files online and sharing account logins with family – that leave them open to attack.

Despite crackdowns by authorities, illicit or problematic online networks prove resilient. Last November, administrators from the shuttered Silk Road online black market, led by a new pseudonymous Dread Pirate Roberts (DPR), re-launched the site. Dubbed "Silk Road 2.0", it recreated the original site's setup and promised improved security. The new DPR took the precaution of distributing encrypted copies of the site's source code to allow the site to be quickly recreated in the event of another shutdown.[43] In mid-September 2014, online black market Silk Road 2.0 experienced a DDoS attack, which forced the site's administrators to temporarily shut down service. News of the attack broke on Bitcoin forums hours after it started. There is speculation that the attack was launched by law enforcement trying to locate the Silk Road 2.0 servers, while others believe criminals or competitors launched the attack.[44]

In early July 2014, security company Symantec revealed that the group of hackers known as "Dragonfly" had inserted malware into the legitimate software of three manufacturers of industrial control systems.[45] Focused largely in the U.S. and European energy sectors, Dragonfly's targeted cyberespionage campaign gave the attackers the ability to sabotage major power supplies. The state-sponsored group—also known as "Energetic Bear" based somewhere in Eastern Europe—had been in operation since 2011, gaining long-term access to computers through spam email and watering hole attacks.[46] Dragonfly's ability to evolve in order to target new victims and remain unnoticed made it one of the most insidious groups ever to target American economic infrastructure.

In this environment, it has become increasingly difficult to distinguish state from non-state actors, as the former may use the latter as a proxy, quietly supporting the group while feigning innocence and denying involvement. Russia, in particular, has stepped up its cyber aggression when it perceives it is under attack from foreign entities. In its war with Georgia, the Russian state deployed cyberattacks as a complement to its military campaign. Following the relocation of a prominent Soviet-era statue in Estonia's capital of Tallinn in 2007, Russia bombarded Estonian organizations with DDoS attacks, marking one of the largest instances of state-sponsored cyberwarfare to date.[47] In recent months, dozens of computers in the Ukrainian prime minister's office and at least ten of Ukraine's embassies abroad have been infiltrated by a cyberespionage weapon linked to Russia.[48]

The Russian government does not always employ these cyber groups explicitly; however, they often maintain close ties to those in power and may benefit from a degree of funding. Scott Borg, chief executive of the U.S. Cyber Consequences Unit, an independent non-profit research institute said of Russian cyber criminals, "They are tolerated and even to some degree protected by the Russian government because they regularly engage in 'patriotic hacking.'"[49] Borg added, "they will often carry out cyberattacks that allow them to profit, while still falling in line with what they perceive to be Russia's political interests."[50] Alliances of convenience – between autocratic regimes and proxy groups around the world – may be the new modality in the cyber domain.

Private and Public Sector Response

Both the public and private sector have reacted to the growing threat from cyberattacks and intrusions – in large part by spending more on technical systems and expertise to defend against serious attacks. In recent years, spending on cybersecurity has exploded. Gartner, a research firm, estimates that in 2013 organizations around the globe spent $67 billion on information security. According to Allied Business Intelligence, Inc., cybersecurity spending by critical infrastructure industries alone was expected to hit $46 billion in 2013, up 10 percent from a year earlier.[51]

PricewaterhouseCooper's (PwC) 2014 Global Economic Crime Survey found that seven percent of U.S. organizations lost $1 million or more due to cybercrime incidents in 2013, compared with 3 percent of global organizations. 19 percent of U.S. entities reported financial losses of $50,000 to $1 million, compared with eight percent of worldwide respondents.[52]

Many U.S. retailers believe the risk of legal liability and costly lawsuits will escalate. Today, claims by businesses that they are unaware of cybercrime risks and the need to invest in updated cybersecurity safeguards have become increasingly unconvincing. Tom Ridge, CEO of security firm Ridge Global and first Secretary of Department of Homeland Security, said, "I think there will be a lot more litigation than we've seen in the past. These high-profile attacks have the attention of every board of directors."[53]

Cybersecurity analysts say that retailers are spending less on cybersecurity measures than banks and healthcare providers. Retailers spend 4 percent of their IT budgets on cybersecurity, while financial services and healthcare providers spend 5.5 percent and 5.6 percent, respectively. On cybersecurity spending per employee, the banking and finance industries spend roughly $2,500 per employee, while retailers invest about $400 per employee.[54] In early September 2014, Home Depot became the latest retailer to investigate a potential major breach of customer credit or debit card data. The stolen information from Home Depot will likely be put toward a massive new collection of stolen credit and debit cards that went on sale in early September in the cybercriminal underground.

Retailers spend far less than organizations of comparable size on cybersecurity, making themselves vulnerable to attack. Neiman Marcus Group, Sally Beauty Supply, Michaels, SuperValu, and Target Corp were targeted earlier this year. Research director for cybersecurity at Gartner Inc. Lawrence Pingree, said, "Retailers have been the low-hanging fruit for attackers since they don't spend as much as banks and government entities in cybersecurity."[55] In 2005, Gartner also said that for every $5.62 businesses spend after a breach, they could spend $1 beforehand on encryption and network protection to prevent intrusions and minimize damage.[56] Today, the ratio remains about the same. Perhaps most worrying is that companies often lack basic procedural guidelines for what to do when they are hacked. According to a PwC survey, only 49 percent of the CEOs in the study have a plan for responding to insider cybersecurity threats, despite evidence that those events are typically more damaging than those from outside.[57]

Regardless of the amounts spent, it is cheaper to hack than to defend a hack. Richard Bejtlich, chief security strategist at FireEye Inc. and a former cyber investigator for the U.S. Air Force, said he could assemble a team that could hack offensively into nearly any target.[58] But $1 million would not be nearly enough for a company to defend itself.

Thanks to the growing recognition of this threat, however, there is a greater impetus for government and private companies to cooperate and share information. On October 13, 2014, Jamie Dimon, chief executive of JPMorgan, exhorted his counterparts on Wall Street to coordinate their cybersecurity efforts while also calling on the U.S. government to help more

directly. He also pledged to double the bank's spending on digital security over the next four to five years.[59]

But collaboration between the public and private sector is not new. The Information Sharing and Analysis Centers (ISAC) fora have served as important venues for information sharing, and they have gained more momentum in the financial services and technology industries. The Financial Services Information Sharing and Analysis Center (or FS-ISAC) is the first widespread not-for-profit intelligence service designed to assist with cyber defense and analysis and has recently attracted extra funding from twelve large companies —including the financial, energy, transport, and healthcare sectors.[60]

The FS-ISAC has grown more operational over time. In June 2013, Microsoft teamed up with the FS-ISAC to disrupt the "Citadel" botnet, which cybercriminals deployed to infect thousands of computers to steal banking information and identities from unwitting victims. Microsoft, working with FBI, disrupted more than 1,000 botnets, but the malware resulted in losses of more than $500 million and affected more than five million people.[61] Most were located in the U.S., Europe, Hong Kong, Singapore, India, and Australia, but Microsoft has found evidence of Citadel in more than ninety countries.[62]

More recently, Microsoft assisted law enforcement in the United Kingdom to disrupt the "Caphaw" botnet, which targeted banks and their customers across Europe.[63]

On September 29, 2014, Microsoft and FS-ISAC expanded their operational relationship and signed a deal to share threat data when combating cybercrime, in a bid to help firms defend themselves against malware.[64] This will allow participating FS-ISAC members access to Microsoft's Cyber Threat Intelligence Program feed, giving them near real-time information on known malware infections affecting more than 67 million unique IP addresses.

FS-ISAC has recently teamed up with the Depository Trust and Clearing Corporation, which provides post-trade financial services, to launch a new software platform. Beginning with a pilot of 45 organizations, it will be used to share information about attacks and attempts at attack at a real-time speed intended to prevent hackers from deploying the same cyber weapons against several companies consecutively. The joint venture, known as Soltra, has seen its membership double since January as more institutions become aware of the threat.[65]

Until now, the process for sharing information in the private sector (and with government) has been threat-specific, slow, and not automated – or has relied on reports that are rarely analyzed, as with the security violations filed by financial institutions with the Treasury's Financial Crimes Enforcement Network, as part of Suspicious Activity Reports. It has also relied on private sector threat intelligence services that do not necessarily communicate with others.

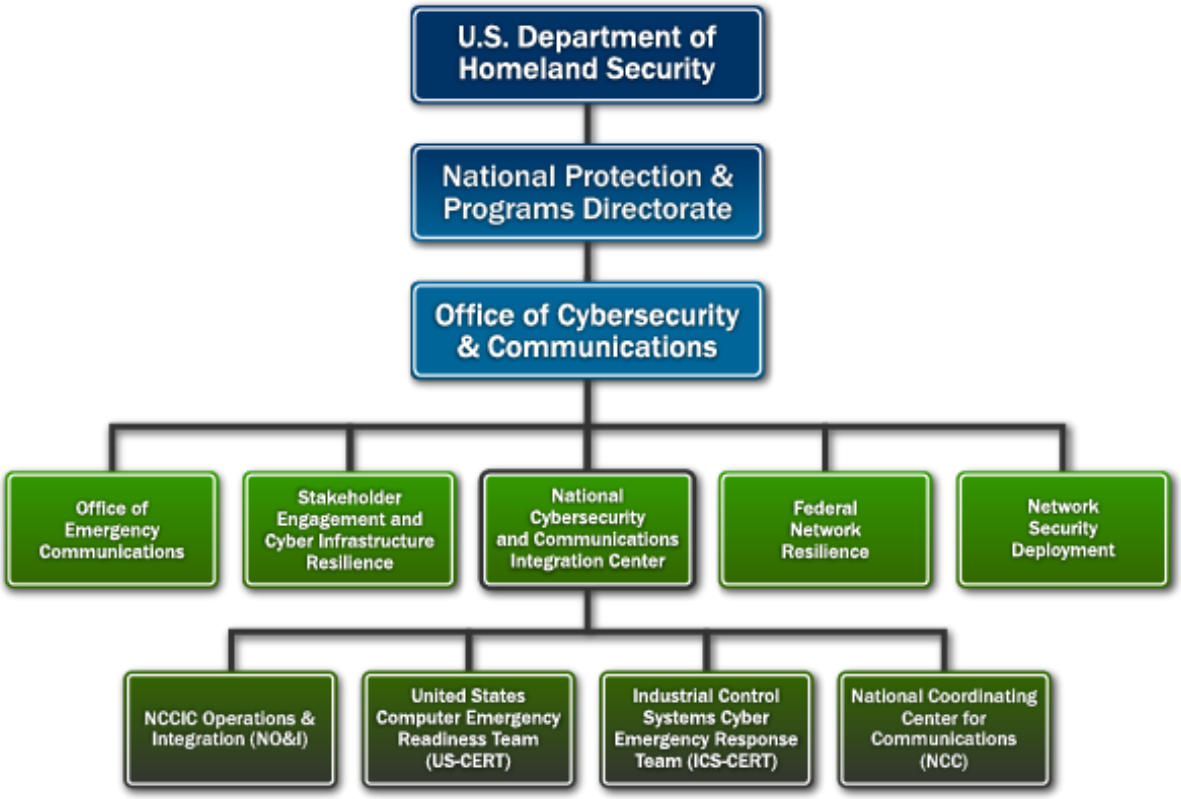
The Treasury Department has tried to accelerate the sharing of timely and actionable cybersecurity information that financial institutions can use to defend themselves by establishing the Cyber Intelligence Group. This group works closely with the FS-ISAC to produce circulars and information in response to requests by the financial sector.

More broadly, the U.S. government has attempted to bring more focus, coordination, and information sharing on the issue of cybersecurity. President Obama has repeatedly labeled cybersecurity a priority national security issue. Executive Order 13636 signed in February 2013 – "Improving Critical Infrastructure Cybersecurity" – gave rise to the National Institute of Standards and Technology's (NIST) Cybersecurity Framework, a compendium of best practices and security standards developed to perform risk assessment and mitigation, as well as encourage information-sharing between those in the private sector and government.

Cybersecurity legislation requiring heightened security protocols in the private sector and enabling better public-private information sharing has failed to pass in recent years, with cyber experts urging the Administration and Congress to pass new legislations. In his 2015 State of the Union address, President Obama urged Congress "to finally pass the legislation we need to better meet the evolving threat of cyberattacks."[66] This push, along with others from industry, has put cybersecurity information sharing at the forefront of congressional priorities.

The Obama Administration has also facilitated greater cooperation between the U.S. and the EU on cybersecurity issues. The new high-level U.S.-EU Cyber Dialogue announced at the 2014 U.S.-EU Summit will formalize and serve as the platform for closer U.S.-EU coordination on international cyberspace developments; the promotion and protection of human rights online; international security issues; such as norms of behavior in cyberspace, cybersecurity confidence building measures, and application of existing international law; and cybersecurity capacity building in third countries.

Exhibit 1



SOURCE: Department of Homeland Security.

Within the U.S. government, a range of departments, agencies, and shared initiatives is responsible for the nation's cybersecurity. The first line of defense is the U.S. intelligence community – including agencies within the NSA, FBI, and DHS – where monitoring systems and cyber analysts work to identify threats and disseminate information to the rest of government. At the Department of Homeland Security (DHS), the National Cybersecurity and Communications Integration Center (NCCIC) is a 24-7 cyber situational awareness, incident

response, and management center that is a national nexus of cyber and communications integration for federal government, intelligence community, and law enforcement.

Within DHS, the U.S. Secret Service uses the Electronic Crimes Task Force (ECTF) to leverage the combined resources of local, state, and law enforcement with prosecutors, private industry, and academia to combat cybercriminal activity. FBI's NCIJTF is its "next-generation cyber initiative" and serves as a coordination, integration, and information-sharing center for nineteen U.S. agencies and cyber threat investigations. FBI's Key Partnership Engagement Unit (KPEU) manages a targeted outreach program focused on building relationships with senior executives of key private sector corporations.

There has been no lack of effort by the U.S. government to try to increase information sharing with the private sector. Indeed, the private sector – including the financial industry – often feels bombarded by different agencies of government attempting to gain access to information or serve as the principal interlocutor for the government. They also feel exposed without legislation to protect their activities.

The private sector has tried to do its part in preparing the next generation to better understand the challenges of cybersecurity. At a Wilson Center event on October 16, 2014, officials from the University of Maryland, the Department of Homeland Security, and Northrop Grumman discussed cooperative efforts to build "tomorrow's workforce" of cyber-savvy leaders. With funding from Northrop Grumman, the University of Maryland's Honors College founded the Advanced Cybersecurity Experience for Students (ACES), the first four-year undergraduate program in cybersecurity that seeks to address the current shortage of cyber-enabled graduates.[67]

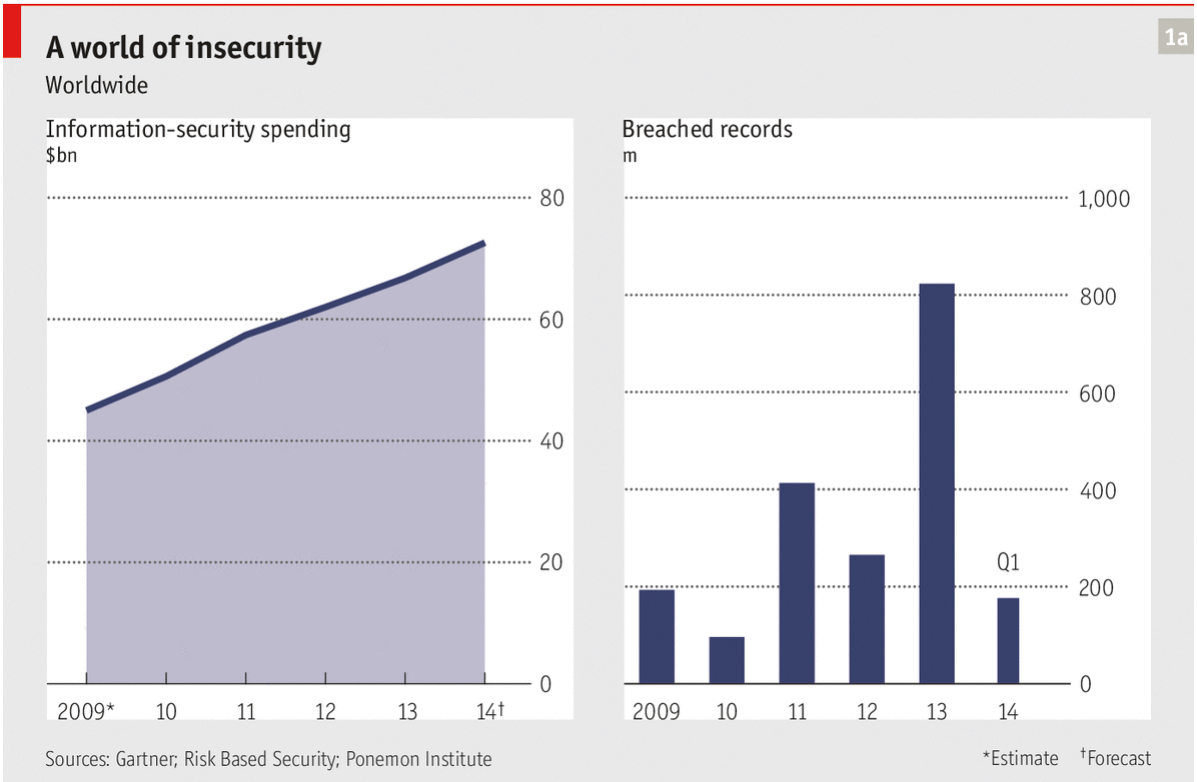
Attempts to bridge the public-private sector divide are not limited to the United States. On October 5, 2012, the United Kingdom established The Centre for Global Cyber-Security Capacity Building, which hoped "to draw on the expertise generated by eight research universities, is designed to improve international co-ordination, increase access to expertise, and promote good governance online."[68] It will act as a forum for collaboration between leaders from across the world, including from think tanks and the private sector.

The British Bankers Association (BBA) is another institution working toward better sharing of cyber information between public and private entities. The BBA plans to launch the Financial Crimes Alert Service (FCAS), designed to allow banks and other financial groups react faster to major incidents and to learn of the latest techniques used by fraudsters, cyber criminals, and terrorists.[69] BBA says it is working with BAE Systems to get the service up and running by early 2015.

The association's Chief Executive Anthony Browne called the FCAS "a powerful new weapon against fraudsters, cyber criminals and other crooks intent on stealing our clients' money," calling it "a shining example of how banks and government can work together to benefit all customers."[70] This will add onto the framework that already exists within the UK called the National Fraud Intelligence Bureau, which has prevented more than $163m of fraud losses through information-sharing. The new system will pool intelligence from twelve government and law enforcement agencies and share it with the teams working inside banks to combat fraud, cybercrime, terror financing, money laundering, and bribery.[71]

These are important attempts to foster more information sharing and real-time attempts to understand and counter breaches to key private sector data sets and systems. All of these models, however, maintain a strict divide between public and private sector actors, often with liability and risk attached to those private sector entities willing to share information or divulge openly their vulnerabilities.

Exhibit 2



To date, the approach applied by governments tends to be reactive and case-specific, with little capability to appreciate or communicate the systemic risks to key systems and infrastructure from sophisticated or even state actors. Under the current system, there is little incentive for pro-active defense of financial systems and legal restrictions on more aggressive monitoring and disruption in cyber-space by systemically relevant and important private sector entities.

Instead of fostering a culture of cooperation, the current model creates frustration as financial institutions feel more vulnerable and less able to defend their systems. They also feel less supported by the government. In a recent speech, Ellen Richey, Visa's vice chairman for risk and public policy, concluded, "The primary thing the government can do is number one, get out of the way. Eliminate the barriers that exist legally to sharing information, stop punishing the victim and assuming that every company that is breached is some sort of criminal and deserving of multiple investigations and lawsuits…"[72]

But in light of recent attacks, federal regulation organizations have come down hard on banks, urging them to more actively share their cyber threat information. Five of the United States' banking regulators – most prominently the Federal Financial Institutions Examination Council (FFIEC) – are threatening the industry with increased oversight if more stringent measures to protect consumer financial data are not implemented. An FFIEC report published alongside the announcement reinforced the need for engagement beyond the board of directors and senior management. The report emphasized the benefit of routinely discussing cybersecurity issues in meetings and identifying inherent vulnerabilities.[73]

In some cases, companies are considering more self-help options to defend their systems from identified hackers, like "hacking back" or "active defense" to defend against identified cyberattacks. This remains illegal under U.S. law; however, more financial executives and experts have begun discussing this option more openly in recent months. Technology research firm Gartner Inc. projects that countermeasures on the part of the cybersecurity industry will surpass $78 billion in 2015. House Homeland Security Committee Chairman Michael McCaul has said that "some victim companies may already be conducting offensive operations without permission from government and are 'very frustrated.'"[74] Regardless, a new, more pro-active model should be considered as the financial industry finds itself in the eye of the cyberstorm and as the financial system appears more and more at risk from sophisticated attackers.

A New Cyber-Privateering Framework

A new economic and cybersecurity approach requires a new paradigm of U.S. public-private engagement and collaboration. This involves an evolution from classic, state-based national security actions toward deeper involvement of the private sector in arenas previously confined to the halls of government, with a commensurate and widening appreciation within governments of the power of markets and the private sector to influence international security. In arenas like financial sanctions, and anti-money-laundering and counterterrorist-financing programs, the United States has already moved in this direction, relying on the private sector and the ability of financial institutions to act as gatekeepers to the financial system by identifying, reporting, and preventing the use of financial facilities by transnational actors and criminals of concern.

The utility of this approach is that it is not based on private sector altruism or civic duty, but on the self-interest of legitimate financial institutions that want to minimize the risk of facilitating illicit transactions that could bring high regulatory and reputational costs if uncovered. In other economic arenas, this symbiosis takes hold only with great effort, particularly given the private-sector aversion to increased regulatory burdens and associated costs. This means that governments need to check their regulatory practices and work closely to build consistent requirements and regimes across borders to help international financial institutions operate effectively and efficiently. The challenge of cooperation will be exacerbated as governments continue to unveil new regulatory structures and requirements in the wake of the 2008 financial crisis.

Innovation in public-private coordination is already occurring by necessity in the cyber-domain, with approximately 80 percent of cyber-infrastructure in private sector hands. After the attacks on Google servers by Chinese hackers, Google and the National Security Agency began to work together in 2010 to help Google defend against future attacks.[75] In the wake of the massive attacks on U.S. banks in 2012 and 2013, the National Security Agency had begun a pilot project with the banks to try to track and prevent cyberattacks.[76] Other pilot projects – driven by the private sector and governments – are emerging to accelerate information sharing and collaboration in creating defenses against significant cyberattacks. This kind of collaboration opens the door for more creative and widespread public-private cooperation to tackle cyber-threats and serves as a testing ground for such collaboration on broader issues of national economic security.

Indeed, the broader paradigm of leveraging financial suasion in national security involves empowering and catalyzing key private sector actors to protect the integrity of the financial system by making market and risk-based decisions. This paradigm can be the basis of this new framework to address financial cyberattacks.

In the first instance, financial and cyber intelligence need to be enhanced and driven toward the creation of useful, actionable information. Many banks are now establishing units – including internal financial intelligence units – to analyze internal data and understand and manage financial crime and sanctions compliance risk. These systems complement the cyber and technical defenses being built in all major financial institutions. Banks can build on these financial and analytic systems to better understand potential cyber intrusions and the transactions flowing through their systems.

More importantly, the private sector must be allowed to share more information with each other and government to detect and prevent cyberattacks. Secretary of the Treasury Jack Lew recently made the case for clearer rules of the road to allow for information sharing and protection of rights:

> As it stands, our laws do not do enough to foster information sharing and defend the public from digital threats. We need legislation with clear rules to encourage collaboration and provide important liability protection. It must be safe for companies to collaborate responsibly, without providing immunity for reckless, negligent or harmful behavior. And we need legislation that protects individual privacy and civil liberties, which are so essential to making the United States a free and open society.[77]

The current financial information-sharing regime requires financial institutions to monitor transactions and customer behavior and submit suspicious activity and other reports (to include information sharing about cyberattacks) to the U.S. Treasury, and provides for greater information sharing within the financial community. Section 314(b) of the USA PATRIOT Act allows financial institutions to share information about suspect financial activity within their sector without liability. There should be a similar provision for cyber intrusions and attacks, as well as legal safe harbors for cyber defense-related information sharing with and among private sector actors.

In addition to new forms of real-time and legally protected information sharing, new tools should be applied to accelerate the U.S. government's identification of state actors, networks, and individuals that attempt to breach U.S. private sector systems—especially financial systems. U.S. law enforcement has consistently investigated cases of breaches, including of organized crimes rings and hackers that successfully penetrate U.S.-based systems, with indictments often following.

The most significant indictment was made public on May 19, 2014, when the U.S. government charged five Chinese People's Liberation Army officials for cyberespionage. Though the individuals may never see the inside of a federal courthouse, the indictment was significant because it laid out the specifics of official Chinese cyberespionage and gave weight to U.S. government accusations that the Chinese government is behind massive, commercially motivated cyber infiltrations of the American private sector. These types of cases need to be pursued and networks of cyber criminals—of whatever type—exposed. Such cases, in combination with the aggressive enforcement of financial criminal statutes against those that are directing and financially benefitting from cyber intrusions and espionage, can begin to create accountability and perhaps even a form of deterrence against those actors that want to appear legitimate.

The president should use his emergency economic powers to implement a broader strategy for the use of multiple tools to address the reality of major cyberespionage, crime, and infiltration affecting the U.S. financial and commercial system. On April 1, 2015, the president took an important step by signing Executive Order (EO) 13694, based on his power under the International Emergency Economic Powers Act (IEEPA), that allows the Secretary of the Treasury, in coordination with the Secretary of State and the Attorney General, to identify and isolate from the U.S. financial system those who are engaged in "significant malicious cyber-

enabled activities" outside the United States. This EO allows for the blocking of assets and property of those engaged in activities "that are reasonably likely to result in, or have materially contributed to, a significant threat to the national security, foreign policy, or economic health or financial stability of the United States" and are intended, among other things, to affect or disrupt substantially critical infrastructure, systems, or cause misappropriation of financial information, trade secrets, and economic resources. This includes the targeting of those responsible for the receipt or use of any such misappropriated resources for commercial or competitive advantage.

With this new executive order, the U.S. government has created a cyber-financial battlespace to identify and financially isolate potential targets, including the full spectrum of actors that may be involved in significant cyber intrusions. Though hackers and those responsible for cyber-intrusions are the most obvious targets, potentially the deepest impact will be on the behavior of state actors like China, as well as state-owned enterprises seeking access to American markets and Western commercial legitimacy, and corporations that may seek to leverage stolen intellectual property for commercial advantage. All those actors, including everything they own and control, and any entity or person that may support financially or benefit intentionally from such cyber activities, may be targeted and put at risk under this EO, with the potential that significant economic players will be isolated from the U.S. financial and economic system.

The U.S. government can now use the tools of economic and financial isolation—including freezing assets and blocking transactions—against those companies, entities, networks, and individuals identified as being behind major cyber infiltrations, disruptions, and espionage. As with Executive Order 13224, which formed the cornerstone of the counter-terrorist financing campaign after 9/11, EO 13694 has the potential to drive a new strategy and innovations that leverage the convergence of cyber and financial warfare.

In addition, as with the provisions of Section 311 of the USA PATRIOT Act regarding "primary money laundering concerns," Congress could amplify the effects of this new EO and craft legislation to empower the Secretary of the Treasury to identify jurisdictions, institutions, or networks that are sponsoring or willfully allowing their territory or systems to be used to attack American financial institutions. The label of "primary cybersecurity concern" could be applied to any such actor and could bring with it a range of consequences and potential countermeasures against a jurisdiction's economy, including measures to sanction or bar from any business in the United States those companies or entities found to be benefiting or profiting from cyberespionage.

Congress could further empower the private sector—creating a twenty-first century cyber privateering regime that rewards, enables, and empowers it to defend itself in concert with government. This would require rule-setting, more active collaboration, and explicit line drawing and processes, but such a regime is imaginable. This model could be based on the tradition of congressional issuance of "letters of marque and reprisal," as provided for explicitly in Article 1, Section 8 of the U.S. Constitution. Governments provided these letters to private merchant ships, granting them the authority and monetary incentive to attack and capture enemy vessels and bring the cases before admiralty courts. In the age of piracy and maritime insecurity, this was a legitimate method of providing maritime security in the early days of the Republic.

This approach was proposed in part by Professor Jeremy Rabkin of the George Mason School of Law and his son, Ariel Rabkin in the *Chicago Journal of International Law* in Summer 2013. The Rabkins argue that approaching cyber conflict in the context of armed conflict is misguided; rather, they write, "cyber conflict should be open—as naval war has been—to hostile measures short of war, to attacks on enemy commerce, to contributions from private

auxiliaries."[78] Adopting this model would also force the U.S. government to resolve lingering questions of authority and responsibility within the government for assisting or acting in concert with the private sector.

This "privateering" model could take different forms. In June, Irving Lachow and Evan Wolff proposed a future scenario in which a cadre of "cyber cops" could take action against hackers on behalf of private individuals and small business—those who would lack the resources to address cybercrime on their own.[79] This could include a reward program for those groups able to uncover, identify, and even "deliver" cyber hackers to U.S. courts or authorities, as security groups have done in the past. Eric Rosenbach, the recently confirmed Assistant Secretary of Defense for Homeland Defense and Global Security, mentioned at an October 2, 2014, event at the Center for Strategic and International Studies that the capabilities of the government to track and identify organizations and individuals responsible for cyberattacks against the U.S. have never been greater. Rosenbach claimed that the capability for "attribution" —the technical wherewithal to accurately name and shame those who threaten us—are a key component of our cyber deterrence strategy. [80]

The capability to track and identify hackers exists in the private sector, as demonstrated by Mandiant's ability to identify the specific PLA office behind certain attacks against Western companies and the Information Warfare Monitor's ability to track Chinese-based infiltration of dozens of computers systems throughout the world, including the Dalai Lama's computers in India.[81] The "attribution revolution" in the private sector—with better cyber forensic technology to identify the source of cyberattacks—opens up the possibility of more aggressive tracking, detection, and targeting.

Groups pursuing these techniques already exist. Companies like CrowdStrike—staffed by former FBI cyber officials including Shawn Henry and Steve Chabinsky—provide services to help governments and companies protect themselves through attribution and active defense. By identifying zero-day vulnerabilities and quickly locating the origin of threats, CrowdStrike and other companies like it accomplish two tasks at once, both decapitating the existing threat and creating an environment that may deter others from joining in the first place. On October 28th, 2014, *Bloomberg* reported that a coalition of several technology companies—led by Novetta and including Microsoft, Cisco, Symantec, and FireEye—had joined in disrupting a hacking campaign originating with Chinese intelligence.[82] Dubbed by those involved as a "first-of-its-kind effort," the efficacy of the private sector effort demonstrated its reach and the potential for future coordination on cyber threats within its own ranks and with government.

New legal actions and authorities that unleash the power of cyber forensic teams, private litigants, and plaintiff's lawyers against those attacking U.S. systems should be considered as well. *Qui tam* actions that allow private litigants to benefit from the identification of prosecutions should be designed to reward those building cases against cyber hackers and state sponsors. This would incentivize further those able to attribute attacks and would deputize the private sector and lawyers to investigate significant cases.

Victims of attacks should be given the right to sue the perpetrators and those benefitting directly from any cyber infiltrations, just as victims of terrorism have the right to sue terrorists, state sponsors, and terrorist financiers and facilitators. Thus, shareholders and companies would have the right to sue those who have perpetrated, sponsored, or benefited directly and knowingly from cyberattacks. This would have the benefit of unleashing the power of the plaintiff's bar, focusing less attention on those victimized by the breaches and more, instead, on those sponsoring or benefiting from the attacks.

Greater attribution and awareness of attacks could also lead to foreign litigation, World Trade Organization-related suits, and other forms of trade, intellectual property, and fraud

causes of action in foreign and international courts. All of this would be in furtherance of allowing companies and those affected by cyberattacks the ability to use the court system and judgments to defend themselves.

Moreover, the Departments of Justice, Homeland Security, and the Treasury could create and issue special cyber warrants—another type of "letter of marque and reprisal"—to allow U.S. private sector actors to track and even "hack back" or disrupt cyberattacks in certain instances to defend their systems. This would require a real-time capability to respond to targets of opportunity and evaluation of the negative externalities of any such action, especially those that affected friendly states or systems. The issuance of the warrants by the government would allow for legal, diplomatic, and systemic considerations before any preemptive or counter-attacks were approved.

The government today is in a position to enable the private sector—and even private individuals—to pursue economic warfare on its behalf vis-à-vis a new model of cyber-privateering. Individuals would be given the resources necessary to bring suits against those who threaten their assets abroad and domestically. The burden of financial integrity would move from top-down federal control to a democratized, flattened system to match the more distributed and amorphous cyber threat environment.

The U.S. government has been growing more comfortable enabling hackers working with private industry—known as "cyber privateers"—to identify weaknesses in existing cybersecurity and build it back stronger. According to an October 2014 article from the *Financial Times*, banks say that regulators—such as the Bank of England and the Federal Reserve—have been pushing them to identify threats and testing their cyber resilience with a program of "ethical hacking" with events like "Def Con," known as "the Olympics of Hacking," where computer hackers gather annually to compete, share their knowledge, and meet like-minded hackers.[83] The Securities Industry and Financial Markets Association (SIFMA) has been trying to foster better collaboration between the government and industry for some time, organizing simulated cyberattacks dubbed "Quantum Dawn" that involve authorities, regulators, and banks.[84] Harnessing the dynamism of the private sector for purposes of cyber information sharing could provide just the lift stagnant Washington lawmakers need.

The idea of coopting hackers and enlisting them has taken hold in the private sector. When 17 year-old George Hotz became the world's first hacker to crack AT&T's lock on the iPhone in 2007, the company ignored him while it scrambled to fix the bugs his work exposed. He later reverse-engineered Sony Playstation 3, and Sony summarily sued him, settling only after he agreed never to hack a Sony product again. By contrast, earlier this year, after Hotz dismantled the defenses of Google Chrome's operating system, the company paid him a $150,000 reward for helping fix the flaws he had uncovered. Two months later, Chris Evans, a Google security engineer, followed up via email with Hotz, making him an offer to join Google's elite team of full-time hackers paid to hunt security vulnerabilities in software across the internet.[85]

Indeed, the United States and other governments around the world have grown more comfortable with enlisting the private sector in the security space, employing hundreds of thousands of private contractors to provide a range of defense and security-related services over the past two decades. Former NSA general counsel Stewart Baker—an advocate for limited "hacking back"—believes that government officials today are far likelier to enable companies burdened by cyberattacks than they are to prosecute them for considering actively defending themselves against adversaries.[86] Cyber experts are considering implementing a warning mechanism called a "beacon" that could be attached to stolen data, allowing sleuths to determine the origins of an attack.[87] In the cybersecurity context, there should be consideration

for a new framework that allows for private actors to take on more of their own defense, within bounds and with clears lines of authority and responsibility.

This approach would need to be matched by new international arrangements and alliances that set standards of international conduct, established principles of state control and responsibility, and allowed for closer collaboration to address problems of attack attribution and response coordination. The United States has attempted to spur international cooperation in the cyber domain and discussions of limits on the use of cyber weapons, including reported briefings to Chinese government officials regarding U.S. capabilities and willingness to restrain U.S. cyber activities. But these efforts have not been reciprocated and the international system remains bereft of broader international standards and processes, especially in the cyber financial context.

International efforts could build on Estonia's Cyber-Defense League, intended to build multi-lateral and private sector capabilities to detect and react to cyberattacks. This could be replicated more broadly in a new NATO mission, especially given concerns over repeated use of cyber tools and attacks by Russian actors. Bilateral and multilateral working groups or investigations—combining key private sector actors and cyber forensic experts—could coordinate responses to sophisticated infiltrations and attacks, assuming the idea of broader cooperation and coordination among trusted actors *ab initio*. Interpol could have a role in an international effort, perhaps by creating a new "silver notice" for international attention and action against cyber criminals and sponsors.

Even the United States and China could try to collaborate on specific investigations of attacks that affect both their financial systems. By starting with a particular investigation affecting both countries, the United States could test whether the Chinese could be enlisted to address systemic concerns about attacks on the international financial system, which they rely on as much as the United States does.

More broadly, a new collection of relevant state and private actors could be assembled to help establish international cyber norms—in particular to address questions of attribution and response. This could allow for the establishment of norms around the use of cyber warrants by the private sector and development of laws and strictures to address cyber hacking, espionage, and crimes without squelching innovation.

The Financial Action Task Force (FATF), the international body comprised of 36 jurisdictions that set international standards on anti-money laundering, countering the financing of terrorism, and proliferation financing, would serve as an excellent model of a successful collaborative international effort. The FATF, along with regional-style FATF bodies, elaborate these standards and practices and, along with the IMF and World Bank, assess countries on their implementation and effectiveness. The FATF also provides a forum to address new issues—like the emergence of digital currencies—and to engage the private sector directly.

Underlying the international development of norms, there needs to be recognition that the Internet and the cyber domain require careful tending. The cyber domain can be and is misused by nefarious actors, and the trust and legitimacy of this world can be quickly undermined and broken if the attacks increase in severity and disrupt key national systems.

In addition, this new framework might allow for doctrinal innovation in the cyber field—to include exploring new forms of a cyber deterrence strategy that take lessons from financial warfare deterrence models. In the context of a cyber arms race, there may ultimately be no way to match the cyber intrusive efforts of multiple, sophisticated actors, especially those collaborating or enabled by state sponsors. The "attribution revolution" has afforded both

government and private sector cyber sleuths unprecedented means to identify cyberattack aggressors, but since these actors fear no retaliation, they are unlikely to change their behavior.

By using proxies for plausible deniability, nation-states are increasingly emboldened to go after symbols of economic prosperity. North Korea's November 24, 2014 attack on Sony Pictures Entertainment demonstrated that a cyber event need not disrupt key national security systems to prove strategically relevant or elicit an official U.S. government response. But lack of clarity about what sort of "retaliation" the U.S. might have planned for a country with little technological infrastructure and already burdened by economic sanctions may do little to deter other state or non-state actors from launching similar attacks.

Expanding the field of actors who might be targeted for economic sanctions, legal censure, international opprobrium, or even cyber retaliation or attacks, may help develop a new form of deterrence affecting not just the hackers, but the entire spectrum of individuals and entities who support, finance, or benefit from cyberattacks. This may also begin to force "responsible" state actors to curb their cyber hacking activity to avoid damaging attacks on their own systems and unwanted scrutiny in a variety of fora and from a range of non-state or private actors. A doctrine of cyber deterrence may emerge in the context of the cyber-privateering model delineated above.

Unlike in the financial context, where the U.S. Treasury and government worry about the "magnificent glass house" of the international financial system, there is little coordination and consideration of the systemic risks to the global cyber and digital domains. Other actors in the domain—including the Chinese, Russian, and Iranian governments—have demonstrated little concern at this stage for managing the health or sustainability of either the financial or cyber systems. Yet, these actors do rely on these systems for their economic well-being and are more and more entangled in the global, commercial, and cyber systems that allow their economies and countries to function. As these actors begin to predominate in cyberspace and perhaps sponsor or direct attacks against key international financial actors, there needs to be a broader policy and wider international debate about how the key states and private sector actors protect the integrity of both the financial and cyber systems. Indeed, there may be new models of both deterrence and international cooperation that emerge among the responsible state actors that rely most heavily on the uninterrupted functioning of the cyber and financial systems.

A new model of collective and local cyber defense may be necessary to address the increasing threats and risks, especially to the financial community. Banks now sit at the heart of the cyber storm—targeted by all actors in cyberspace. They are looking for more support from government and more freedom to collaborate within their sector. Given the current legal and policy constructs, these measures are likely to be reactive and represent marginal improvements to the current system.

Without a more revolutionary approach to public-private collaboration and cyber defense, the financial community will remain at risk. The banks will spend hundreds of millions to strengthen and defend key systems, while sophisticated actors, including nation states, will up the ante in the cyber arms race. In so doing, the underpinnings of the financial system will remain at risk. Now is the time to address the convergence of cyber and financial warfare before a systemic breakdown and disaster occur. In so doing, we may create a new and more enduring model for ensuring global cybersecurity.

1 The author thanks Daniel Paltiel from the Center for Strategic and International Studies for his dedicated research and assistance in preparing this paper.

2 Kara Scannell and Tom Braithwaite, "Fidelity Hack Points to JPMorgan Link," *Financial Times*, October 9, 2014, http://www.ft.com/intl/cms/s/0/2564f64e-4f2e-11e4-9c88-00144feab7de.html#axzz3GJX0s0Ma.

3 Emily Glazer And Danny Yadron, "J.P. Morgan Says About 76 Million Households Affected By Cyber Breach," *Wall Street Journal*, October 3, 2014, sec. Markets, http://online.wsj.com/articles/j-p-morgan-says-about-76-million-households-affected-by-cyber-breach-1412283372.

4 In a *Financial Times* interviews, Frank Abagnale — inspiration for *Catch Me If You Can* and anti-fraud specialist — is dubious that the hackers would not have taken additional data. "The Benefits of Being a Real Fraudster," *Financial Times*, October 9, 2014, http://www.ft.com/intl/cms/s/2/1e7ad07c-4ae4-11e4-839a-00144feab7de.html#axzz3GJX0s0Ma.

5 "Obama Had Security Fears on JPMorgan Data Breach," *DealBook*, accessed October 16, 2014, http://dealbook.nytimes.com/2014/10/08/cyberattack-on-jpmorgan-raises-alarms-at-white-house-and-on-wall-street/.

6 Joel Brenner, "Nations Everywhere Are Exploiting the Lack of Cybersecurity," *The Washington Post*, October 24, 2014, http://www.washingtonpost.com/opinions/joel-brenner-nations-everywhere-are-exploiting-the-lack-of-cybersecurity/2014/10/24/1e6e4b70-5b85-11e4-b812-38518ae74c67_story.html.

7 "Finextra: MasterCard Unveils Tool to Tackle Cyber Threat," accessed January 30, 2015, http://ww.finextra.com/news/fullstory.aspx?newsitemid=26532&topic=sibos.

8 Charles Blauner, Global Head of Information Security for Citi Bank and the Chair of the Financial Services Sector Coordinating Council, "The cyber wars escalate," SIBOS Conference, Boston, MA, September 30, 2014.

9 Barry Vengerik et al., *FireEye, Inc. | Hacking the Street? FIN4 Likely Playing the Market* (FireEye, 2014), https://www2.fireeye.com/fin4.html.

10 Mike Rogers, "Stopping the Next Cyberassault," *Wall Street Journal*, December 25, 2014, sec. Opinion, http://www.wsj.com/articles/mike-rogers-stopping-the-next-cyberassault-1419543945.

11 Juan Zarate, *Treasury's War: The Unleashing of a New Era of Financial Warfare* (Public Affairs, 2013).

12 Ibid.

13 Kara Scannell, "NY Bank Regulator Targets Cyber Threat," *Financial Times*, October 6, 2014, http://www.ft.com/intl/cms/s/0/5a981338-4cdf-11e4-a0d7-00144feab7de.html#axzz3GJX0s0Ma.

14 "WikiLeaks And Cyber War," accessed October 16, 2014, http://www.smh.com.au/federal-politics/political-opinion/its-time-to-get-serious-about-cyber-attack-risk-20101228-1998p.html.

15 David E. Sanger and Eric Schmitt, "Cyberattacks Are Up, National Security Chief Says," *The New York Times*, July 26, 2012, sec. U.S., http://www.nytimes.com/2012/07/27/us/cyberattacks-are-up-national-security-chief-says.html.

16 "2014 McAffee Report on the Global Cost of Cybercrime | Center for Strategic and International Studies," accessed September 20, 2014, http://csis.org/event/2014-mcafee-report-global-cost-cybercrime.

[17] Ellen Nakashima and Ashkan Soltani, "FBI Warns Industry of Chinese Cyber Campaign," *The Washington Post*, October 15, 2014, http://www.washingtonpost.com/world/national-security/fbi-warns-industry-of-chinese-cyber-campaign/2014/10/15/0349a00a-54b0-11e4-ba4b-f6333e2c0453_story.html.

[18] Ibid.

[19] "Double-edged Sword: Australia Economic Partnerships Under Attack from China," *FireEye Blog*, accessed October 28, 2014, http://www.fireeye.com/blog/technical/2014/10/double-edged-sword-australia.html.

[20] James Andrew Lewis, "The Key to Keeping Cyberspace Safe? An International Accord," *The Washington Post*, October 7, 2014, http://www.washingtonpost.com/postlive/key-to-keeping-cyberspace-safe-international-accord/2014/10/07/ae50a35e-4812-11e4-b72e-d60a9229cc10_story.html.

[21] "Hashcat's GPU-accelerated Gauss Encryption Cracker – Securelist," accessed January 30, 2015, http://securelist.com/blog/events/34884/hashcats-gpu-accelerated-gauss-encryption-cracker-4/.

[22] Kim Zetter, "Researchers Seek Help Cracking Gauss Mystery Payload," *WIRED*, August 14, 2012, http://www.wired.com/2012/08/gauss-mystery-payload/.

[23] Katherine Maher, "Did the Bounds of Cyber War Just Expand to Banks and Neutral States?," *The Atlantic*, August 17, 2012, http://www.theatlantic.com/international/archive/2012/08/did-the-bounds-of-cyber-war-just-expand-to-banks-and-neutral-states/261230/.

[24] "The Terror Finance Blog: Is the New 'Gauss' Malware a Counter-terror Finance Intelligence Tool?," accessed October 17, 2014, http://www.terrorfinance.org/the_terror_finance_blog/2012/08/is-the-new-gauss-malware-a-counter-terror-finance-intelligence-tool.html.

[25] Chris on January 2 and 2013 in Uncategorized, "Deconstructing the Al-Qassam Cyber Fighters Assault on U.S. Banks," *Recorded Future*, accessed October 28, 2014, https://www.recordedfuture.com/deconstructing-the-al-qassam-cyber-fighters-assault-on-us-banks/.

[26] E. Scott Reckard, "Banks Fail to Repel Cyber Threat," *Los Angeles Times*, September 27, 2012, http://articles.latimes.com/2012/sep/27/business/la-fi-bank-attacks-20120927.

[27] Harald Malmgren and Mark Stys, *Computerized Global Trading 24/6: a Roller Coaster Ride Ahead?: An Article from: The International Economy*, n.d.

[28] "The Real Story of Trading Software Espionage," *Wall Street & Technology*, accessed October 17, 2014, http://www.wallstreetandtech.com/trading-technology/the-real-story-of-trading-software-espio/218401501.

[29] "Staff Report on May 6 Market Events - CFTC," FragLibs, accessed October 17, 2014, http://www.cftc.gov/marketreports/staffreportonmay6marketevents/index.htm.

[30] "2.2 Global Risks Arising from the Accelerated Interplay Between Geopolitics and Economics," Global Risks 2015, accessed January 30, 2015, http://reports.weforum.org/global-risks-2015/part-2-risks-in-focus/2-2-global-risks-arising-from-the-accelerated-interplay-between-geopolitics-and-economics/.

[31] Martin Arnold, "Banks Face Rising Threat from Cybercrime," *Financial Times*, accessed October 6, 2014, http://www.ft.com/intl/cms/s/0/5fd20f60-4d67-11e4-8f75-00144feab7de.html#axzz3FOFcGxgh.

[32] "2014 McAffee Report on the Global Cost of Cybercrime | Center for Strategic and International Studies."

[33] "Press Release - May 06, 2014: Governor Cuomo Announces New Cyber Security Assessments For Banks," accessed October 28, 2014, http://www.dfs.ny.gov/about/press2014/pr1405061.htm.

[34] Michael Riley, "How Russian Hackers Stole the Nasdaq," *BusinessWeek: Technology*, July 17, 2014, http://www.businessweek.com/articles/2014-07-17/how-russian-hackers-stole-the-nasdaq.

[35] "Mandiant," *Mandiant*, accessed October 28, 2014, http://www.mandiant.com.

[36] "U.S. and China Accuse Each Other of Cyber Warfare," accessed October 20, 2014, http://rt.com/usa/cyber-china-war-unit-604/.

[37] Nicole Perlroth and David Gelles, "Russian Hackers Amass Over a Billion Internet Passwords," *The New York Times*, August 5, 2014, http://www.nytimes.com/2014/08/06/technology/russian-gang-said-to-amass-more-than-a-billion-stolen-internet-credentials.html.

[38] "The State of Financial Trojans in 2013," *Symantec Security Response*, accessed July 24, 2014, http://www.symantec.com/connect/blogs/state-financial-trojans-2013.

[39] Ibid.

[40] "Security Response Publications, Internet Security Threat Report | Symantec," accessed October 20, 2014, http://www.symantec.com/security_response/publications/threatreport.jsp.

[41] Ibid.

[42] "2013 Norton Report | Symantec," accessed October 20, 2014, http://www.symantec.com/about/news/resources/press_kits/detail.jsp?pkid=norton-report-2013.

[43] "Silk Road 2.0 Hit by 'Sophisticated' DDoS Attack," *CoinDesk*, accessed September 19, 2014, http://www.coindesk.com/silk-road-2-0-shrugs-sophisticated-ddos-attack/.

[44] Ibid.

[45] "FBI Investigating Russian Cyberattacks on U.S. Banks," *The Feed*, accessed October 20, 2014, http://www.the-american-interest.com/blog/2014/08/28/fbi-investigating-russian-cyber-attacks-on-us-banks/.

[46] "The State of Financial Trojans in 2013."

[47] Christian Lowe, "Kremlin Loyalist Says Launched Estonia Cyber-attack," *Reuters*, March 12, 2009, http://www.reuters.com/article/2009/03/12/us-russia-estonia-cyberspace-idUSTRE52B4D820090312.

[48] Sam Jones, Defence, and Security Editor, "Ukraine PM's Office Hit by Cyberattack Linked to Russia," *Financial Times*, August 7, 2014, http://www.ft.com/intl/cms/s/0/2352681e-1e55-11e4-9513-00144feabdc0.html#axzz3DtMfpRac.

[49] "FBI Investigating Russian Cyberattacks on U.S. Banks."

[50] Ibid.

[51] "Defending the Digital Frontier," *The Economist*, July 12, 2014, http://www.economist.com/news/special-report/21606416-companies-markets-and-countries-are-increasingly-under-attack-cyber-criminals.

[52] "Global Economic Crime 2014 Survey," *PwC*, accessed October 20, 2014, http://www.pwc.com/gx/en/economic-crime-survey/index.jhtml.

[53] Ibid.

[54] "Cybersecurity Business Cyberwarfare Critical Infrastructure | Homeland Security News Wire," accessed October 28, 2014, http://www.homelandsecuritynewswire.com/dr20140905-retailers-spend-less-on-cybersecurity-than-other-industries-and-it-shows.

[55] "Retail Spends Less on Cybersecurity Than Banking, Healthcare - The CIO Report - WSJ," accessed October 20, 2014, http://mobile.blogs.wsj.com/cio/2014/09/02/retail-spends-less-on-cybersecurity-than-banking-healthcare/.

[56] Danny Yadron, "Companies Wrestle With the Cost of Cybersecurity," *Wall Street Journal*, February 26, 2014, sec. Tech, http://online.wsj.com/articles/SB10001424052702304834704579403421539734550.

[57] "Global Economic Crime 2014 Survey."

[58] Yadron, "Companies Wrestle With the Cost of Cybersecurity."

[59] "JPMorgan's Dimon: There Will Be Wins, Losses in Cyber Security War," accessed October 28, 2014, http://fortune.com/2014/10/17/jpmorgan-jamie-dimon-data-breach/.

[60] Hannah Kuchler, "U.S. Financial Industry Launches Platform to Thwart Cyberattacks," *Financial Times*, September 24, 2014, http://www.ft.com/intl/cms/s/0/080092b2-437a-11e4-8a43-00144feabdc0.html?siteedition=intl#axzz3FOFcGxgh.

[61] "Taking Down Botnets," *FBI*, accessed October 28, 2014, http://www.fbi.gov/news/testimony/taking-down-botnets.

[62] Chloe Albanesius June 6 and 2013 09:55am EST 11 Comments, "Microsoft, FBI Take Down 'Citadel' Botnet Targeting Bank Info," *PCMAG*, accessed October 28, 2014, http://www.pcmag.com/article2/0%2c2817%2c2420046%2c00.asp.

[63] Richard Domingues Boscovich, "Microsoft Partners with Financial Services Industry on Fight Against Cybercrime," *Microsoft on the Issues*, accessed October 28, 2014, http://blogs.microsoft.com/on-the-issues/2014/09/29/microsoft-partners-financial-services-industry-fight-cybercrime/.

[64] Kuchler, "U.S. Financial Industry Launches Platform to Thwart Cyberattacks."

[65] DTCC press release, September 24, 2014, accessed October 28, 2014, http://www.dtcc.com/news/2014/september/24/fs-isac-and-dtcc-announce-soltra.aspx.

[66] Lily Hay Newman, "In State of the Union, Obama Promotes Cybersecurity Measures," *Slate,* January 20, 2015, http://www.slate.com/blogs/ruture_tense/2015/01/20/in_state_of_the_union_obama_promotes_cybersecurity_measures_especially_to.html.

[67] "Tomorrow's Workforce: How Can America Remain Competitive?," accessed October 28, 2014, http://www.wilsoncenter.org/event/tomorrow%E2%80%99s-workforce-how-can-america-remain-competitive.

[68] "About | The Global Cyber Security Capacity Centre | Programmes," *Oxford Martin School*, accessed October 28, 2014, http://www.oxfordmartin.ox.ac.uk/research/programmes/cybersecurity/.

[69] "Banks Team up with Government to Combat Cyber Criminals and Fraudsters | BBA," accessed October 28, 2014, https://www.bba.org.uk/news/press-releases/banks-team-up-with-government-to-combat-cyber-criminals-and-fraudsters/#.VE-nx_nF8uc.

[70] Martin Arnold and Banking Editor, "Banks Launch Fresh Drive Against Cybercrime," *Financial Times*, September 23, 2014, http://www.ft.com/intl/cms/s/0/15630060-433f-11e4-be3f-00144feabdc0.html#axzz3EF608RSt.

[71] Ibid.

[72] Dakin Campbell and Michael J. Moore, "Cyberattacks Require Coordinated Defense, Executives Say," *Bloomberg*, October 11, 2014, http://www.bloomberg.com/news/2014-10-11/cyber-attacks-require-coordinated-defense-executives-say.html.

[73] Ben Goad, "Regulators urge banks to share cyber threat info," Text, *TheHill*, (November 3, 2014), http://thehill.com/policy/cybersecurity/222730-regulators-urge-banks-to-share-cyber-threat-info.

[74] Jordan Robertson, "It's the Government's Job to Respond to Cyberattacks: Bloomberg Poll," Bloomberg.com, accessed January 30, 2015, http://www.bloomberg.com/news/articles/2015-01-21/cyber-attack-retaliation-seen-as-government-s-job-in-global-poll.

[75] Shane Harris, "Google's Secret NSA Alliance: The Terrifying Deals Between Silicon Valley and the Security State," accessed January 30, 2015, http://www.salon.com/2014/11/16/googles_secret_nsa_alliance_the_terrifying_deals_between_silicon_valley_and_the_security_state/.

[76] Ellen Nakashima, "Banks Seek NSA Help Amid Attacks on Their Computer Systems," *The Washington Post*, January 10, 2013, http://www.washingtonpost.com/world/national-security/banks-seek-nsa-help-amid-attacks-on-their-computer-systems/2013/01/10/4aebc1e2-5b31-11e2-beee-6e38f5215402_story.html.

[77] July 24 and 2014, "Wall Street Confronts Cyber Threats," *Markets Media*, accessed November 11, 2014, http://marketsmedia.com/wall-street-faces-cyber-threats/.

[78] Jeremy Rabkin and Ariel Rabkin, *Navigating Conflicts in Cyberspace: Legal Lessons from the History of War at Sea*, SSRN Scholarly Paper (Rochester, NY: Social Science Research Network, September 15, 2014), http://papers.ssrn.com/abstract=2496625.

[79] Thomas E. Ricks, "When Your Computer Gets Hacked, Why Can't You Call the Police to Deal with It?," *Foreign Policy Blogs*, June 26, 2014, http://ricks.foreignpolicy.com/posts/2014/06/26/when_your_computer_gets_hacked_why_cant_you_call_the_police_to_deal_with_it.

[80] "Cyber Leaders: A Discussion with the Honorable Eric Rosenbach | Center for Strategic and International Studies," accessed October 28, 2014, http://csis.org/event/cyber-leaders.

[81] Tania Branigan, "Cyber-spies Based in China Target Indian Government and Dalai Lama," *The Guardian*, April 6, 2010, sec. Technology, http://www.theguardian.com/technology/2010/apr/06/cyber-spies-china-target-india.

[82] Chris Strohm and Michael Riley, "China-Linked Hacking Foiled by Private-Sector Sleuthing," *Bloomberg*, October 28, 2014, http://www.bloomberg.com/news/2014-10-28/china-linked-hacking-foiled-by-private-sector-sleuthing.html.

[83] Hannah Kuchler, "Def Con: The 'Olympics of Hacking'," *Financial Times*, August 15, 2014, http://www.ft.com/intl/cms/s/2/e7243fec-22e2-11e4-9dc4-00144feabdc0.html#axzz3FOFcGxgh.

[84] "Cybersecurity Exercise: Quantum Dawn 2 | BCP | Services," accessed October 28, 2014, http://www.sifma.org/services/bcp/cybersecurity-exercise--quantum-dawn-2/.

[85] ! Subscribe to our RSS Feed, "Famous iPhone Jailbreaker Geohot Is Now Working At Google As A Project Zero Hacker," *Redmond Pie*, accessed October 28, 2014, http://www.redmondpie.com/famous-iphone-jailbreaker-geohot-is-now-working-at-google-as-a-project-zero-hacker/.

[86] Craig Timberg, Ellen Nakashima and Danielle Douglas-Gabriel, "Cyberattacks Trigger Talk of 'hacking Back'," *The Washington Post*, October 9, 2014, http://www.washingtonpost.com/business/technology/cyberattacks-trigger-talk-of-hacking-back/2014/10/09/6f0b7a24-4f02-11e4-8c24-487e92bc997b_story.html.

[87] Ibid.

CHAPTER 5

Threats to Critical Infrastructure and the Transportation Sector

By Tiffany Rad

Introduction

Twenty years ago, industrial facilities implemented a technology that reduced the need for copper wires to be connected between each door, switch or contact point with a sensor by aggregating a multitude of wires into a single device – a logic controller – which would, in turn, send only a few wires to a control center. By reducing the wires, costs were reduced and connections between points became easier to manage. With the advent of information technology (IT) advances in the past couple of decades, the old networks and logic controllers became "smart." Internet access was later added, and because necessary changes could be made remotely, convenience, reduced costs, ease of monitoring and added safety benefits resulted. Just as wired networks matured into wireless networks, logic controllers evolved into programmable logic controllers (PLCs).

IT changes have added convenience and cost-savings to industrial systems but also increased security risks. A few decades ago, before it was conceived how advanced and aggressive computer hackers would become, control system engineers had one top priority: to "make it work." With the addition of Internet access to control systems, it soon became apparent that security needed to be added and/or enhanced.

When control systems were connected to the Internet, there were added benefits such as being able to update software with newer and more secure patched versions of software and firmware. Also, remote access added another level of convenience and the ability to make corrections or changes to the control systems quickly without the need for any people on-site. But these improvements also produced increased access and exposure.

Theoretically these vulnerabilities were recognized many years ago, but accidental revelations regarding the first known digital weapon, Stuxnet, brought much more scrutiny to them beginning in mid-2010.[1] Adversaries of the United States began testing access to the country's critical infrastructure. Cyber-enabled economic warfare became not just possible, but actual.

The power to access wind-turbines controlling power for a rural town or the water treatment facility in Texas puts small groups of hackers in a position to cause significant damage to the U.S. without using traditional military means such as kinetic weapons.[2] Hackers—both independent and state-sponsored—can metaphorically reach across thousands of miles and

access utilities that our society counts on to function. The financial effects the U.S. would experience after such attacks make the threat of cyber economic warfare real.

It Started with Executive Order 13636

On February 12, 2013, President Obama signed Executive Order 13636, "Improving Critical Infrastructure Cybersecurity," which called for the development of a voluntary set of industry standards for managing cybersecurity threats.[3] In response, for more than a year afterwards government, private sector, and independent security researchers collaborated to create the Cybersecurity Framework.[4, 5] Meeting at locations across the country and online, participants discussed the best procedures and ways in which the threats to our country's infrastructure could be addressed. Partnerships between these sectors were strengthened as a result of these discussions. The group agreed that disseminating "best practices" would be more useful at this time rather than mandatory regulations that included penalties for compliance failures. Some energy sectors, such as nuclear, had had mandatory regulations for years, but for the other critical infrastructure sectors these voluntary guidelines were new.

In addition to addressing threats to the electrical grid and the banking industry, the Framework devotes substantial attention to improving cybersecurity in the transportation sector. A nightmare scenario would be if the nation experienced a coordinated cyber and physical attack on a vital segment of the transportation infrastructure. In such a case, disruption of transportation (e.g. airplanes, trains, and/or automobiles) would generate panic and prevent emergency responders from getting to destinations where their services were needed. In cities such as Washington, D.C. and New York City, which are accessed primarily (or completely) via bridges and tunnels, stopped vehicles could choke-off ingress and egress, thereby forcing responders to walk as their primary means of circumventing jams.

Traffic Management and Control

In 2012, I was asked to do a TV program for The Discovery Channel called "True Story: Live Free or Die Hard."[6] Jim Christy,[7] a former Director of DC3, and I were asked to critique the computer hacking in the movie *Die Hard* and comment on whether it could really happen. In the movie, a former NSA employee is disgruntled with the U.S. government and seeks to wreak havoc and gain financially from what he hopes will be the demise of the U.S. government, and in particular, the Washington, D.C. area. The malicious hacker sets up a mobile hacking command unit in the back of a tractor-trailer truck parked downtown, where his team is able to tap into the communications for emergency services, law enforcement and mass transit. In particular, he threatens to destroy critical infrastructure, such as the electrical grid, that supplies D.C.

The program's producers did not allow Christy and me to communicate about our responses to questions about the technical hacks in the movie prior to filming the segment, but anticipated the "hacker's opinion" (mine) would be at odds with the "Fed's." It was not. Both Christy and I agreed that apart from the gratuitous explosion and combat scenes, the hacks done in the movie were feasible. In particular, I was asked to comment about whether it was possible to turn all of the traffic lights to "green," thus causing accidents and snarling traffic in the city.

There are different kinds of technologies used in traffic lights throughout Washington, D.C. Some use supervisory control and data acquisition (SCADA) and are expensive; these typically are used in areas where remote control of the lights is important for movement of politicians and diplomats, such as around the White House. Other traffic lights rely upon radio signals to change the control when approached by law enforcement and emergency services.

In 2011, my research team was one of the first to show that there are significant vulnerabilities in Industrial Control Systems. With just $2,500 in a lab in our basement, we were able to create a proof-of-concept (POC) exploit that had the capability to take control of ICS/SCADA systems and enable malicious remote control. We bought a Programmable Logic Controller (PLC) and set up a fictitious prison system. Inspired by Stuxnet, we theorized we could introduce a malicious exploit onto the PLC control computer in a prison's system that would allow us to remotely open and close prison doors and without the prison's control room knowing because the "open" doors would appear on the computer as "closed" and vice versa.[8]

This hack would not only work on prison doors. Similar control technology is used in some traffic lights, braking systems for trains, elevators, factory controls, the electrical grid, gas pipelines, HVAC units for buildings, and in the critical air conditioning units in computer data storage centers. The POC exploit code we created for demonstration purposes could be adapted to work in those facilities, too. Following the introduction of Stuxnet to Iran's nuclear facilities, the United States knew that the same ICS/PLCs were also in nuclear enrichment facilities. My team discovered many critical vulnerabilities when we did the research in 2011 and presented our findings to the U.S. government to show that ICS threats went beyond nuclear facilities.

So when asked by Discovery if a similar hack could be done to control the ICS traffic lights, the answer was, "Yes." As for the radio frequency lights, the answer was provided in 2014 with Cesar Cerrudo's traffic lights hack. With a radio in his backpack and walking around Washington, D.C., he was able to access and potentially control traffic lights. Similar to my research findings with SCADA/ICS systems, Cesar could not only access and control them, but he could destroy them if he wanted. As Adam Greenberg noted: "Traffic control systems used in the U.S. and other countries can be hacked to cause significant traffic problems, or can even be 'bricked' to cause millions of dollars in damages to infrastructure." [9]

Airplanes

Researching vulnerabilities on airplanes is a difficult task for the private sector, especially for independent security researchers. The cost of access to an airplane and the potential harm associated with inadvertently breaking something critical is more of a risk than most researchers want to take. However, there has been some research done regarding cybersecurity for airplanes. While it is known that airplanes use SCADA systems, few reports have been publicly released about the vulnerability of this practice to cyber threats. However, reports about vulnerabilities of communications between the ground and individual airplanes as well as communications among airplanes in-flight have been released.

Ruben Santamarta presented findings at the Black Hat computer security conference in Las Vegas, Nevada in August 2014 that showed that a hacker could use a plane's Wi-Fi signal or inflight entertainment system to hack into the plane's avionics equipment and thereby potentially disrupt and/or alter satellite communications.[10] Additionally, he found that equipment used on the ground to communicate with airplanes had vulnerabilities that:

> … an attacker could use to bypass authorization mechanisms in order to access interfaces," according to the whitepaper, which "…could compromise control of the satellite link channel used by the Future Air Navigation System (FANS), Controller Pilot Data Link Communications (CPDLC) or Aircraft Communications Addressing and Reporting System (ACARS).[11]

The U.S. government is aware of this risk and has established an information sharing program led by the Transportation Security Administration (TSA) in conjunction with the National Intelligence and National Counterterrorism Center. This partnership also includes companies in the private sector such as airplane manufacturers.[12]

Trains

Both freight and passenger trains use remote control technologies that have been shown to have cyber vulnerabilities. Some braking systems on trains use a similar SCADA/ICS technology that in other applications has been proven vulnerable; that research was referenced above. In addition to braking, cyber vulnerabilities also exist for track switching and signaling along railways.

While initial reports from the January 12, 2015, Washington DC Metro incident show no signs of mal-intent for the start of the fire, there had been issues with radio communications that complicated the effort to rescue 200 people trapped in a smoke-filled Metro train near L'Enfant Plaza.[13] The Metro's Silver Line has SCADA systems that include remote indication and control of traction power substations, the tiebreaker system, AC control, ventilation and other systems including for remote control.[14, 15] These examples show that there are cyber risks in DC's public transit system.

There has not been a confirmed public train hacking incident in the U.S. and one incident that was initially flagged in a TSA memo as malicious hacking of trains, was later reclassified as inconclusive.[16] Nevertheless, the transportation sector is aware of risks to both freight and passenger trains, especially those with SCADA systems. Consequently various parties are establishing educational programs for operators so that they can guard against unauthorized access into train control centers. These programs also aim to make operators aware of the importance of adhering to computer usage policies to minimize the risk of accidental malware infections on control computers.

Some other countries have experienced malicious train hacking. In Poland, a teenager turned public transit trams into his own private train set by taking control of them. He discovered the radio frequency used to switch rails for the city trams and converted a television control device into a hand-held remote allowing him to switch the trains on the rails. Four trams de-railed and injured 12 people.[17]

While not an attack directed at trains, in 2003 the "Sobig" virus that spread via email impacted train signaling systems at CSX Corporation which manages a large number of trains across the eastern U.S. Signaling, dispatching and other related systems at CSX were affected, causing a 2-hour signal outage that resulted in delays for both freight and commuter trains.[18]

The National Academies of Science in conjunction with the Transportation Research Board has established the *Protection of Transportation Infrastructure from Cyber Incidents* project and awarded funding to a contractor to create and deliver formal educational programs for both decision makers (C-levels) and transportation operators to make them aware of cyber risks that are unique to the transportation sector.[19] Rail safety and security was a significant part of that program as was an emphasis on SCADA security. This is an excellent example of the U.S. government and the private sector working together and sharing important vulnerability information along with recommendations for improvement.

Passenger Cars

External access to automobile computers has been going on for more than a decade. The first car hacking presentation was given at Defcon 12 in 2004 with the *Open Otto Project*.[20] Four years later in 2008, it evolved into the first device allowing consumers to access their cars' networks via the On Board Diagnostic (OBD2) port. A device was planned that would output

speed, engine diagnostics, tire pressure and text messages sent to a car's owner to show the car's location.[21]

In 2010, researchers from the University of Santa Barbara and the University of Washington become the first to demonstrate remote control of vehicles via access to the OBD2 port.[22] Later at Defcon 21 in 2013, Charlie Miller and Chris Valasek[23] gave a presentation about automotive networks and in 2014 they demonstrated that they could take control of a vehicle by connecting to it wirelessly. It is anticipated that at the 2015 security conferences for Black Hat and Defcon, they will show how they can remotely access and control a vehicle via telematics and/or Bluetooth connectivity in vehicles.

How likely is it that car hacking is an imminent threat to the transportation sector? At the time of publication of this report, the threat is low. It takes significant knowledge about both automotive networks and communication protocols (such as cellular, Wi-Fi, radio frequencies, Bluetooth) to find vulnerabilities. Additionally, the messages sent across vehicles' bus networks are not easy to decipher, and apart from diagnostic messages that are federally-mandated for emission control, control messages are challenging to decipher from the hexadecimal raw CAN bus[24] output that is visible via plugging devices into the OBD2 port. These messages can also be different between manufacturer, model and year.

Nevertheless, in recent years, there has been a significant amount of vehicle car computer research that has been done publicly. Numerous hobbyist tools are available in community-funded sites such as Kickstarter[25]; many are open source and released for free by computer hardware engineers.[26]

The availability of the tools and public interest in accessing car computers may arouse concerns and skepticism in some, but this research has actually brought to light many vulnerabilities in safety-critical systems that might otherwise have not been recognized. When videos have been distributed online of security researchers taking control of vehicles both by discretely plugging devices into the On Board Diagnostic (OBD2) port and/or accessing cars remotely and controlling them, manufacturers have taken notice and are making changes to their future vehicle designs.

The SAE committee for Vehicle Electrical System Security begins its bi-monthly meeting by reviewing and discussing recent media articles and security conference presentations about accessing car computers. This committee is composed of members from the U.S. government, automobile manufacturers, and private industry. They discuss the most recent publicly released car computer research and are acutely aware of its results. Sharing this information publicly assists all interested parties; one vendor's vulnerability may be relevant to others. The sooner all parties know about problems, the sooner they all can work – both together and within their own organizations – to make necessary changes and/or patches to fix the vulnerability.

The vehicle manufacturers appreciate responsible disclosure of vulnerabilities that are made to them before the information is disseminated to the public. This allows them time to make patches, issue warnings to the public, or do a recall if the patches cannot be implemented. If no vulnerability research is done or disseminated, there is a chance that no one else will discover a problem making it a non-issue for the vehicle manufacturer. But that is a risky chance to take; if someone discovers a problem and exploits the vulnerability for malicious purpose, the vehicle manufacturer and public safety are at a greater disadvantage than in the responsible disclosure scenario. In this case, there is no time advantage for the manufacturer; they have been "zero dayed."

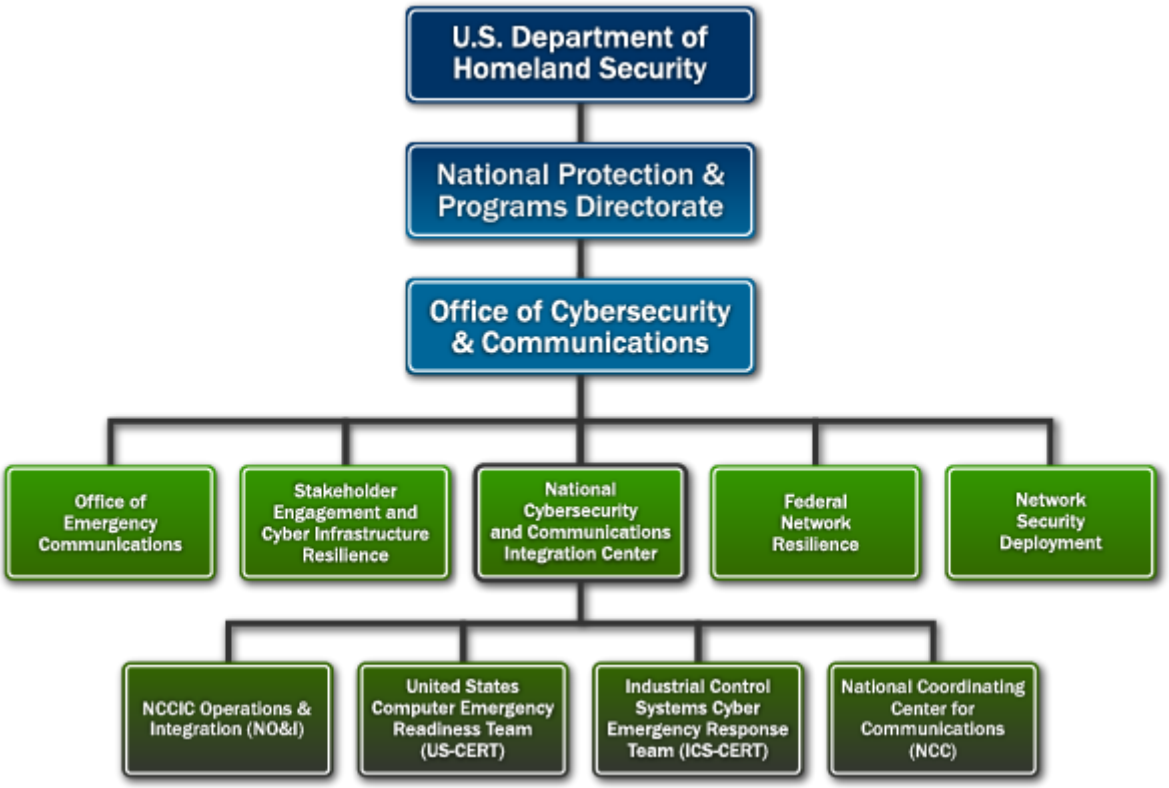
How the U.S. Government Handles These Threats

The U.S. government has organized responsibilities across agencies for the detection, assessment, analysis, and prosecution of malicious hacking. This is a summary of the principal organizations involved and their cyber-related tasks:[27]

> **Department of Homeland Security** (DHS): The DHS's United States Computer Emergency Readiness Team (U.S.-CERT) leads efforts to improve the nation's cybersecurity posture, coordinate cyber information sharing, and proactively manage cyber risks to the Nation.
>
> **National Institute for Standards and Technology** (NIST): The Computer Security Division's (CSD) Computer Security Resource Center (CSRC) facilitates broad sharing of information security tools and practices, provides a resource for information security standards and guidelines, and identifies key security web resources to support users in industry, government, and academia.
>
> **The Federal Bureau of Investigation** (FBI): The FBI's key tasks include investigating computer and network intrusions, identity theft, and operating the Internet Crime Compliant Center for online fraud.
>
> **The Secret Service**: The role of the U.S. Secret Service has gradually evolved since the agency's inception in 1865, from its initial mandate — suppressing the counterfeiting of U.S. currency — to protecting the integrity of the nation's financial payment systems. During this time, as methods of payment have evolved, so has the scope of the Secret Service's mission. Computers and other chip devices are now the facilitators of criminal activity or the target of such, compelling the involvement of the Secret Service in combating cybercrime.
>
> **The National Security Agency** (NSA): The National Security Agency gathers foreign intelligence and helps to defend U.S. government information systems.
>
> **U.S. Strategic Command (Stratcom)—Cyber Command**: CYBERCOM plans, integrates, synchronizes and conducts activities to: direct the operations and defense of specified Department of Defense information networks; and prepare to, and when directed, conduct full spectrum military cyberspace operations in order to enable actions in all domains, ensure U.S./Allied freedom of action in cyberspace, and deny the same to U.S. adversaries.

In 2009, in an effort to combine the intelligence gathering, threat monitoring, and cyber security analysis done by these Agencies, the DHS established the National Cyber Security and Communications Integration Center (NCCIC). It was tasked to create "a 24x7 cyber incident response, situational awareness and management enter."[28] The NCCIC is composed of the U.S.-CERT, ICS-CERT (the industrial control systems group of CERT), and an Operations and Integration Team. Operations are currently conducted from three states: Virginia, Idaho, and Florida.[29]

Exhibit 1



SOURCE: Department of Homeland Security.

According to DHS's National Protection & Programs Directorate chief, Deputy Undersecretary for Cybersecurity and Communications Phyllis Schneck:

> During the first eleven months of 2014, the NCCIC has had 108,734 incidents reported to the center, issued over 11,514 actionable cyber-alerts, and had over 219,805 partners subscribe to our cyber threat warning sharing initiative. NCCIC teams have also detected over 87,797 vulnerabilities and directly aided in the mitigation of near 53,624 unique challenges.[30]

In December 2014, Congress passed, and President Obama signed, the National Cybersecurity Protection Act of 2014 (NCPA). The NCPA codifies the NCCIC and its existing cybersecurity responsibilities at DHS. The new law directs the NCCIC to provide a number of services, including sharing information about cybersecurity risks and incidents, and providing technical assistance, risk management support, and incident response capabilities to federal and non-federal entities.[31] As part of its January 2015 initiative for "Enabling Cyber Security Information Sharing," the Obama Administration bolstered the NCCIC by designating this Center as both the hub for monitoring current cybersecurity trends and an operations center for managing responses to any on-going threats.[32]

A few weeks later, on February 10, 2015, President Obama went further and created the Cyber Threat Intelligence Integration Center (CTIIC), largely in response to perceived intelligence and coordination problems following the November Sony attack. The $35 million agency will bypass congressional approval and be created through a presidential memorandum under authority granted by the 2004 Intelligence Reform and Terrorism Prevention Act. According to Lisa Monaco, assistant to the President for Homeland Security and Counterterrorism, CTIIC is designed to "connect the dots" among cyberthreats facing the United

States "so that relevant departments and agencies are aware of these threats in as close to real time as possible… No existing agency has the responsibility for performing these functions, so we need these gaps to be filled to help the federal government meet its responsibilities in cybersecurity."[33]

As is evident in these developments and other White House cybersecurity initiatives,[34] President Obama has placed considerable importance on reducing hacking and cyberattacks as well as on improving information sharing between the U.S. government and the private sector about IT vulnerabilities and cyber threats. The private sector has been sharing threat information in some cybersecurity sectors with pre-competitive information that allows for sharing of information regarding vulnerabilities, but this is usually done *after* a breach or vulnerability information has been shared publicly. What the U.S. government desires is for such information to be shared either before the information is publicly disclosed or very soon after discovery of a breach. However, even with the Administration's proposal for a maximum 30-day requirement for breach notification, this may still be too late. Ideally, knowing about vulnerabilities *before* they are exploited is most useful.

Unfortunately, one of the Administration's legislative initiatives – a proposed amendment to the Computer Fraud and Abuse Act (CFAA – an anti-hacking statute)[35] – is at odds with the Administration's stated interest in increasing threat and vulnerability information sharing. The problem in essence is that the proposal substantially increases criminal penalties in the proposed CFAA amendment while at the same time failing to address definitional ambiguities within the law that have allowed it to be overzealously applied and enforced by legal authorities. The result, as explained next, is that in practice cybersecurity researchers are potentially at risk of criminal prosecution when conducting legitimate, vital research on IT vulnerabilities. This has a chilling effect both on conducting such research and especially on sharing it.

Some of the most useful security vulnerability information sharing occurs at the biggest computer security conferences in the world, which are held in Las Vegas during early August every year. Defcon started more than 22 years ago as an "underground" computer hacker conference. It was underground because at that time, the U.S. court system generated a lot of fear and uncertainty about the legal consequences for investigating IT vulnerabilities. If wise U.S. government agents could keep a low profile, they knew Defcon was the place to hear the best computer professionals talk about what was really possible to do with computers and the rapidly evolving Internet.

In its early years, there may have been only a couple of hundred people attending Defcon but by 2014, more than 18,000 people attended. Because of U.S. freedom of speech protections, only a handful of presentations are pulled every year, and many of those are due to contractual disputes between presenters and their employers and/or intellectual property concerns such as violations of the Digital Millennium Copyright Act (DMCA). The DMCA is a significant "silencer" of those who wish to share their computer security research because researchers have technical requirements not to "break" or "circumvent" "technological anti-circumvention" measures. Another piece of legislation that has unintended consequences every year is the CFAA, which causes researchers to avoid submitting their work, or to pull their presentations.

One such security researcher who was adversely affected by the CFAA is Andrew Auernheimer (aka, "Weev"),[36] who went to prison on a multi-year sentence for incrementing (adding) a number in a URL. The following example illustrates what Auemheimer did. A few popular online women's clothing vendors allow consumers to make a purchase online and to go to their online "cart" to review their finalized orders. In the URL, a few of these vendors show something that looks similar to the following:

https://www.womens_clothing_store_order39000

If you were to highlight and copy the URL, but change the end to "_order39001," a change of one digit at the end, you might see the next person's order contents, personally identifying information (PII) such as name, phone number and mailing address, and credit card number (some full and some only the last four digits).

Auernheimer did the same with a publicly accessible site he found for iPads using AT&T data connections, but wrote a script (an easy, short program) to increment the numbers at the end of a URL automatically. In the case of the women's clothing store online order, I legally represented a security researcher who had discovered the bug and contacted the California clothing company with details about it, including instructions on how to fix it. The clothing company threatened to report the researcher and me to the FBI for "malicious hacking." The researcher was prominent in the computer security industry and was not interested in a multi-year battle in court, so the bug was not fixed.

In Auernheimer's case, he took his findings to a journalist who published them online. AT&T quickly fixed the flaw, but the FBI mounted a criminal case against Auernheimer for "exceeding authorized access" in violation of the CFAA, for which he was found guilty and received a sentence of more than three years in prison.[37] He spent more than one year in jail – much of it in solitary confinement – before his case was overturned on appeal (although please note that this was due to a jurisdictional error, not because of a challenge to the CFAA).[38]

Were people's AT&T contact information more worthy of this protection than people's clothing purchases with full names, mailing addresses, (some) full credit card numbers and potentially embarrassing women's undergarment purchases? Which example is more worthy of a CFAA criminal investigation? Only one of the researchers went public with his findings, and he was the one who went to prison.

Whichever example one may deem as more worthy of time in prison, they both make it clear how the CFAA discourages security researchers from sharing their findings. Many security researchers and legal scholars think the "unauthorized access" clause in the CFAA is too vague, essentially because the definition of "unauthorized access" is weak.[39] In Auernheimer's case, he accessed an AT&T website that was publicly available, yet AT&T argued successfully that Auernheimer should have known that even though the public could access the site, he was not authorized to do incrementation to find "hidden" information.[40]

Of course impediments to desirable norms for sharing vulnerability information with the government also extend well beyond the ones the CFAA creates for independent researchers. There are many executive discussions within private companies about security vulnerabilities discovered during security research conducted as part of new product development. Often these pertain to vulnerabilities within the U.S.'s critical infrastructure (e.g. water, power, telecommunications, transportation, etc.). Due to civil and criminal liability concerns arising from the CFAA and related laws (as well as to other reasons such as competitive and reputational considerations), executives often do not share these findings with the government.

The Obama Administration's proposed revisions to the CFAA are intended to combat hacking and enhance deterrence through increased penalties for violations.[41] Unfortunately they continue to assume that people should know when access is authorized or not, even if it is not labeled as "restricted access" or the like. This is wrong-headed. Instead of increasing the prison terms for violations of vague CFAA provisions, the Administration should first define the critical term "unauthorized access" much more clearly. Security researchers should know when their work could "cross the line" from research to criminality so they are free to conduct legitimate research and disclose their findings in appropriate fora. The current ambiguity in the legal interpretation of "unauthorized access"[42] forces researchers to decide whether to share their vulnerability findings or, as a handful of prominent researchers do each year, to pull their

research from public venues and instead either bury the research or release it publicly, but anonymously. The unfortunate consequence of anonymous public disclosure is that it creates a "zero day" scenario where the vendor has no notice before a vulnerability is disclosed to the world and the vendor has to rush to implement a patch before exploitation. In this situation, the vendor also has no way to find the researcher for technical questions or requests for assistance in patching the vulnerability.

In addition to its proposed CFAA reforms aimed at deterring hackers and cyberattacks, the Obama Administration has also repeatedly pushed for new legislation to promote better cybersecurity information sharing between the private and government sectors. In mid-January 2015, the President issued an updated version of his Administration's proposed information sharing legislation.[43] This is an issue that Congress has struggled unsuccessfully with for several years. But in the past few months, especially in the wake of the Sony attack and the many high profile cyberattacks on U.S. businesses and government agencies, Congress seems to be very close to passing legislation that will meet with the President's approval.

Three similar legislative proposals in particular seem to be nearing final votes, one in the Senate and two before the House. The Senate Select Committee on Intelligence voted 14-1 on March 13 to approve sending its bill, the Cybersecurity Information Sharing Act (CISA), on for consideration by the full Senate, which could happen as soon as this month (April).[44] In the House, the Permanent Select Committee on Intelligence unanimously approved its version of cybersecurity sharing legislation, the Protecting Cyber Networks Act (PCNA), on March 26.[45] It is being billed as bipartisan. Separately the House Committee on Homeland Security is revising a similar piece of legislation called the Cyber Intelligence Sharing and Protection Act (CISPA). CISPA originally passed the House in 2013 but stalled in the Senate.[46] "If both House committees pass separate legislation, it would fall to Republican leaders to decide how to proceed. They could either shelve one of the bills or direct the committee chairmen to merge them."[47]

The core of all of these proposed bills, including the Administration's, is provisions that would allow threat information from the private sector to be shared within the U.S. government via a designated agency without risk of exposure of the cooperating firms to subsequent civil litigation. This basic proposition has been contained in several similar bills that have been considered by Congress and the White House in recent years but shelved in one way or another essentially in response to waves of public criticism.

Since the CISPA legislation previously passed the House and therefore advanced the farthest among these alternative bills, we focus here on it. CISPA encourages the private sector to share cyber threat information with the DHS's NCCIC. The part of CISPA that generates the greatest criticism is its vague definition of "cyber threat intelligence" as "information…directly pertaining to a vulnerability of, or threat to, a system or network of a government or private entity." This "cyber threat" could either be (a) "efforts to degrade, disrupt, or destroy such system or network," or (b) "theft or misappropriation of private or government information, intellectual property, or personally identifiable information."[48] While this bill has privacy implications that initially caused President Obama serious misgivings, he is now enthusiastically supporting it due to revisions in the bill as well as recent breaches and what he deems to be rising cyber threats to the U.S.

The legal immunity provided for cooperating private companies has been powerfully strengthened with this bill and there has not been another that offers as much legal protection for companies that share cyber threat information with the government. The computer security industry has been waiting more than a decade for this change.

However, what about CISPA immunity for independent security researchers or those at small companies? Within the NCCIC, the U.S.-CERT and ICS–CERT (see Figure 1, above) have been doing a great job in creating a focal location where security researchers can share their vulnerability findings. But this improvement unfortunately is accompanied by a restriction barring security researchers from publicly disclosing their findings until either the vendor has patched the flaw or a certain period of time has passed and the vendor has not or will not patch. The CERTs negotiate that period of time, but for some serious vulnerabilities – like those within critical infrastructure – not all researchers agree that the vendor should be allowed many months or sometimes even an undefined time to patch.

U.S.-CERT and ICS-CERT are doing a good job at negotiating between vendors and security researchers and in pursuing efforts to reward security researchers with public recognition.[49] But if CISPA (or any competing bill) in final form continues to omit immunity for independent researchers, and/or if criminal penalties in laws such as the CFAA are increased (as discussed above), then it is foreseeable that fewer security researchers will want to risk responsibly reporting their findings – especially to the U.S. government and with attribution.

Separate from these concerns, opponents of CISPA argue that it goes too far and that existing rules already allow companies to coordinate sufficiently with government security initiatives. The Administration, however, shifts the locus of the principle failure to the side of the government:

> We've got to stay ahead of those who would do us harm. The problem is that government and the private sector are still not always working as closely together as we should. Sometimes it is still too hard for the government to share threat information with companies. There are legal issues involved and liability issues. Sometimes, companies are reluctant to reveal their vulnerabilities or admit publicly that they have been hacked. At the same time, the American people have a legitimate interest in making sure that government is not potentially abusing information that it's received from the private sector.[50]

Indeed, anyone who has briefed the U.S. government intelligence agencies on cyber threats would agree that information sharing between the private sector and U.S. government is akin to a one-way street. Understandably, there is some information that is too sensitive to pass off without a security clearance in the private sector. That is why the NCCIC is important. Having a round-the-clock facility issuing warnings and sharing threat intelligence with the private sector was something that the U.S. government lacked before its establishment.

In addition to general incident reporting, NCCIC is also handling the distribution of threat and breach information to the private sector as well as providing actionable advice regarding how those who are still unaffected, but potentially vulnerable, can take steps to protect themselves. With the biggest breach of health care information in U.S. history occurring on February 5, 2015 involving over 80 million records being accessed by what the media is currently reporting as a foreign entity as the perpetrator, a single center for coordinating investigations as well as important information distributed to the private sector has never been more important than it is now.[51]

Non-State Actors: Nation-States Not Required

On August 20, 2013, U.S. President Obama issued President Assad's regime in Syria a "red line" warning against moving or using its chemical weapons. As the month progressed, tensions between the U.S., Russia and Syria became heated when use of U.S. deployed missiles was threatened against Syria should they violate President Obama's "red line." As politicians and the military discussed their strategies on Capitol Hill and in the White House, behind the scenes—in a darker world mostly insulated from the media—hacktivists were already engaging in a conflict

with the Internet as their battleground. One of those hacktivists is an American military veteran who calls himself "The Jester" because of his affection for Batman movies. While he uses the moniker "Jester," his actions and secret identity are more akin to the character of Bruce Wayne and Batman. The Jester is considered by many to be an American computer hacker vigilante. When he chats via encrypted chat rooms he states that his reason for hacking these sites, countries, and hacktivist groups who are adversaries of the U.S. is because he served four terms in the U.S. military during the height of the conflict in the Middle East.[52] He did not like what he saw, and after coming back to the U.S. after his service, he wanted to continue to assist the U.S. in their efforts to quash terrorism and threats to his country.

In 2010, one of his first targets was alemarah.info, believed to be the Taliban's first website. Since then, and on a daily basis, he continues his crusade using his computer hacking skills to further the interests of what he believes is protecting the U.S. On July 2, 2013, the Jester took responsibility for a series of DOS cyberattacks against the Ecuadorean stock exchange and the country's tourism website and he promised to attack any other governments considering granting asylum to NSA leaker Edward Snowden.[53] This action may be considered an example of cyber-enabled economic warfare. For political reasons, he threatened to disrupt the economy of any country offering asylum to Snowden.

By the middle of September 2013, President Obama declared that the U.S. would use force if Syria violated the ban on the use of chemical weapons.[54] As media reports circulated with images of ICBMs and explosions—suggestions of what was yet to come if the world's political leaders did not come to a resolution—the Internet battlefield was already active. As is happening right now in connection to Russia's military incursions into the eastern Ukraine, the malware community is extremely active with hacktivists supporting their respective countries by attacking the infrastructure of their country's opposition.

By the time the media reports that critical infrastructure facilities (electrical grid, telecommunications, water, transportation, etc.) have experienced breaches, hacktivists have already done their work. They are not waiting for the red tape bureaucracy as official agents of the government must, but take matters in their own hands and do what their governments cannot or will not do. These vigilantes operate fast, efficiently, and with little trace. If proficient with cryptography, Tor (an anonymizing browser), and the digital weapons trade with a "zero day" (exploit code that is new-to-the-world),[55] a knowledgeable hacker—or hacktivist group—has the potential to possess an arsenal akin to what some countries have amassed. So it is plausible that a small number of very skilled hackers have the ability to incapacitate a country's infrastructure. The Russo-Georgian War of 2008 is a primary example of this. The U.S. Cyber Consequences Unit released a report in August of 2009 that states that, "the cyberattacks against Georgian targets were carried out by civilians"; and that, "The hackers did not carry out physically destructive cyberattacks, although they probably had the technical expertise to do so, suggesting that 'someone on the Russian side was exercising considerable restraint.'"[56] Just a decade ago, it would have taken a nation state to accomplish this kind of disruption to an adversary.

Assuming that a small group of highly skilled and motivated individuals with sophisticated skills may be behind the Advanced Persistent Threats (APTs) we read about with each nation-state sponsored breach, how would a country engage such a group? There have been other examples of APTs that were not state sponsored, but rather small groups of young people causing economic damage to the U.S. and U.K. financial systems. Lulzsec did this for hactivism, but it may be considered an act of cyber-enabled economic warfare. They released the transaction logs of 3,100 automated teller machines in the United Kingdom, among many other attacks.[57] Of equal concern, if vigilante hacktivists from one country engage with another group over international politics, and if their digital weapons are as good as the government's arsenal,

they effectively may stand in the shoes of a super-power, but lacking the red-tape over their heads, there is nothing to block them from metaphorically "pulling the trigger."

In September 2013, The Jester challenged the Syrian Electronic Army (SEA), a Syrian-based group of hackers, over President Obama's "red line." The SEA claimed to have digital weapons that could be used to destroy critical infrastructure in the U.S., and in particular, they claimed they would target the U.S. power grid if the U.S. government launched missiles into their country. The Jester is a one-man army who had previously used powerful digital weapons he created against groups he determined were affiliated with Al Qaeda and attacked other foes of the U.S. government including North Korea.[58, 59]

The threats were instantly thrown across oceans via Twitter; these individuals fought their own battle online. The Jester said that if SEA attacked the U.S.' critical infrastructure, he would "put the lights out" in Syria. Luckily, the Syrian conflict de-escalated, but not before some hacker—or hacktivist group—knocked out the power in Syria for a period of time. The Jester declared on Twitter that he did not do it. Whenever The Jester takes down an online entity, he says "TANGO DOWN." In the example below, he lists "TANGO DOWN" on the Syrian Electronic Army's official site as well as the Syrian Atomic Commission. In the picture below, with regards to the timeline of events, it should be noted that the most recent event is listed at the top, and the next most recent after that.

Exhibit 2

These exchanges occurred on August 26 and were then followed by another round the next day:

The U.S. did not launch missiles into Syria, but if they had, an interesting question is whether these hacktivists in the U.S. would have damaged networks and critical infrastructure before the first U.S. missile hit the ground. In an era when digital weapons neither cost as much nor require expensive resources as do the real-world physical weapons such as a missiles or fighter jets, the nature of a war, usually defined as being directed and funded by nation-states is rapidly being transformed. The concept of war has also evolved to where even the players who are much smaller than their adversaries can be just as dangerous. While asymmetric targets may be attacked for patriotic or terrorist reasons, the secondary consequences also pose a new and serious threat. This is an example of a new, cyber-enabled version of asymmetric warfare.

Can these types of weapons only be created by states or could a small group, or even a sole, non-state actor create one? Is this type of weapon cost-prohibitive for anyone but a well-funded country to create? The answer to these questions, as harrowing as they may sound, can be found by attending any one of the large international computer security/hacker conferences.

Individual security researches come together at security conferences around the world to showcase their work. The abilities and discoveries made by these researchers are astounding: it does not take a nation-state anymore. In a project that was originally for a security conference called Derbycon, two independent security researchers, Terry McCorkle and Billy Rios, set out to find "100 bugs in 100 days" within critical infrastructure technologies.[60] Much to their surprise, they found hundreds of vulnerabilities and have worked in conjunction with ICS-CERT to disclose them.[61] The team of two, who acted in their spare time, proved that with malicious intentions critical infrastructure could indeed be destabilized by a small group of individuals with very little funding. If an adversary had found these vulnerabilities, the consequences could have been quite serious because all were within critical infrastructure technologies.

While Stuxnet—a specifically-targeted digital weapon—took a great deal of operational security intelligence to create, it was successful in setting back Iran's nuclear enrichment program by at least two years.[62] Once Stuxnet was discovered and made public, it was taken apart, analyzed, and—for better or worse—used as a learning tool by security researchers.[63] Stuxnet let the genie out of the bottle and raises the question: would countries, and concurrently, product vendors, prefer to know about vulnerabilities or not? The computer security industry, which includes hackers of all "hat" colors with perceived ethical implications (white, grey and black) discovers critical vulnerabilities every day, but its members have to make decisions with serious ethical and legal consequences about whether or not to share the information. Are these hackers "enemies" or "allies"? The answer depends upon how the information disclosure is handled by both the security researcher and the company or government affected by the vulnerability or proof-of-concept exploit. But if that vulnerability is not discovered and patched, then the possibility remains for opening that fissure using exploits results and producing a breach.

The present may mark a paradigm shift from the Cold War era in which weapons capable of crippling a country's infrastructure were financially cost-prohibitive to create. Obtaining the physical materials for traditional kinetic weapons was expensive as well as hard to get and disseminate because of international treaties and law enforcement organizations working to thwart weapons proliferation. However, now that digital weapons can be pocket-sized—code hidden on a USB drive or even a secret compartment on a coin—or transferred online, discovering trade of digital weapons across borders is infinitely more difficult, if not impossible. While difficult to enforce, the U.S. is contemplating expanding international trade regulations through ITAR (International Traffic in Arms Regulations) that would define zero day exploits as "munitions." If that becomes the case, the international sale of zero day exploits would force computer security professionals developing the exploits to go through international trade

regulations via EAR (Export Administration Regulations), which requires government oversight for the transaction.[64]

Additionally, 41 countries have signed the Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies. This arrangement categorizes zero days under export controls. Among those 41 countries, Spain and the U.S. have both signed this agreement. While efforts were made in the agreement to distinguish zero days from legitimate tools (such as penetration testing tools used with authorization and for hire to test the security of networks), no hacker would want to be the test case selected to clarify that his software was not a "weapon" but a "penetration testing tool." Nevertheless, zero day trade via cryptographically protected communications, anonymizing web browsing, and crypto currency (like Bitcoin) with "Dark" online wallets, is going to be a tough one to regulate. These munitions are tiny and it is possible to be anonymous online.

An additional complication to the U.S. regulating the creation and sale of digital weapons relates to the fact of what zero days, inherently, consist of: computer code. Factually speaking, they are just programs. The U.S. Constitution's First Amendment protects code as "speech." While code does not get the highest protection as would political speech in the U.S., it is still protected. Looking into the purpose or function—or the "content" of the speech—requires a higher level of review as to whether this type of speech can be legitimately "silenced." There has not yet been a legal case in the U.S. involving a defense using a "code is speech" argument, but it is going to be interesting when it happens.

Some American analysts believe that the U.S. Department of Justice should stop imprisoning hackers as the U.S. recently has done in a group of criminal cases involving the issue of "unauthorized access" with the CFAA. In an interview for a PBS "Frontline" documentary in 2001, Robert Steele, CEO of Open Source Solutions, discussed how the federal government handles people caught violating computer crimes laws in the United States:

> The bottom line is that hackers are the pioneers in this electronic frontier. They are way out in front of the rest of the world.... I'm very upset that people don't understand that hackers are, in fact, a national resource. You can't create a hacker. Hackers are born; they are very special people. When the Israelis catch a hacker, they give him a job. When the Americans catch a hacker, they kick him in the teeth and throw him in jail. And that's not good.

There are indeed some countries like Israel that are recruiting hackers as part of their national defense strategy and consider them a national resource. Likewise, Latvia, one of the Baltic States that are concerned about Russia's expanding boarders, has a Cyber Guard program (part of the National Guard volunteer military program) for which they recruit and train hackers to defend Latvia's critical infrastructure from cyberattacks. The Latvian military hired its first 13 "cyber guards" in February of 2014,[65] incorporating cyber into its national defense strategies and training a hundred hackers, both from civilian and military backgrounds, by the end of this year. Additionally, a similar team will be established for the Youth Guard—a movement for teens with computer hacking skills. The Cyber Guard program also participates in a defense program called "Locked Shields"—an annual real-time network defense exercise organized by the NATO Cooperative Cyber Defense Centre of Excellence in Tallinn, Estonia.[66]

As for U.S.' efforts to recruit hackers, NSA Director and head of U.S. Cyber Command, General Keith B. Alexander, gave a keynote speech at a premier computer security hacker conference in the summer of 2012. His speech had some promising elements, including stating the need for a country to keep an army of hackers with offensive skills to ensure its future prosperity. However, Alexander's positive comment was later overshadowed by Former NSA and CIA chief General Michael Hayden who remarked that hackers were "nihilists, anarchists, activists, Lulzsec, Anonymous, twenty-somethings who haven't talked to the opposite sex in five or six years."[67] This undercut the message the U.S. government intended to impart in an effort to

recruit hackers to take sub-paying government jobs out of patriotic enthusiasm for defending their country. Moreover, after the NSA leaks in 2013, the sentiment amongst conference organizers changed, and the founder of the conference politely asked the Feds to stay home that year and to please not attend the conference because a "cooling off" period of time was needed.

Whether hackers are viewed as enemies or allies depends upon one's perspective, but it is clear that the tools, skills and motivation supporting their patriotism for their respective countries are strong and will become stronger as the barrier-to-entry lessens for obtaining hacking skills and the tools-of-the-trade. Whether a county chooses to embrace these individuals with exceptional skills or instead prosecute them after they disclose vulnerabilities that need patching, may affect a country's overall defensive strategy for "cyber war." Similar to the military reserves in the Baltic countries, if the U.S. would organize civilian computer security professionals—either volunteers or paid reservists—this could help the country deter, detect and defend against cyber enabled economic warfare. In addition, it might provide an avenue for U.S. patriotic hackers to direct their skills towards organized and defensive operations instead of becoming solo vigilantes like The Jester.

Current State of Threats for Critical Infrastructure and Transportation

The Ponemon Institute reported that 70% of critical infrastructure organizations were breached in 2014.[68] When these organizations were asked about the likelihood of an attack on their industrial control systems or SCADA systems, 78% responded that a successful attack is at least "somewhat likely" in the next 24 months. Only 21% thought that the risk level to ICS and SCADA has "substantially decreased" because of regulations and industry-based security standards (such as NIST's Cyber Security Framework).[69] The results of this survey suggest that either tighter implementation of regulations or better standards are needed. However, what the survey also shows is that information sharing about vulnerabilities is important too and that the NCCIS, with ICS-CERT and U.S.-CERT in its purview, is making progress.

Coordination of cyber threats, such as directed attacks against critical infrastructure with custom-designed malware, is no longer a "maybe" but has evolved to a "when." We learned in 2014 that a new form is real and has been in development—this would be the first since Stuxnet. Whether the campaign is referred to as "Dragonfly," "Havex," or "Energetic Bear" depends upon the company doing the research, but malware targeting ICS has been discovered "in the wild."[70] Researchers are not yet sure about the motivation behind Havex. While Symantec believes it targets the energy sector, ICS security researcher Joe Langrill with Belden believes that the real target is American pharmaceutical companies.[71] Whether the motive is to steal the formulas for brand pharmaceuticals or perhaps to disrupt the factory process for the drug production is unclear. Considering that the pharmaceutical industry is a part of U.S. critical infrastructure with medical facilities, this possible attack vector is as important as other critical infrastructure vulnerabilities and attacks discussed in this paper.

Symantec theorized that it may be state-sponsored with origins in Eastern Europe, but as discussed in a prior section, creation of powerful exploits on ICS has been done by a single security researcher or a small group with no prior-knowledge of ICS systems and in a short time period with limited financial resources. While Havex may contain "sophisticated malware," knowledge about ICS vulnerabilities, the hardware/software for testing, and educational resources regarding creation of exploits is becoming easier to procure. Indeed, these attacks on critical infrastructure are more likely than not.

Some security researchers believe that a major infrastructure cyberattack is imminent.[72] In the past year, there have been a number of bold, malicious attacks that have caused serious

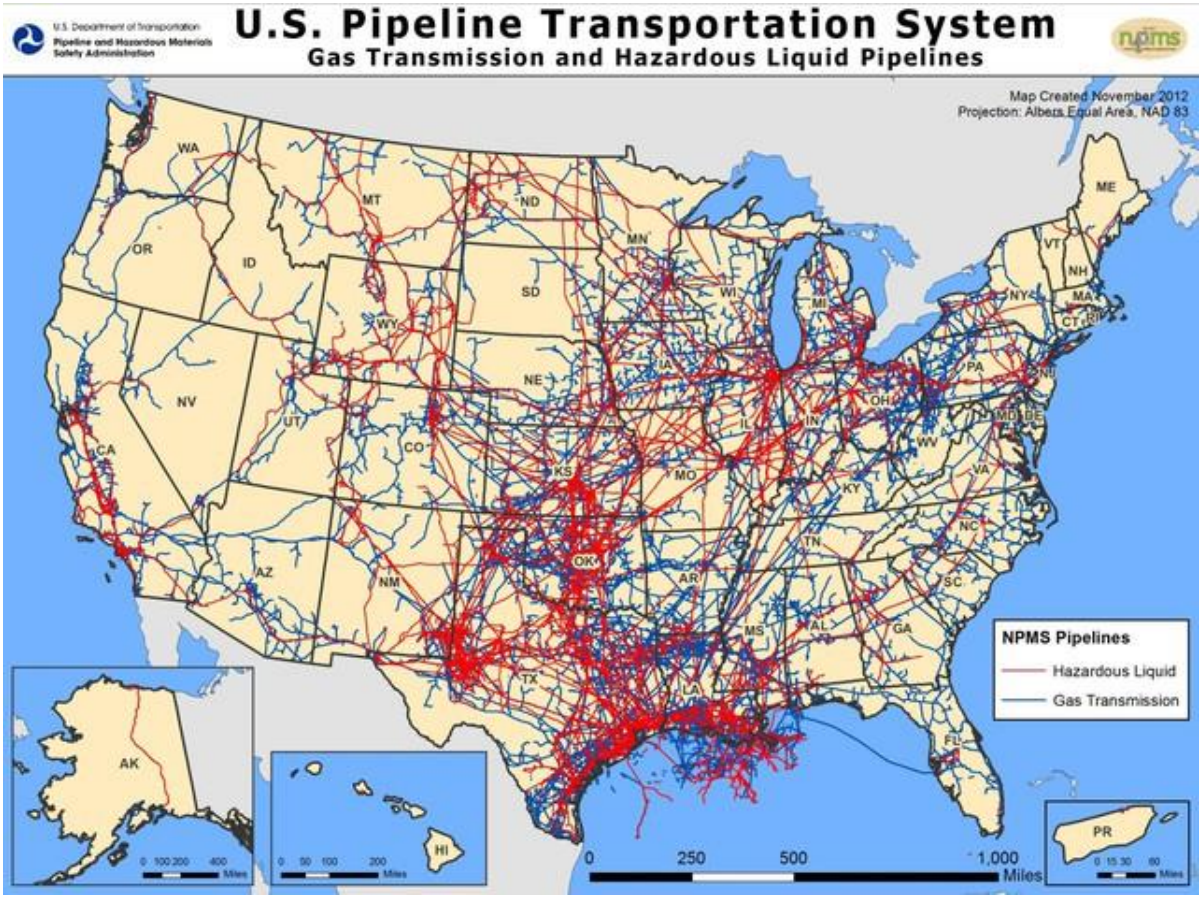
damage. Luckily, there has not yet been any loss of life as a result. Are the attackers practicing for what will be the "big one?"

At the end of December 2014, a metal working plant's ICS system in Germany was attacked. The attackers specifically targeted the company's corporate network with phishing emails.[73] Unfortunately, the ICS facility's network was not property segregated from the corporate network and the attackers were able to get into the ICS control computers and severely damage the factory—rendering it impossible for workers to shut-down a furnace. The German company does not know why anyone would want to target their company. Was this target incidental and were attacker's practicing by "breaking" specific ICS devices?[74]

Quite recently it was disclosed that in 2008 one of the most secure pipelines in the world was attacked. The BP-owned Bake-Tbilisi-Ceyhan pipeline in Turkey exploded in 150 foot flames. Attackers infiltrated the pipeline through a wireless network, tampered with the systems, and caused the explosion.[75] The U.S. has an extensive system of pipelines that run throughout the country, and although they are considered to have good security, vulnerabilities for ICS systems—as publicly published by ICS-CERT—establish the importance for pipeline operators to be cognizant of online security research (see Exhibit 3, next page).

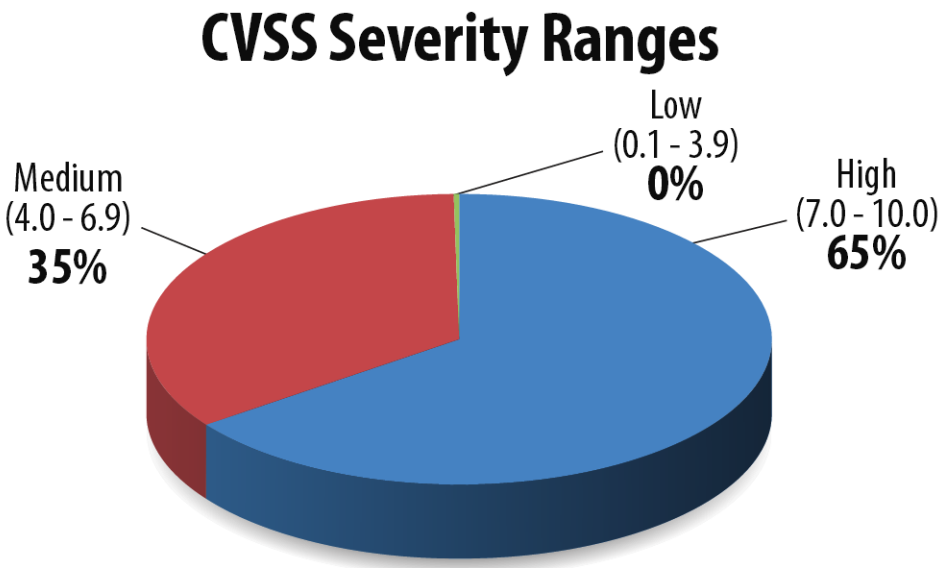
U.S.-CERT released a chart regarding the severity of confirmed attacks. They found that 65% of the successful attacks were "high," meaning severe, per the Common Vulnerability Scoring System (CVSS) guidelines that take into account many factors such as "exploitability," "collateral damage," and "access vector" (see Exhibit 4, next page).

Exhibit 3



SOURCE: USDOT Pipeline and Hazardous Materials Safety Administration

Exhibit 4



SOURCE: U.S.-CERT *Monitor*, Jan-Apr 2014.[76]

In May 2014, ICS-CERT issued a warning about several known attacks against U.S. utilities.[77] While the specific utilities were not publicly named, the information was released to make other companies could be aware of targeted, on-going attacks. The administrative systems attacked were Internet-accessible and intruders gained access by discovering weak passwords.

In a November 20, 2014, hearing for the House Intelligence Committee, NSA Director Admiral Michael Rogers said that foreign governments had already hacked into U.S. energy, water, and fuel distribution systems. The potential to damage the essential services was severe. "There should be [no] doubt in anybody's mind that the cyber challenges we're talking about are not theoretical," Rogers said. "This is something real that is impacting our nation and those of our allies and friends every day."[78]

Policy Recommendations

Government authorities responsible for protecting critical infrastructure have more awareness of the risks than they did before the NIST Cybersecurity Framework was established last year. Now, most government agencies are aware of these risks and are taking action to secure the country's infrastructure. With the assistance of NCCIS, detection and monitoring of risks has become more centralized.

However, with the advances in information technologies and greater Internet connectivity of devices, the threat landscape has widened. With that increase in vulnerabilities, and with more potential threats to monitor, there currently is a dearth in skilled information security professionals to meet this demand. While there have been increases in funding to universities teaching these skills, graduates are being rapidly employed by the private sector for information security jobs. The U.S. government has a difficult time recruiting and retaining cybersecurity professionals because of the salary difference between what the government can pay and what the private sector offers. As more breaches of private companies become commonplace, private sector salaries are rising.[79] More funding for universities with cybersecurity education programs

would help, and creative incentives to motivate talented cyber professionals to work in the government sector are needed.

Additionally, the employment requirements are challenging for some of the personalities and work-habits associated with professionals in computer security. Traditional work habits such as an eight hour work day and office dress codes are unappealing for many computer security professionals. As trivial as it may sound, working night-hours in a casual-dress environment are features that are highly important to many information security professionals and their scarcity in the government sector is a turn-off that prevents many from taking jobs with the U.S. government. While some private companies have changed their corporate cultures to attract and retain these kinds of employees, the U.S. government is having a more difficult time accommodating these workers' requests as well as increasing pay commensurate with the private industry. U.S. government agencies need to adjust their hiring policies, work rules, and compensation packages for cybersecurity professionals if they are going to succeed in attracting and retaining the skilled individuals they need.

In addition to improved recruitment and retention programs for computer security professionals, critical infrastructure protection should have heightened priority. SCADA systems have vulnerabilities associated with their ease of access and interconnectedness. While there may be technical vulnerabilities that go beyond issues experienced by specific vendors, there are general policy guidelines that have been recommended for protection of SCADA systems. More and stricter attention is needed to fortify protection of the control computers and segregate the control network from the networks used for the generation company communications. Most companies implementing SCADA systems are now aware of the risks associated with their connections to the Internet but have not fully constructed their defenses against those risks.

With the still continuous stream of industrial control system vulnerabilities being reported to U.S.-ICS CERT, some facilities have questioned their need to have continuous, always-on Internet connections to their SCADA systems (e.g. if a facility is part of critical infrastructure and it does not need remote access to function). Some facilities are taking their systems off the Internet except to do scheduled software and firmware updates. Even then, the sites to which the control computers can connect are "white list" restricted to those of the system's vendor.

Suggested policy recommendations for computers and devices considered to be critical infrastructure would particularly affect the network availability and physical access. All infrastructure computers and devices should have remedial testing conducted to assure the integrity of both the network segmentation and segregation. Air gapping the networks that contain critical infrastructure computers or devices should take priority whenever the situation allows. Additionally, access to these computers and devices should be entirely restricted to only critical personnel. The NIST cybersecurity framework makes these policy recommendations; perhaps it is time to make some of the recommendations requirements for the energy sector components of critical infrastructure.

Similar to the way in which ICS-CERT shares vulnerability information with the private sector, NCCIS has been established as a focal point to collect vulnerability information and coordinate sharing of threat and attack information with those who need it in both the private and government sectors. More vulnerability information could be shared between the private sector and the government if existing legislation was suitably modified. Currently, the CFAA and the DMCA do not provide the appropriate exceptions for those who do security research to be able to disclose vulnerabilities which are discovered. Furthermore, certain methods of research, if disclosed, could be considered Federal crimes. Any American citizen is thus hindered in the scope of available research methods while adversaries are not. Providing both a venue and exceptions in legislation would allow researchers to discover and report vulnerabilities to the appropriate organizations without fear of criminal repercussions. For these reasons, a policy

recommendation is to create exemptions for security researchers and immunity as is provided by CISPA to private sector companies.

Summary

Critical infrastructure encompasses not only the electrical grid, water treatment, communication networks, and healthcare, but also transportation. Airplanes, trains, trucks and passenger vehicles all make up an important part of our country's backbone. In Hollywood movies, there are dramatic scenes in which hackers attack one or more parts of a country's critical infrastructure networks. In the movie, "Live Free or Die Hard," a disgruntled former NSA employee sets out to destroy multiple critical infrastructure systems in the U.S., including traffic controls and portions of the electrical grid. These "Hollywood" hacks are of course fictions but nonetheless have a strong basis in fact.

Small-group and independent research confirms that such hacks are feasible; it does not take a great deal of sophistication or financial resources to create successful exploits that can access PLCs in a ICS or SCADA system controlling either a power plant, a water treatment facility or a dam, or doors and gates in a prison. While the success of the Stuxnet attack, designed to disrupt and delay Iran's secret nuclear power program, did require considerable sophistication and insider knowledge, it should also stand as a warning to how vulnerable much more public infrastructure systems can be to a dedicated adversary's cyberattack.

In January 2015, President Obama again urged Congress to pass bold and long-awaited cybersecurity legislation in order to enhance information sharing between the U.S. government and the private sector. While there are privacy groups disagreeing with definitions regarding when the U.S. government will access communications during times of "cyber threats," nevertheless, the Administration has produced its own proposed legislation and encouraged the relevant House and Senate Committees to move quickly to pass an acceptable version. The Senate Intelligence Committee has forwarded CISA to the full Senate and it is likely to be considered in April. House Committees have produced similar bills (i.e. CISPA and PCNA) that also appear like to be taken up by the House in April.

The immunity these bills provide to organizations—not specifically independent security researchers—that are willing to share cyber vulnerabilities and threat intelligence with designated U.S. government cybersecurity agencies is an exciting prospect for promoting security research in companies. However, considering that independent researchers and small companies are also generating valuable research and currently appear to fall outside of the immunity protection, it is advisable that the legislation be modified so that immunity will be extended to these groups.

This is especially important when one takes into consideration the undesirable legal consequence of the DMCA intellectual property law that prohibits and penalizes security researchers from "circumventing technological protections" on copyright software or firmware, which can apply even when security researchers make a safety-critical discovery of a vulnerability that is in dire need of patching. Additionally, one of President Obama's new cyber legislation proposals enhances the already vague CFAA to almost double the years in prison for hacking crimes without adequately resolving definitional ambiguities.

The unfortunate flip-side to cracking down on cybercrimes is that it likely will also chill much-needed cybersecurity research and may, in fact, push this kind of research back into "underground" conferences, thus reducing instead of enhancing the sharing of cyber threat information. The U.S. needs researchers to generate exploit code in order to enhance penetration testing software which, under some U.S. requirements, is needed for yearly testing of security measures for companies conducting financial transactions. Exploit code is only a

"weapon" if it is used as such. Otherwise, it is a valuable "tool" for testing security systems. We need U.S. researchers to feel comfortable creating these tools; the Administration's proposed CFAA enhancements may instead put them at risk.

A strong defense and offense is needed in today's cyber-connected world. The U.S. and other countries are beginning to recruit "cyber warriors" to fulfill this need. Timing for this initiative may be just right. Some security researchers believe that a major cyberattack on critical infrastructure will happen soon. Whether or not these researchers are correct with their projections about imminent major attacks, statistics show that attacks on crucial infrastructure in the U.S. are increasing in frequency. Additionally, when these attacks or breaches of these systems do occur, the danger of severe adverse consequences is quite "high."

President Obama's recent cybersecurity legislation has already had a big impact on the computer security community. The NCCIS along with other information-sharing agencies such as U.S.-CERT and ICS-CERT are the correct places to generate information gathering and sharing within the U.S. government. With a bit of tweaking to his CFAA enhancement and exemptions for security research for the DMCA, the cybersecurity industry, through the significant research they share with the U.S. government, private sector and the public, will strengthen the U.S. government's emphasis on information sharing in its vital effort to protect critical infrastructure.

---

[1] Eric Byres. (2011, March 21) Summing up Stuxnet in 4 Easy Sections – (plus Handy Presentation). Tofino Security. Retrieved March 7, 2015, from https://www.tofinosecurity.com/blog/summing-stuxnet-4-easy-sections-plus-handy-presentation

[2] Elinor Mills. (2011, November 18) Hacker says he broke into Texas water plant, others. CNET. Retrieved March 1, 2015, from http://www.cnet.com/news/hacker-says-he-broke-into-texas-water-plant-others/

[3] Executive Office of the President. (2013, February 12) Executive Order 13636 – Improving Critical Infrastructure Cybersecurity. Executive Office of the President. Retrieved from https://www.whitehouse.gov/issues/foreign-policy/cybersecurity/eo-13636

[4] NIST. (2013, October 29) Improving Critical Infrastructure Cybersecurity Executive Order 13636: Preliminary Cybersecurity Framework. National Institute of Standards and Technology. Retrieved from http://www.nist.gov/itl/upload/preliminary-cybersecurity-framework.pdf

[5] NIST. (2014, February 12) Framework for Improving Critical Infrastructure Cybersecurity, Version 1.0. National Institute of Standards and Technology. Retrieved from http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214-final.pdf

[6] The True Story: Die Hard 4.0. (2012). Discovery Channel. Retrieved from http://www.discoveryuk.com/web/the-true-story/about/die-hard-4/

[7] Robin Mejia. (2007, January). CSI: TCP/IP. Wired, (15.01). Retrieved from http://archive.wired.com/wired/archive/15.01/cybercop.html

[8] Kim Zetter. (2011, July 29). Researchers Say Vulnerabilities Could Let Hackers Spring Prisoners from Cells. Wired. Retrieved from http://www.wired.com/2011/07/prison-plc-vulnerabilities/

[9] Adam Greenberg. (2014, August 8). Defcon: Traffic Control Systems Vulnerable to Hacking. SC Magazine. Retrieved from http://www.scmagazine.com/defcon-traffic-control-systems-vulnerable-to-hacking/article/365416/

[10] Ruben Santamarta. (2014, August 11). SATCOM Terminals: Hacking by Air, Sea and Land. Black Hat. Retrieved from https://www.youtube.com/watch?v=YeKswEamOl4

[11] Airplanes Could be Taken Over Through Inflight Entertainment Systems, Hacker Claims. (2014, August 4). RT. Retrieved from http://on.rt.com/etdj5j

[12] Amber Corrin. (2014, April 25). Government, Industry Target Air Traffic Cyberattacks. Retrieved from http://www.federaltimes.com/article/20140425/CYBER/304250012/Government-industry-target-air-traffic-cyber-attacks

[13] District of Columbia Fire and EMS. (2015, January 17). Initial Report on the LEnfant Plaza Metro Incident January 12 2015. Retrieved from http://www.scribd.com/doc/252899205/Initial-Report-on-the-LEnfant-Plaza-Metro-Incident-January-12-2015

[14] Jennifer Strong-Michas. (2011, November). Hi Ho Silver Line. Electrical Contractor. Retrieved from http://www.ecmag.com/section/your-business/hi-ho-silver-line

[15] Metropolitan Washington Airport Authority: Final Design and Construction. (2012, July 12). Retrieved from http://www.mwaa.com/file/8-13-C001_RFQI.pdf

[16] Aliya Sternstein. (2012, January 23). Hackers manipulated railway computers, TSA memo says. Nextgov.com. Retrieved March 2, 2015, from http://www.nextgov.com/cybersecurity/2012/01/hackers-manipulated-railway-computers-tsa-memo-says/50498/

[17] John Leyden. (2008, January 11). Polish teen derails tram after hacking train network. The Register. Retrieved March 2, 2015, from http://www.theregister.co.uk/2008/01/11/tram_hack/

[18] Wayne Chung. (2013, May 1). SCADA security and understanding the risk impacts - CSO | The Resource for Data Security Executives. Retrieved March 2, 2015, from http://www.cso.com.au/article/460613/scada_security_understanding_risk_impacts_/

[19] Transportation Research Board. (2014). Effective Practices for the Protection of Transportation Infrastructure from Cyber Incidents. TRB No. NCHRP 20-59(48). Retrieved from http://apps.trb.org/cmsfeed/TRBNetProjectDisplay.asp?ProjectID=3461

[20] Nothingface. (2004, August 1). Automotive Networks. Presented at the Alexis Park, Las Vegas, Defcon 12. Retrieved from http://althing.cs.dartmouth.edu/secref/resources/defcon12/dc-12-speakers.html#nothingface

[21] Tiffany Rad. (2008, December 4). OpenOtto. Presented at the Pace University, New York City, 5th Annual Pace Pitch Contest. Retrieved from http://www.pace.edu/lubin/departments-and-research-centers/entrepreneurship-lubin/pace-pitch-contest/fifth-annual-pace-pitch-contest

[22] Karl Koscher, Alexi Czeskis, Franziska Roesner, Shwetak Patel, Tadayoshi Kohno, Stephen Checkoway, Damon McCoy, Brian Kantor, Danny Anderson, Hovav Shacham, Stefan Savage. (2010, May). Experimental Security Analysis of a Modern Automobile. 2010 IEEE Symposium on Security and Privacy. Retrieved from http://www.autosec.org/pubs/cars-oakland2010.pdf

[23] Charlie Miller, & Chris Valasek. (2014) Adventures in Automotive Networks and Control Units. Retrieved from http://illmatics.com/car_hacking.pdf

[24] The CAN bus is akin to a car's "brain" and "neural network."

[25] *Op. cit.,* Charlie Miller & Chris Valasek.

[26] Eric Evenchick. (2013, November 5). CAN Hacking: The Hardware. Hackaday. Retrieved March 2, 2015, from http://hackaday.com/2013/11/05/can-hacking-the-hardware/

[27] The definitions and descriptions of the agencies have been obtained from the respective agencies' websites.

[28] About the National Cybersecurity & Communications Integration Center | Homeland Security. (2014, November 4). Retrieved March 2, 2015, from http://www.dhs.gov/about-national-cybersecurity-communications-integration-center

[29] Phyllis Schneck. (2014, December 10). Written testimony of NPPD Deputy Under Secretary for Cybersecurity Phyllis Schneck for a Senate Committee on Banking, Housing, and Urban Affairs hearing titled "Cybersecurity: Enhancing Coordination to Protect the Financial Sector." Department of Homeland Security. Retrieved March 2, 2015, from https://www.dhs.gov/news/2014/12/10/written-testimony-nppd-senate-committee-banking-housing-and-urban-affairs-hearing

[30] Ibid.

[31] Sean B. Hoar. (2014, December 18). Cyber and National Security. Policy and Regulatory Positioning, Privacy and Security Law Blog. http://www.privsecblog.com/articles/cyber-national-security/

[32] Executive Office of the President. (2015, January 13). Securing Cyberspace - President Obama Announces New Cybersecurity Legislative Proposal and Other Cybersecurity Efforts. The White House Office of the Press Secretary. Retrieved at https://www.whitehouse.gov/the-press-office/2015/01/13/securing-cyberspace-president-obama-announces-new-cybersecurity-legislat

[33] Dustin Volz. (2015, February 10) Obama Is Creating a New Agency to Combat Cyberthreats. National Journal. http://www.nationaljournal.com/tech/obama-is-forming-a-new-agency-to-combat-cyber-threats-20150210

[34] President Obama's February cybersecurity conference at Stanford University is one example; see Damian Paletta. (2015, February 11). The White House Cybersecurity Event to Draw Top Tech, Wall Street Execs. Wall Street Journal. Retrieved from http://www.wsj.com/articles/white-house-cybersecurity-event-to-draw-top-tech-wall-street-execs-1423659629

[35] Executive Office of the President. (2015, January) Updated Administration Proposal: Law Enforcement Provisions. Whitehouse.gov. Retrieved from https://www.whitehouse.gov/sites/default/files/omb/legislative/letters/updated-law-enforcement-tools.pdf

[36] U.S. v. Auernheimer, 13-1816.

[37] RT.com. (2013) AT&T Hack Lands Andrew Auernheimer in Jail. RT.com. Retrieved from http://on.rt.com/oyic10

[38] Jerry Markon. (2014, April 11) Computer Hacker Andrew Auernheimer's Conviction is Overturned by Appeals Court. Washington Post. Retrieved from http://www.washingtonpost.com/politics/computer-hacker-andrew-auernheimers-conviction-is-overturned-by-appeals-court/2014/04/11/0744a3bc-c1bc-11e3-b195-dd0c1174052c_story.html

[39] Ryan H. Niland. (2014) Do Not Read This Article at Work: The CFAA's Vagueness Problem and Recent Legislative Attempts to Correct it. North Carolina Journal of Law & Technology, Volume 15. Retrieved from http://ncjolt.org/wp-content/uploads/2014/05/Niland_Final.pdf

[40] Orin Kerr. (2013, March 21) *United States v. Auernheimer*, and Why I am Representing Auernheimer Pro Bono on Appeal Before the Third Circuit. The Volokh Conspiracy. Retrieved from http://volokh.com/2013/03/21/united-states-v-auernheimer-and-why-i-am-representing-auernheimer-pro-bono-on-appeal-before-the-third-circuit/

[41] Op. cit., Executive Office of the President. Updated Administration Proposal: Law Enforcement Provisions.

[42] See for example David S. Weber. (2012, June 20) Circuit Courts Struggling with Scope of CFAA. Digital Discovery. Retrieved from http://www.digitaldiscoveryesi.com/Blog/Circuit%20Courts%20Struggling%20with%20Scope%20of%20CFAA/

[43] Executive Office of the President. (2015, January 13). Updated Department of Homeland Security Cybersecurity Authority and Information Sharing. Office of Management and Budget. Retrieved from https://www.whitehouse.gov/omb/legislative_letters

[44] Dustin Volz. (2015, March 18). Here's What Is in the Senate's Cybersecurity Bill. National Journal. Retrieved from http://www.nationaljournal.com/tech/here-s-what-is-in-the-senate-s-cybersecurity-bill-20150318

[45] HPSCI. (2015, March 26). HPSCI Passes Cyber Bill Out of Committee. House Permanent Select Committee on Intelligence. Retrieved from https://intelligence.house.gov/press-release/hpsci-passes-cyber-bill-out-committee

[46] Kate Knibbs. (2015, January 14). The New CISPA Bill Is Literally Exactly the Same as the Last One. Retrieved March 2, 2015, from http://gizmodo.com/the-new-cispa-bill-is-literally-exactly-the-same-as-the-1679496808

[47] Damien Paletta. (2015, March 19) Dueling Bills complicate U.S. Cyberdefense Efforts. Washington Wire, Wall Street Journal. Retrieved from http://blogs.wsj.com/washwire/2015/03/19/dueling-bills-complicate-u-s-cyberdefense-efforts/

[48] Mike J. Rogers. (2013) Related Bills: H.R.624 – 113th Congress (2013-2014): Cyber Intelligence Sharing and Protection Act. Congress.gov. Retrieved from https://www.congress.gov/bill/113th-congress/house-bill/624/related-bills

[49] U.S.-CERT. (2014). U.S.-CERT Federal Incident Notification Guidelines. DHS U.S.-CERT. Retrieved March 2, 2015, from https://www.us-cert.gov/incident-notification-guidelines

[50] Tanya Somanader. (2015, January 14). Securing Our Cyberspace: President Obama's New Steps to Strengthen America's Cybersecurity. The White House. Retrieved March 2, 2015, from http://www.whitehouse.gov/blog/2015/01/14/securing-our-cyberspace-president-obamas-new-steps-strengthen-americas-cybersecurity

[51] Anna Wilde Mathews, & Danny Yadron. (2015, February 4). Health Insurer Anthem Hit by Hackers. Wall Street Journal. Retrieved March 2, 2015, from http://www.wsj.com/articles/health-insurer-anthem-hit-by-hackers-1423103720

[52] Anthony Freed. (2012, April 10). Transcript: Patriot Hacker th3j35t3r Addresses USM Students. Retrieved March 2, 2015, from http://www.infosecisland.com/blogview/20975-Transcript-Patriot-Hacker-th3j35t3r-Addresses-USM-Students.html

[53] Dana Liebelson. (2013, July 2). Snowden and Assange Targeted by Mysterious Hacker "The Jester." Mother Jones. Retrieved March 2, 2015, from http://www.motherjones.com/politics/2013/07/hacker-jester-targets-assange-snowden-ecuador

[54] Jillian Blake, & Aqsa Mahmud. (2013). A Legal 'Red Line'? Syria and the Use of Chemical Weapons in Civil Conflict. UCLA Law Review Discourse. Retrieved March 2, 2015, from http://www.uclalawreview.org/?p=4919

[55] Kim Zetter. (2014, November 11). Hacker Lexicon: What Is a Zero Day? Wired. Retrieved March 2, 2015, from http://www.wired.com/2014/11/what-is-a-zero-day/

[56] Jeanne Meserve. (2009, August 17). Study warns of cyberwarfare during military conflicts. CNN.com. Retrieved March 2, 2015, from http://www.cnn.com/2009/U.S./08/17/cyber.warfare/index.html?iref=24hours

[57] Fox News. (2011, June 21). A Brief History of the LulzSec Hackers. Retrieved March 2, 2015, from http://www.webcitation.org/5zbwTf458

[58] Mathew J. Schwartz. (2013, April 12). Anonymous-Linked Hacker Claims North Korea Win. Retrieved March 2, 2015, from http://www.darkreading.com/attacks-and-breaches/anonymous-linked-hacker-claims-north-korea-win/d/d-id/1109520?

[59] Emil Protalinski. (2012, March 14). Hacker threatens to expose Anonymous members, Al Qaeda supporters. ZDNet. Retrieved March 2, 2015, from http://www.zdnet.com/article/hacker-threatens-to-expose-anonymous-members-al-qaeda-supporters/#!

[60] Terry McCorkle & Billy Rios. (2011). 100 Bugs in 100 Days: An Analysis of ICS (SCADA) Software. Derbycon 2011. Retrieved from https://www.youtube.com/watch?v=pV3Dng6yo8E

[61] Terry McCorkle & Billy Rios. (n.d.). mccorkle rios - U.S.-CERT - ICS-CERT Search Results. Retrieved March 2, 2015, from https://search.usa.gov/search?utf8=%E2%9C%93&affiliate=us-cert-cs&query=mccorkle+rios

[62] Ralph Langer. (2013, November 19). Stuxnet's Secret Twin. Foreign Policy. Retrieved from http://foreignpolicy.com/2013/11/19/stuxnets-secret-twin/

[63] See for example Eric Byres, op. cit., or Nicolas Falliere, Liam O. Murchu, & Eric Chien. (2011, February). W32.Stuxnet Dossier. Symantec Security Response. Retrieved from http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf

[64] See for example Trey Herr & Paul Rosenzweig. (2015) Cyber Weapons and Export Control: Incorporating Dual Use with the PrEP Model. Journal of National Security Law & Policy. Retrieved from http://static1.squarespace.com/static/53b2efd7e4b0018990a073c4/t/54ee0bd4e4b012bd41abc2c6/1424886740160/JNSLP+v2.1+for+CSPRI+(Herr+and+Rosenzweig).pdf

[65] Gederts Gelzis. (2014, April 3) Latvia Launches Cyber Defence Unit to Beef up Online Security. DW. http://www.dw.de/latvia-launches-cyber-defence-unit-to-beef-up-online-security/a-17471936

[66] NATO Cooperative Cyber Defense Centre of Excellence. (2014, May 22). Locked Shields 2014. NATO CCDCOE. Retrieved March 2, 2015, from https://ccdcoe.org/locked-shields-2014.html

[67] Spencer Ackerman. (2013, August 6). Former NSA chief warns of cyber-terror attacks if Snowden apprehended. Retrieved March 2, 2015, from http://www.theguardian.com/technology/2013/aug/06/nsa-director-cyber-terrorism-snowden

[68] Infosecurity Magazine. (2014, July 11). 70% of Critical Infrastructure Organizations Suffered Breaches in the Last Year. Infosecurity Magazine. Retrieved March 2, 2015, from http://www.infosecurity-magazine.com/news/70-of-critical-infrastructure/

[69] *Ibid.*

[70] Heather MacKenzie. (2014, September 15). How Dragonfly Hackers and RAT Malware Threaten ICS Security. Retrieved March 2, 2015, from http://www.belden.com/blog/industrialsecurity/How-Dragonfly-Hackers-and-RAT-Malware-Threaten-ICS-Security.cfm

[71] Joel T. Langill. (2014, December 10). Defending Against the Dragonfly Cyber Security Attacks, Version 3.0. Belden. Retrieved March 2, 2015, from http://www.belden.com/docs/upload/Belden-White-Paper-Dragonfly-Cyber-Security-Attacks.pdf

[72] Katherine Brocklehurst. (2015, February 1). Cyberterrorists Attack on Critical Infrastructure Could Be Imminent. Retrieved March 2, 2015, from http://www.tripwire.com/state-of-security/security-data-protection/security-controls/cyberterrorists-attack-on-critical-infrastructure-could-be-imminent/

[73] "Phishing" is where attackers send unsolicited email to employees at a company hoping that one will open the malicious attachment or click on a malicious link, thereby infecting that computer and allowing the attackers a way into the corporate network.

[74] Die Lage der IT-Sicherheit in Deutschland 2014. (2014). Retrieved from http://www.wired.com/wp-content/uploads/2015/01/Lagebericht2014.pdf

[75] Jordan Robertson & Michael Riley. (2014, December 10). The Map That Shows Why a Pipeline Explosion in Turkey Matters to the U.S. Bloomberg Business. http://www.bloomberg.com/news/2014-12-10/the-map-that-shows-why-a-pipeline-explosion-in-turkey-matters-to-the-u-s-.html

[76] ICS-CERT. (2014, January - April). Internet Accessible Control Systems At Risk. ICS-CERT Monitor. Retrieved from https://ics-cert.us-cert.gov/sites/default/files/Monitors/ICS-CERT_Monitor_%20Jan-April2014.pdf

[77] Ibid.

[78] Cheryl Pellerin. (2014, November 21). Cybercom Chief Details U.S. Cyber Threats, Trends. DoD News, Department of Defense. Retrieved March 2, 2015, from http://www.defense.gov/news/newsarticle.aspx?id=123696

[79] Clint Boulton, & Rachael King. (2015, January 23). As Cyber Threats Soar, So Do CISO Salaries - The CIO Report - WSJ. Retrieved March 2, 2015, from http://blogs.wsj.com/cio/2015/01/23/as-cyber-threats-soar-so-do-ciso-salaries/

CHAPTER 6

Conclusions

By Samantha Ravich

Changes Since the Project Began

The conception and initial work for this project on cyber-enabled economic warfare occurred during the autumn of 2013. Since then, the situation in the U.S. has changed markedly. Cyberattacks have escalated dramatically in size, scope, and sophistication. That they pose a grave threat to the U.S. is no longer obscured or unrecognized. The private sector continues to ramp up investment in, and attention to, cybersecurity—one insider estimate is that private spending on cybersecurity exceeded $67 billion in 2014.[1] Neither is the U.S. government's response any longer half-hearted or lethargic. On the contrary, the plethora of new inquiries, plans, and initiatives taken up across numerous government bodies is beginning to look almost frenetic. Clearly cybersecurity has moved to center stage in American consciousness, galvanized in no small part by last November's North Korean-sponsored cyberattack on Sony Pictures:[2]

> In last year's [2014's] M-Trends we noted that cybersecurity had gone from a niche IT issue to a boardroom priority. This year, cybersecurity (or perhaps more accurately, cyber insecurity) entered the mainstream. In the first few weeks of 2015 alone, the issue was a pillar of the U.S. president's State of the Union address, the plot of a big-budget film, and the opening punchline of Hollywood's Golden Globe awards broadcast.[3]

As work on this research has proceeded during the past 18 months, facts on the ground have seemed to accelerate. Consequently, following the completion of the five research papers published in this monograph, it is useful to pause here to reflect on the big picture. How is the situation evolving? What has this research endeavor found? What more is needed, and what are the next steps?

Escalating Attacks, Threats and Hostile Disclosures

Virtually no-one disputes that cyberattacks throughout the government and private sectors have continued to increase dramatically during the past two years in "frequency, scale, sophistication, and severity of impact."[4] Already by 2011, more than half of CEOs from large companies surveyed by the Ponemon Institute stated that their companies had been subjected to cyberattacks that year "either daily or hourly."[5] In November, 2014, Michael McCaul, chairman of the House Committee on Homeland Security, stated, "In 2013, U.S.-CERT responded to a total of 228,700 cyber incidents involving federal agencies, companies that run critical

infrastructure and contract partners. That's more than double the incidents in 2009."[6] For the private sector, Symantec has reported that: "the number of breaches increased by 62% in 2013 with a total of over 552 million identities compromised. Additionally, targeted attacks grew by 91% and are increasingly aimed at small businesses."[7] The Ponemon Institute found that in 2014 the average cost of cybercrime per company in the U.S. rose by close to 10% overall and in the retail sector more than doubled from 2013 to an annual average of $8.6 million per company in 2014.[8]

Radware Inc, another leading cybersecurity firm that conducts an annual survey of cyberattacks, stated recently that, "2014 was a watershed year for the security industry… Cyberattacks reached a tipping point in terms of quantity, length, complexity and targets."[9] And yet another prominent cybersecurity vendor, FireEye, noted in late 2014, "It doesn't matter what types of firewall, intrusion prevention system (IPS), Web gateway, sandbox and endpoint systems make up organizations' Maginot Line; attackers are circumventing them all."[10] The same report later stated, "The implication is clear: no corner of the world is remote enough to avoid falling into attackers' crosshairs, and current defenses are stopping virtually none of them."[11]

In Tokyo, the National Institute of Information and Communications Technology (NICT) issued an astounding statement on February 17, 2015:

> More than 25 billion cyberattacks on the Japanese government and other bodies were logged in 2014, an agency said Tuesday (Feb 17), with 40 per cent of them traced to China. The NICT, which has a network of a quarter of a million sensors, said there were 25.66 billion attempts to compromise systems, according to a report by Kyodo News… The survey was first carried out in 2005, when it recorded just 310 million attempts to breach security.[12]

Finally, a September 2014 survey from the Ponemon Institute showed that,

> …while many companies have made some positive changes on the security front, their governance and overall data-breach preparedness continue to lag. Companies continued to have trouble in areas like data breach response, risk assessments, network anomaly detection, and continuous network monitoring.[13]

To provide a more fine-grained feel for how the cyber threat landscape has been heating up, we briefly review several of the more prominent successful cyberattacks that have occurred during the past 18 months, first with examples from the private sector and then in the government sector. We conclude this section with a brief examination of some especially damaging disclosures by certain hostile insiders and their relevance for understanding current cyber enabled economic warfare threats.

Major Cyberattacks on Business

Target, Supervalu, and UPS. In January, 2014, Target announced that hackers had breached their payment system and exfiltrated personal information on an estimated 110 million accounts. The attack occurred from November 27 to December 5, 2013.[14] It cost Target $148 million in losses and $61 million in new cybersecurity technology; caused substantial harm to Target's reputation and stock price; subjected the firm to numerous lawsuits from affected customers; forced the resignations of Target's CEO and CIO; and cost interdependent financial institutions approximately $200 million.[15] The attack compromised personal information on 70 million customers and approximately 40 million credit cards "by using software that may have cost less than $2,500 at an online marketplace."[16] It was later discovered that the hackers apparently operated from Eastern Europe.[17] As bad as the initial revelations were, subsequent reports showed that the damage was actually much more substantial than was first disclosed:

> More than 1,000 U.S. businesses have been affected by the cyberattack that hit the in-store cash register systems at Target, Supervalu, and most recently UPS Stores. The attacks are much more pervasive than previously reported, and hackers are pilfering the data of millions of payment cards from U.S. consumers without companies knowing about it, according to a new Department of Homeland Security advisory released Friday afternoon [Aug. 22, 2014]."[18]

eBay. In May 2014, eBay issued a request for *all* of its users to change their passwords.[19] The online retailer disclosed that cyberattacks in late February and early March had compromised a database containing eBay employee passwords, enabling hackers to gain access to the company's corporate network. That database contained "eBay customers' name, password, email address, physical address, phone number and date of birth"[20]—for 233 million customers.

JPMorgan Chase. In mid-2014, JPMorgan Chase issued a shocking announcement: their systems had been severely breached, compromising more than 83 million accounts involving 76 million households (approximately two out of three households in the U.S.) and 7 million small businesses.[21] The attackers successfully operated inside JPMorgan's system for several months before they were detected. The attack also targeted nine other major financial institutions.[22] Some experts assert that a group of Russian criminals are responsible for the attack.[23] "However, the origin of the attack is still far from settled, though the FBI officially ruled out the Russian government as a perpetrator."[24] As of October 9, 2014, the only other company believed to have had data stolen in the same attack is Fidelity Investments, though investigators reported that the attackers attempted to infiltrate the networks of banks and financial companies such as Citigroup, HSBC Holdings, E*Trade, Regions Financial Corporation and payroll-service firm Automatic Data Processing (ADP).[25]

420,000 Assorted Websites. Almost unbelievably, a single Russian criminal group managed to hack 420,000 websites and steal 1.2 billion user names and passwords as well as more than 500 million email addresses.[26] Hold Security, a Milwaukee security firm, discovered the group's haul, which ranged indiscriminately across companies of virtually all sizes, from Fortune 500 to very small websites.

Home Depot. In September, 2014, Home Depot confirmed it had become another major retail victim and that its payment system had been hacked, compromising an estimated 56 million credit cards in a five month long attack on its payment terminals.[27] This meant the breach had been bigger, in terms of credit cards compromised, than the holiday 2013 attack at Target Corp. "Each of the attacks was the result of software that had been slipped into the companies' networks and used to skim payment-card data."[28]

Sony Pictures Entertainment. In an already infamous incident widely considered "one of the worst cyberattacks ever" on a company operating in the U.S.,[29] a team of hackers who called themselves the Guardians of Peace completed a devastating multi-dimensional cyberattack against Japanese entertainment giant Sony Pictures during late November, 2014. Numerous U.S. officials have stated that the hackers are affiliated with the government of North Korea.[30] The initial breach on November 24 forced the shutdown of the company's entire computer network. The hackers stole more than 100 terabytes of data – "a breach so massive technology experts said it will take Sony more than a year to analyze exactly what's been released into the wild."[31] In short order, they posted approximately 40 gigabytes of stolen data to an internet file sharing site, including a horde of documents on the company's business dealings. Eventually they posted at least five of Sony's unreleased films, and a substantial amount of personal data on Sony employees.[32] They also drew attention to their postings by, among other things, sending email alerts to reporters and others who had shown interest in searching the Sony files.[33]

> 'This attack signifies a lot of resources went into the breach and it increases difficulty for the defender to discover whether there will be more to come,' said Fengmin Gong, the Santa Clara, California-based co-founder and chief strategy officer for information technology security firm Cyphort Inc. 'This is most challenging (for companies). The threat landscape is changing.'[34]

Anthem, Inc. The nation's second largest health insurer, Anthem, Inc., was breached during December 2014 and January 2015, during which time records with personal data for more than 78 million people were illicitly accessed.[35] "The compromised information includes Social Security numbers, names, employment information, addresses, phone numbers, email addresses, dates of birth and member IDs… That means that for the rest of their lives, millions of Americans may have to take precautions to keep their finances safe from criminals."[36] News reports indicate the FBI believes it is close to finding the hackers responsible.[37] Some reports indicate that a Chinese government hacker group known as "Deep Panda" committed the breach.[38] Medical and health care breaches accounted for 43% of data breaches in 2014, according to the Identity Theft Resource Center—the third year the sector logged the highest proportion of compromises.[39]

TurboTax. In early February, 2015, Intuit announced that its subsidiary TurboTax was suspending e-filing all state tax returns for 24 hours because of mounting incidents of fraudulent filings for refunds. Initial appearances indicate that the company itself was not breached, but that criminals were using TurboTax software to file fraudulent claims and, in effect, steal refunds using stolen identity data obtained elsewhere.[40] Since then, TurboTax has resumed processing state tax returns and implemented additional security;[41] more than two dozen states have experienced problems this year with fraudulent filings for returns.[42]

Premera Blue Cross. Yet another health insurance company, Premera Blue Cross, announced on March 15 that it was the victim of a sophisticated cyberattack. Premera acknowledged that hackers gained access to the personal information of approximately 11 million consumers. The company, a not-for-profit based in Washington State, indicated that the breach originally occurred on May 5, 2014 but was not detected until January 29.[43] According to a March 17 letter from Premera to its affected customers and applicants, the prolonged hack exposed individuals' records that included "name, address, telephone number, date of birth, Social Security number, member identification number, email address … and claims information, including clinical information."[44] Some news reports state additionally that customers' "bank account information" may also have been stolen.[45] Many are increasingly worried about how such data may be abused in the future.

> Those that hacked into Premera's systems have all they need to 'get loans, commit tax fraud, medical identity theft, child identity theft (assuming children were part of the covered community), synthetic identity theft and criminal identity theft,' Adam Levin, chairman and co-founder of Credit.com, said in an email. 'Depending upon what clinical information they got, they have an opportunity to commit blackmail and extortion,' added Levin, the former director of the New Jersey Division of Consumer Affairs. 'Premera customers will be forced to look over their shoulders for the rest of their lives.'[46]

Although these nine examples comprise just a few of the most successful among the millions of cyberattacks on corporations that have occurred in the U.S. since late 2013, they do provide a sense of how the threat of cyberattacks to various portions of the U.S. economy is growing in scope, complexity, and seriousness. The government sector has also been affected by the growing severity of cyberattacks, as the following examples illustrate.

Noteworthy Recent Cyberattacks on Government

U.S. Navy Marine Corps. "In September of 2013, Iranian hackers breached the unclassified network used by the Department of the Navy to host websites and store non-sensitive information and communications. Many details of the attack remain classified, but hackers were able to enter the 'bloodstream' of the Navy's unclassified network and conduct surveillance on the system. There is no evidence that any data were stolen, but it took about four months to fully purge the hackers from the system. One senior U.S. official told *The Wall Street Journal* that the attack 'was a real big deal.... It was a significant penetration that showed a weakness in the system.'"[47]

Office of Personnel Management. During March of 2014, Chinese hackers breached the computer systems of the OPM, the U.S. government agency with personnel records on all federal employees. The *New York Times* reported that they "appeared to be targeting the files on tens of thousands of employees who have applied for top-secret security clearances."[48] It is unknown publicly whether any personal information was stolen, but the risk of serious abuse if any such theft did occur is obvious.

NATO. On March 15, 2014, a pro-Russia hacktivist group using a DDoS (distributed denial of service) attack succeeded in temporarily crashing "several" public NATO websites.[49] These included NATO's main public website (nato.int), an affiliated one in Tallinn, Estonia (ccdcoe.org), and NATO's Parliamentary Assembly (nato-pa.int).[50] The attacks also targeted NATO's unclassified email network. A group calling itself "Cyber Berkut" (KiberBerkut) claimed responsibility for the attacks in retaliation for alleged NATO interference in Ukraine. Members are believed to be staunch supporters of former Ukrainian President Victor Yanukovich.[51] Journalists noted:

> Tensions between Moscow and the West have been rising steadily since Russia intervened following the ouster of Yanukovich. Ukrainian and Russian websites have both been targets for cyberattacks in recent weeks but this appeared the first major attack on a Western website since the crisis began.[52]

Department of Homeland Security Contractor. The DHS acknowledged on August 8, 2014, that an undisclosed amount and type of DHS employee information was stolen by hackers. The attack targeted two contractors, U.S. Investigations Services (USIS) and KeyPoint Government Solutions, which conduct personnel investigations on behalf of many agencies, including the OPM.[53] Experts who have reviewed the facts gathered to date believe it has all the markings of a state-sponsored attack.[54]

White House. In late October 2014, White House officials disclosed that they had learned from "an ally" that hackers had breached the unclassified White House computer network over a period of at least a few weeks. The *Washington Post* reported that the hackers were "thought to be working for the Russian government."[55] The attacks interfered with the unclassified network used by employees of the Executive Office of the President but apparently did not damage or hack any of the classified systems. Officials from the NSA, Secret Service, and FBI investigated. According to the Post's sources, "the nature of the target is consistent with a state-sponsored campaign."[56]

U.S. Postal Service. On November 10, 2014, the U.S. Postal Service reported that their computer networks had been breached, compromising the data of the postmaster general and approximately 800,000 other employees. The *Washington Post* reported that Chinese government hackers were likely responsible.[57] The intrusion into the USPS, officials said, was carried out by a sophisticated actor who did not appear to be interested in identity theft or credit card fraud. In the same story, the *Post* also noted that, "China has been tied to several recent intrusions, including one into the computer systems of the Office of Personnel Management and

another into the systems of a government contractor, USIS, that conducts security-clearance checks."

U.S. State Department. In mid-November, 2014, State Department officials revealed that unclassified networks for handling non-classified emails had been breached weeks earlier. A State Department spokesman said that the origin of the cyber breach was unknown and under investigation. State Department officials also said it appeared the hack was linked to a somewhat similar breach, in October 2014, of the White House's unclassified computer network.[58] The *Washington Post* previously has quoted sources indicating that hackers working for the Russian government likely were responsible for the White House breach.[59]

U.S. CENTCOM. Islamic State sympathizers hacked the U.S. military's Central Command Twitter and YouTube accounts and posted ISIS propaganda, including: "AMERICAN SOLDIERS, WE ARE COMING, WATCH YOUR BACKS. ISIS."[60] The breach did not involve Defense Department secure computers, accounts or data, and thus was deemed by CENTCOM to be "cybervandalism." British news sources have indicated the hacker was a known sympathizer of ISIS.[61] The main concern in the CENTCOM breach is not so much the direct damage done to CENTCOM information technology or data, or even the propaganda gains the hack produced for ISIS, although the latter are real. Rather, it is the escalation of the use of cyber capabilities by a deadly, well-funded, and determined terrorist group to a new, albeit rather rudimentary, dimension of offensive cyberwar well beyond previous recruiting and fund raising functions. The real concern would be if this proves to have been an initial step toward the development of much more sophisticated offensive cyber capabilities, threats, and attacks. With the cyberattack tools that are readily available in black markets, and with the deep pockets ISIS has to purchase such tools and capabilities, ISIS's development of offensive cyberwarfare skills is fast becoming a question of vision and strategy, not of capability.

Department of Defense. In February 2015, the director of the Defense Intelligence Agency, Marine Corps Lieutenant General Vincent Stewart, provided testimony to the House Armed Services Committee warning that global cyber threats are increasing and pose a risk to U.S. defense networks:

> Threat actors now demonstrate an increased ability and willingness to conduct aggressive cyberspace operations—including both service disruptions and espionage—against U.S. and allied defense information networks… For 2015, we expect espionage against U.S. government defense and defense contractor networks to continue largely unabated, while destructive network attack capabilities continue to develop and proliferate worldwide… Threat actors increasingly are willing to incorporate cyber options into regional and global power projection capabilities… In response, states worldwide are forming "cyber command" organizations and developing national capabilities… Iran and North Korea now consider disruptive and destructive cyberspace operations a valid instrument of statecraft, including during what the U.S. considers peacetime…[62]

The first set of cases reviewed above involves successful cyberattacks on corporations; those cases fit rather obviously with the concerns raised in this project about the evolving possibilities and dangers of cyber-enabled economic warfare. For the second set of examples, which are focused on cyberattacks in the government sector, the connection to *economic* warfare is perhaps not so readily apparent. These cases and others like them do not principally involve economic assets and do not seem to pose direct threats to the U.S. economy. Upon reflection, however, the growing wave of cyberattacks upon government entities raises critical concerns for this project on cyber-enabled economic warfare. We take those up in the final section of this chapter.

Hostile Insider Disclosures

In addition to these and myriad other similar corporate and government cyberattacks (the vast majority of which are unsuccessful), there is another category of hacks worth reviewing: hostile insider disclosures. Research on cyberespionage, cyber fraud, cyber IP piracy, and other forms of cybercrime consistently show that disgruntled employees, laid-off workers, and dishonest business partners often play a critical role in such activity.[63] Thousands of these insider attack cases occur each year, and only a relative few are either prosecuted or publicly revealed. Much of the activity is cyber-enabled in one form or another, as information increasingly is stored and transferred via computing and communications technologies and networks. The FBI and Department of Homeland Security recently issued a public warning that this insider threat is increasing:

> There has been an increase in computer network exploitation and disruption by disgruntled and/or former employees. The FBI and DHS assess that disgruntled and former employees pose a significant cyber threat to U.S. businesses due to their authorized access to sensitive information and the networks businesses rely on.[64]

DIA Director Vincent Stewart provided a similar warning in his testimony in early February before the House Armed Services Committee: "Trusted insiders who disclose sensitive U.S. information for nefarious purposes will also remain a significant threat in 2015. The technical sophistication of this insider threat exacerbates the challenge."[65]

For this project, there is one hostile insider whose cyber-enabled attacks on the U.S. Intelligence community have been especially damaging: Edward Snowden. His theft and ongoing public disclosure of massive amounts of classified U.S. intelligence information have been widely covered in the media and with the exception of two points that have direct implications for this project, will not be recounted. First, the Snowden leaks have in general caused grave harm to the reputation of U.S. intelligence agencies—especially the NSA—and have thereby made the government's task of winning cooperation from the private sector on cybersecurity initiatives much more difficult:

> Privacy advocates are also wary about information-sharing, having warned for years that giving the government more doors through which to access user information could expand its surveillance capabilities—a refrain that has only grown louder since the Edward Snowden disclosures. Many groups have said they will not support any information-sharing legislation if Congress does not first reform the National Security Agency's domestic spying authority.[66]

Second, a number of the stolen documents that Snowden has disclosed have revealed information about classified U.S. cyber operational capabilities and initiatives that make it more difficult for U.S. agencies to conduct the work they need to do in order to protect Americans and their allies from cyber threats.[67] Many of these disclosures also have encouraged U.S. adversaries to justify, and in some cases even increase, their own cyber plans and capabilities. We offer but two of many possible representative examples. The first shows how the Chinese have used Snowden's disclosures to defend their extensive cyber espionage and IP piracy:

> Computer intrusions have been a major source of discussion and disagreement between the two countries, and the Chinese can point to evidence, revealed by Edward J. Snowden, that the National Security Agency went deep into the computer systems of Huawei, a major maker of computer network equipment, and ran many programs to intercept the conversations of Chinese leaders and the military.[68]

The second Snowden fallout example is a *Washington Post* article about the U.S.'s purported "offensive cyber-operations" that is likely to compromise U.S. cyber intelligence methods and encourage U.S. adversaries to consider ratcheting up their cyberattacks on U.S. targets:

> U.S. intelligence services carried out 231 offensive cyber-operations in 2011, the leading edge of a clandestine campaign that embraces the Internet as a theater of spying, sabotage and war, according to top-secret documents obtained by *The Washington Post*. That disclosure, in a classified intelligence budget provided by NSA leaker Edward Snowden, provides new evidence that the Obama administration's growing ranks of cyberwarriors infiltrate and disrupt foreign computer networks. Additionally, under an extensive effort code-named GENIE, U.S. computer specialists break into foreign networks so that they can be put under surreptitious U.S. control. Budget documents say the $652 million project has placed 'covert implants,' sophisticated malware transmitted from far away, in computers, routers and firewalls on tens of thousands of machines every year, with plans to expand those numbers into the millions. Of the 231 offensive operations conducted in 2011, the budget said, nearly three-quarters were against top-priority targets, which former officials say includes adversaries such as Iran, Russia, China and North Korea and activities such as nuclear proliferation. The document provided few other details about the operations.[69]

To sum up this section, both the private and government sectors have experienced continued escalation of cyberattacks from a variety of state and non-state actors, including hostile insiders. The cyber threat landscape is rapidly shifting and both the U.S. private and government sectors are having difficulty keeping up. These are the facts on the ground that help underscore the need to improve understanding of what cyber-enabled economic warfare contributes to the problem. They also help illuminate why it is so important that both the private and government sectors find far more effective strategies to combat the threat:

> As these results show, today's attackers have evolved their tactics from just a few years ago. Broad, opportunistic, scattershot attacks designed for mischief have been eclipsed by sophisticated attacks that are advanced, targeted, stealthy, and persistent. This new generation of attacks includes high-end cybercrime and state-sponsored campaigns known as advanced persistent threat (APT) attacks.[70]

> Criminals are developing new tools that are more sophisticated and more intuitive than previous generations, and then selling them in online marketplaces. This reality is lowering the barriers to network entry and giving more malicious actors the capability to threaten critical systems, in both the private and public sectors.[71]

Lessons from the Five Chapters

We initiated this project to investigate whether the U.S. is at serious risk of being blindsided by what we term cyber-enabled economic warfare. The chapter authors have completed their research and discussed it with numerous other experts who participated in the Hudson Institute Seminar in November. No one doubts that the United States in general has greatly increased its awareness of very serious threats posed by a wide variety of ongoing and potential cyberattacks. It is also evident that the U.S. private and public sectors are well in motion to develop and implement a broad range of intended improvements to U.S. cybersecurity. These are very positive and encouraging steps. There is also consensus that the U.S. has not yet gone far enough, and that both private and government actors have not caught up to, much less gotten ahead of, the capabilities and tactics of various cyber threat actors. Beyond this consensus, however, we remain deeply concerned that the U.S. response is fundamentally inadequate and, in some vital respects, simply askew. Four concerns stand out as particularly urgent:

1. Recognize that cyber-enabled economic warfare is happening and that the U.S. is not prepared for it. It is readily apparent that both the private and government sectors are devoting a considerable amount of attention, resources and action to improving defenses against cyberattacks from state- and non-state-threat actors. Yet so far there seems to be substantial fragmentation of understandings of what the heart of the problem is. Analysts often seem to view the phenomenon through whatever lens seems best to fit that part of it with which they are most familiar. Most of the attention has focused pragmatically on various forms or applications of cyberattacks; alternatively a considerable amount of attention also addresses more dire conceptions of cyberwarfare and/or cyberterrorism.

Academics sometimes have a tendency to get bogged down in definitional disputes and semantics, and certainly no one involved in this project is interested in recommendations that produce that outcome. But it is necessary to recognize that there are real differences between cyberattacks in general, cyberwarfare (which easily can be, and often is, understood as an analogue to, or new type of, traditional kinetic warfare), cyberterrorism, and cyber-enabled economic warfare (which can occur either in peacetime with no connection to kinetic war, or as a prelude to kinetic war, or in conjunction with it). There is an abundance of literature, research, and policy analysis on each of the first three categories—Google any of them and a wealth of sources is immediately available. But there is almost no literature or policy discussion of cyber-enabled economic warfare. And it is not simply because the term is itself awkward or that the substantive issues are readily addressed under a different label. Rather, there simply is little recognition that cyber-enabled economic warfare even exists, much less that it is already prevalent and rapidly growing.

When criminals independently use cyber-enabled means to engage in cybercrimes such as identity theft, credit card fraud, tax refund fraud, fraudulent bank account fund transfers, data theft, or intellectual property piracy simply for the illicit financial gains they produce, such activity does not constitute economic warfare. When hacktivists independently use cyber-enabled means to vandalize a target for political or personal motives, this does not constitute economic warfare. When terrorists independently use cyber-enabled means to communicate, plan, recruit, disseminate propaganda, or raise funds, this does not constitute economic warfare. And when states use cyber-enabled means to spy on other states, this is not economic warfare either.

However, it may well constitute cyber-enabled economic warfare when gangs of criminals are supported by a state to use cyber-enabled means to engage in economic crimes that weaken an adversarial state's economy. Or when groups of hacktivists are supported by a state to engage in campaigns using cyber-enabled means to disrupt key economic institutions within an adversary's economy in order to weaken it. Or when terrorist groups, either independently or with state support, use cyber-enabled means to sabotage critical infrastructure within an adversary's economy in order to weaken it. Or when state entities themselves use cyber-enabled means (such as massive cyber theft) to implement strategies designed to weaken an adversary's economy. All these circumstances need to be analyzed as such.

Of course the point here is that all of these scenarios, as well as others like them, are in fact either occurring already, or could soon occur, with the U.S. and its allies as targets. Yet almost no one is analyzing events or threats in these terms. As Dubowitz and Fixler note in their chapter: "Based on our discussions with government officials and private sector experts, neither the U.S. government nor the private sector has engaged in serious planning about how to protect America and its allies against economic warfare." A big part of the problem, it seems, is that there is little tradition of framing the problem in these terms, and thus a paucity of intellectual tools for conducting the analyses that are needed. As a result, the U.S. is not prepared to address these threats, and is therefore vulnerable.

2. Understand the Transition from Traditional to Cyber-Enabled Economic Warfare. We recognize that traditional means of conducting economic warfare have long existed. Examples include trade embargoes, blacklists, blockades, sanctions, tariff and/or quota discrimination, sabotage of economic targets, preclusive purchase of scarce critical resources, freezing of capital assets, counterfeiting, restrictions on investment and other capital flows, and expropriation. These practices are all well established, and a considerable body of literature exists on them as well. Moreover, the U.S. has extensive experience with traditional economic warfare, both defensively and offensively. One need look no further than the middle of last century to find rich examples of that history. Prior to World War II, the U.S. created a national economic warfare bureaucracy[72] and used economic warfare strategies extensively against Japan.[73] After the War, the U.S.'s and Soviet Union's Cold War lasted more than forty years and swept the entire world into a global economic war, which the U.S. won handily.[74] After the Cold War ended, the U.S. continued to use traditional economic warfare strategies to nurture and reward strategic allies[75] as well as to punish foes, whether state or non-state actors.[76]

It seems strange, therefore, that there is so little use of this experience in formulating policy for the contemporary conduct of cyber-enabled economic warfare. Few U.S. policy analysts seem to study the U.S. experience with traditional economic warfare to see what lessons can be drawn for understanding cyber-enabled economic warfare today. (The Treasury Department's smart sanctions program reviewed in the opening chapter here by Dubowitz and Fixler has been a notable exception, as is Zarate's excellent 2013 book on the same subject.[77]) It seems as well that the U.S. government does not possess the capability to address holistically the topic of contemporary, cyber-enabled economic warfare, much less to analyze its fundamental dynamic.

Quite simply, cyber-enabled economic warfare is escalating rapidly because cyber-enabled opportunities for conducting it are evolving so rapidly. Both the U.S. and its adversaries are responding to, and also shaping as a result of their choices, those opportunities. Additionally, the U.S. policy analysis community seems to lack a clear awareness that adversaries' strategies for capitalizing on the changing opportunity set will vary by adversaries' individual circumstances and characteristics. China, Russia, Iran, North Korea, Syria, etc., all have different characteristics that will drive their own choices. The same is of course also true for all the relevant non-state actors and for the interactions that are developing across these state and non-state categories. So far there seems to be very limited capacity for U.S. government understanding of these issues, and therefore no sound basis for adequate, properly coordinated response to them. We believe this needs to change.

This is an extremely important subject. Changed possibilities almost inevitably lead to changes in practice, and if the U.S. is to prepare for the latter, it would help greatly to understand the former.

3. Stop Ignoring U.S. Offensive Cyber-Enabled Economic Warfare Initiatives. This blind spot to lessons from our own history is made worse by the difficulty U.S. government officials have in describing accurately the U.S.'s own *offensive* cyber-enabled economic warfare initiatives that reportedly have been underway at least since the late 1990s,[78] and perhaps even well back into the Cold War.[79] Government officials who are knowledgeable about the programs cannot discuss them publicly in any depth because they are classified and highly sensitive. Additionally, public discussion may compromise means and methods and thus damage very valuable programs and capabilities, as seems to have happened following some of Snowden's unlawful disclosures about these programs. On the other hand, non-government individuals generally cannot discuss them accurately because they are not privy to the details and thus have limited insights into them.

We do not mean to imply that there has been no informed discussion of the U.S.'s offensive cyberwarfare and cyber-enabled economic warfare capabilities and initiatives. Certainly there has been significant authorized government acknowledgement of U.S. offensive cyberwarfare capabilities at least since 2013, perhaps beginning with the public statements of former Defense Secretary Leon Panetta and former NSA Director and Commander of U.S. Cyber Command General Keith Alexander.[80] There has also been a significant amount of journalistic coverage of these issues in the past three years, particularly following the discovery of the Stuxnet malware and the extensive Snowden leaks.[81] Nonetheless these revelations have been limited, as exceptions, and the public discourse about the topic has been shrouded in mystery and speculation.

The relative paucity of public discussion of U.S. offensive cyber capabilities, particularly to conduct *economic* warfare, is damaging to U.S. interests in two main respects. First, it presents an obstacle to generating a robust public debate on policy, guidelines, and doctrine for the use of said capabilities. Without that debate, the public cannot be well informed, which is damaging to U.S. democracy, and the policies that are formulated are likely to be much weaker than otherwise would be the case. The risk of a "groupthink" effect rises considerably, and the likelihood of eventually incurring harm from unanticipated blowback increases substantially as well.

Second, being unable to discuss U.S. offensive cyber capabilities leads to a debilitating incapacity to understand how our adversaries are responding to U.S. offensive initiatives, or how they perceive the threats we pose to them. The chapters in this monograph produced by Zarate and by Dubowitz and Fixler are exceptions, and doubtless there are others as well.[82] But clearly these are the exceptions, not the norm. If the U.S. policymaking community cannot discuss and properly assess how various adversaries perceive the threat U.S. offensive cyber initiatives pose to them, it seems very unlikely its members will understand or anticipate adversaries' responses to those initiatives. This would seem to be a foundational aspect for a sound assessment of cyber threats, yet it appears that little is being done to address this part of the problem.

4. Address Specific Opportunities to Improve. In addition to the three problems just outlined, we have identified four main opportunities for the U.S. government to improve its capabilities for addressing cyber-enabled economic warfare threats:

History: We have noted above that the U.S. needs to do a better job of learning from its own experience with both offensive and defensive dimensions of economic warfare, as well as deepen its understanding of how traditional economic warfare is being overtaken by cyber-enabled economic warfare. Here we go one step further and note that the broader global history of economic warfare offers a bedrock of cases that seems almost entirely ignored in today's cyber policy debates. The last two centuries in particular contain abundant examples of countries pursuing economic warfare strategies, in a variety of circumstances, and with varying degrees of success. Michael Hsieh's chapter in this monograph is a perfect example of how economic warfare lessons from prior campaigns can provide valuable insights into today's challenges. Somewhere in the U.S. government (perhaps in the War Colleges), some group of suitably trained experts should be tasked with creating a rich base of lessons to be gleaned from this history and disseminated to policymakers in appropriate fashion. Yet one would be hard pressed to find much discussion of such lessons or the underlying cases in U.S. policy debates about how to enhance U.S. cybersecurity.[83] For example, the U.S. government today seems to have almost no knowledge of the economic warfare operations that the British and the U.S. pursued during WWI and especially WWII—when both countries had important central government economic warfare bureaucracies, plans, strategies and initiatives.[84]

Doctrine: During the Hudson Seminar discussions in November, most participants agreed that the U.S. needs to do more to develop doctrine for cyber-enabled economic warfare specifically as well as for economic warfare more generally. The need is especially acute for the U.S.'s offensive dimensions of the problem. The Department of Defense and U.S. Cyber Command seem to be pushing in this direction for establishing doctrine specifically for *cyberwarfare*.[85] We believe the need extends outside the Department of Defense to civilian applications as well. We also contend that the focus on cyberwarfare only is improperly restrictive and limiting: doctrine should be extended specifically to cyber-enabled economic warfare as well, and cyber-enabled economic warfare should be viewed as a component within a broader doctrine of more general offensive and defensive economic warfare (see Dubowitz and Fixler's excellent discussion of this problem in chapter 1). In chapter 2 of this monograph, Abe Shulsky offers a discussion of comparisons of cyber-enabled economic warfare to nuclear warfare and raises doctrinal implications; it is illustrative of the type of analysis we recommend here.

Applying our previous points about learning from relevant history, we note one illustrative example here drawn from World War II. After the Japanese attack on Pearl Harbor, the U.S. created a series of wartime economic planning bureaucracies to manage critical economic planning, production, and procurement functions needed for the war effort.[86] One small but important office within these bureaucracies was the Enemy Objectives Unit, located in London within the Economic Warfare Division of the U.S. Embassy. From mid-1942 through early 1945, the EOU was tasked with guiding the selection of targets for the U.S.'s strategic bombing campaign on German targets—a vital offensive economic warfare function.

> To put no fine point upon it, the U.S. had committed itself to a massive daylight precision-bombing program without developing the doctrine and techniques of target selection or the intelligence required to underpin the exercise or without perceiving initially what it would require to conduct precision-bombing operations against the opposition of the German single-engined fighter force…[87]

From what we have seen, this could also serve as an accurate assessment of the state of preparation in the U.S. today for conducting cyber-enabled economic warfare: the U.S. has undertaken a large and vital commitment to conducting offensive and defensive cyber-enabled economic warfare, without adequately "developing the doctrine and techniques of target selection or the intelligence required to underpin the exercise or without perceiving initially what it would require to conduct precision… operations" against U.S. adversaries. It is instructive to take the historical comparison one step further:

> In the doctrine we evolved, we sought target systems where the destruction of the minimum number of targets would have the greatest, most prompt, and most long-lasting direct military effect on the battlefield. Each of the modifiers carried weight. One had to ask, in assessing the results of an attack, how large its effect would be within its own sector of the economy or military system; how quickly would the effect be felt in front line strength; how long the effect would last; and what its direct military, as opposed to economic, consequences would be. The application of these criteria was serious, rigorous intellectual business. In part, it required taking fully into account the extent to which the military effect of an attack could be cushioned by the Germans by diverting civilian output or services to military purposes or buying time for repair by drawing down stocks of finished products in the pipeline. In all this, our knowledge as economists of the structure of production, buttressed by what we had learned from the aiming-point reports, converged with the classic military principles Hughes and his best senior colleagues brought to the task.[88]

We wonder, which part(s) of the U.S. cyber protection system possesses both the authority and the capacity to produce this type of analysis and doctrine for the analogous strategic functions needed for the U.S.'s conduct of offensive and defensive cyber-enabled economic warfare?

Capabilities and Organization: We consider it likely that at a minimum China, Russia, Iran, and to a lesser extent North Korea are all pursuing alternative versions of cyber-enabled economic warfare strategies against the U.S. in order to degrade U.S. economic strength and thereby eventually weaken U.S. security. We agree with FBI Director Comey and others that it is likely that some non-state actors are also developing similar ambitions,[89] either independently or in conjunction with state supporters. Many have argued that Bin Laden and Al Qaeda already have been pursuing an asymmetric version of traditional economic warfare against the U.S. with significant success, so the step from that to inclusion of cyber-enabled dimensions seems at least plausible and perhaps likely.[90] And we note that hardly anyone in the U.S. policymaking community is attending to precisely these issues (i.e., cyber-enabled economic warfare against the U.S.), with the result that the U.S. is vulnerable to these strategies.

If we are correct, the U.S. needs to add to its cyber defense capabilities. We need specialists who understand these economic warfare issues and can conduct expert analyses of them (just as the EOU needed suitable specialists and new analytic methods in the WWII strategic bombing example cited above). This means that someone needs to determine exactly what kinds of expertise are needed, and what types of training will help produce them. For example, in line with our earlier recommendations, it seems that certain types of era-specific historians, economic historians, economists, and political scientists, among others, all could help generate a valuable body of lessons learned from relevant historical events. Additionally, someone needs to determine where to locate those individuals within the multitude of organizations that currently share responsibilities for U.S. cybersecurity. Should they be widely distributed across numerous, or at least the principal, U.S. cybersecurity agencies? Should there be a concentrated team of these individuals working within one entity so as to deepen their insights and strengthen their recommendations? If so, which agency? These are questions that require further study and debate (see Dubowitz's and Fixler's recommendations in Chapter 1 for a good start on this discussion).

Deterrence: One idea that has risen clearly from this project's research is the recognition that the U.S. currently does not possess an effective method or plan to deter cyber threats in general, or cyber-enabled economic warfare in particular. This is a weakness that is acknowledged by at least some top U.S. officials responsible for cybersecurity. DNI Director James Clapper analyzed the problem concisely in his recent testimony to the Senate Armed Services Committee:

> Numerous actors remain undeterred from conducting economic cyber espionage or perpetrating cyberattacks. The absence of universally accepted and enforceable norms of behavior in cyberspace has contributed to this situation. The motivation to conduct cyberattacks and cyber espionage will probably remain strong because of the relative ease of these operations and the gains they bring to the perpetrators. The result is a cyber environment in which multiple actors continue to test their adversaries' technical capabilities, political resolve, and thresholds. The muted response by most victims to cyberattacks has created a permissive environment in which low-level attacks can be used as a coercive tool short of war, with relatively low risk of retaliation. Additionally, even when a cyberattack can be attributed to a specific actor, the forensic attribution often requires a significant amount of time to complete. Long delays between the cyberattack and determination of attribution likewise reinforce a permissive environment.[91]

It appears that at least some other senior officials share this concern and are prepared to try to do something about it. Admiral Michael Rogers, head of both the NSA and U.S. Cyber Command, provided public statements about the problem in March in testimony to the Senate Armed Services Committee.[92] Pressed to explain how the U.S. could deter cyberattacks:

> Admiral Rogers said that erecting ever-higher digital fences would never be enough, and that 'we have got to broaden our capabilities to provide policy makers and operational commanders with a broader range of options. Because in the end, a purely defensive reactive strategy will be both late' and would become 'incredibly resource-intense.... So, I have been an advocate of, we also need to think about how can we increase our capacity on the offensive side here, to get to that point of deterrence.'
>
> ... The committee chairman, Senator John McCain of Arizona, who has argued for a robust offensive cybercapability, jumped in to say, 'But right now, the level of deterrence is not deterring.'
>
> 'That is true,' Admiral Rogers responded.[93]

Rogers' testimony reinforces our previous point about the need for the U.S. policymaking community to develop ways to discuss more forthrightly U.S. offensive cyber capabilities and initiatives. His testimony may in fact signal that senior officials have reached the same conclusion and have begun that process. So we welcome this advance.

The Obama Administration also seems to be pursuing enhanced deterrence for cyberattacks through additional means. Very recently the President took a concrete step in this direction by issuing an Executive Order that would enable the Treasury Department to impose sanctions on individuals or entities that engage in particularly serious types of destructive cyberattacks or commercial espionage from outside U.S. borders.[94] The EO was explicitly identified as an intended deterrent:

> When it comes to the worst actors, one of the biggest challenges we currently face is developing tools that will allow us to respond appropriately, proportionately, and effectively to malicious cyber-enabled activities, and to deter others from engaging in similar activities.[95]

Substantively, however, there are clearly reasons for concern about whether the enhanced exercise of offensive cyber capabilities or the limited types of sanctions contained in the President's new EO will serve as the intended deterrent. Probably all involved in these decisions are well aware of the risks of blowback and unintended consequences (see Dubowitz and Fixler's chapter for an excellent discussion of this problem in the context of the Treasury's cyber-enabled smart sanctions program). Many already contend that Stuxnet, for example, "crossed a Rubicon" and spurred Iran to develop its own extended campaigns of cyberattacks first on Saudi and Qartari oil and gas facilities in 2012,[96] then on a number of large U.S. banks in a series of attacks from 2012 at least through 2013,[97] and then, in a greatly broadened campaign, to "coordinated attacks against more than 50 targets in 16 countries, many of them corporate and government entities that manage critical energy, transportation and medical services."[98] Some have gone even further and speculated that the Iranian program has established functional links to enhance North Korean and Syrian cyberwarfare programs.[99] Even if none of these linkages were true (which is highly unlikely), the point would still remain: cyber aggression is likely to produce serious unintended consequences, if for no other reason that the evidence of its use can itself become a viral learning tool for those who study the effects.

As we noted above, the U.S. needs a well-thought-out doctrine to provide guidance for the use of offensive cyber capabilities. It also needs to develop a better plan than it has established so far for creating an effective deterrent to cyberattacks, or at least to major ones. And it needs to be sure that the government agencies creating these plans have personnel in place with the necessary expertise to understand not just cyberwar, cybercrime and cyberterrorism, but also cyber-enabled economic warfare.

Future Research: Cyberattacks on Government and Cyber-Enabled Economic Warfare?

Earlier in this chapter after reviewing details of a number of prominent cyberattacks on government sector entities in the past two years, we suggested that despite initial appearances to the contrary, these attacks actually present important concerns for future developments in cyber-enabled economic warfare. We conclude this chapter with some speculative considerations that warrant additional future research.

The gist of our earlier question was how are attacks on government targets with no direct economic consequences relevant to likely future threats from cyber-enabled *economic* warfare? The answer turns out to be very similar to the analysis offered above for the ISIS / CENTCOM hack. As in the case of ISIS, the concern is not so much with the particulars of any of these attacks or their direct impacts, but instead with what they signify about evolving possibilities and intentions. For the case of adversaries that are state actors, these types of attacks on U.S. government agencies demonstrate several points that are worrisome.

First, adversarial states such as China, Russia, and Iran are all becoming quite sophisticated in their cyberattack capabilities and much more active in the exercise of those skills. This means it is becoming increasingly difficult to detect and defend against their attacks, a fact that experts and senior U.S. officials widely acknowledge.[100] Second, all three of these adversaries and North Korea in addition are, despite important differences, also indicating hostile *intentions*. This means the U.S. needs to prepare for the possibility of hostile, more damaging cyber *actions*. Third, many, if not all, of these adversarial states are developing complex relationships with non-state actors who help them pursue cyberattacks on the West and the U.S. in particular, both in the private and government sectors. Because these relationships are often quite difficult to detect reliably and prove, they make establishing accountability for cyberattacks more difficult. As a result, they generally render U.S. defenses that rely upon law enforcement, diplomacy, and deterrence weaker. They also demonstrate that the strategies of the U.S.'s state actor adversaries are evolving in a dangerous direction. Finally, when one assembles the pieces, the worry is with where the trend is heading. Basically this is like the old story of the connection of 'means, motive, and opportunity' to crime: when those three conditions are all clearly present and reinforcing, the prospects for how hostile actors are likely to respond do not seem bright.

For the case of adversaries who are non-state actors, we note that increasingly such groups are collaborating with sponsoring state actors.[101] In some instances, it seems adversarial states prefer these arrangements as a means to acquire plausible deniability for the attacks they sponsor. As one cyberattack investigator has been reported to observe dryly: "'Twenty-one-year-old hackers are the new stealth,' he says—meaning that militaries use hackers to hide their operations the same way they use advanced design to hide bombers."[102]

In addition to hacktivists who share sympathies with an adversarial state, a new type of non-state actor seems to be rising in number and importance: cyber-mercenaries. These groups are responding to market forces, increasing their sophistication and specialization, and selling their destructive cyber expertise for lucrative sums to both corporations and states.[103] (One begins to wonder, what next, venture capitalists from rogue states vying to invest in the best mercenary groups?) As these cyber mercenaries become more prevalent in black and gray market 'hacker bazaars,' they expand the opportunity set available for motivated, deep-pocketed 'clients' to pursue more aggressive and sophisticated cybercrime, and cyber-enabled economic warfare, strategies.[104] A senior executive at Kaspersky Lab says, "In the future, we predict the number of small, focused 'APT-to-hire' groups to grow, specializing in hit-and-run operations; a kind of 'cyber mercenary' team for the modern world.'"[105]

Additional considerations arise when the non-state actors are in fact terrorists. The literature on cyber terrorism is quite extensive, both in quantity and in age. Nonetheless, to date there have been almost no terrorist cyberattacks by non-state actors.[106] ISIS, for example, is proving adept at using information technology in a variety of ways, but especially for spreading its propaganda, recruiting, training and fund raising.[107] To date ISIS seems to have had no interest in developing and implementing plans for cyber-enabled economic warfare. But as noted above, with successes from steps like their CENTCOM hack, it's possible that at some point that could change. Indeed, it may already be changing. The *New York Times* just reported on March 22 that ISIS has posted online the names, photos, addresses and other information of 100 U.S. military members and "called on its members and sympathizers in the United States to kill" them.[108] To service members and their families, at the very least, this would seem by itself to constitute cyber terrorism. In any case, it seems to be another step toward developing capabilities for cyber terrorism and/or cyber-enabled economic warfare.

The danger, then, with many of these attacks in the government sector is not so much in the attacks' particulars, but in their role as evolutionary steps toward new capabilities, visions, and strategies of economic warfare against the U.S. and its allies. Future research will have to track how in fact these trends and threats unfold.

Next Steps

The research contained in this monograph represents an initial step toward improving U.S. understandings and preparedness for responding to evolving threats posed by cyber-enabled economic warfare. We explore what cyber-enabled economic warfare is; how substantial a threat it is; how and why is it unfolding, particularly in the financial services and critical infrastructure sectors; who are the main threat actors that are pursuing cyber-enabled economic warfare strategies; how well prepared is the U.S. to cope with these threats; and what more needs to be done and what topics need additional research. The core findings of this stage of the project are that cyber-enabled economic warfare is an established and growing threat, and that the U.S. is not adequately prepared to respond to it. We find reinforcement of our main points in the recent Congressional testimony of DNI Director James Clapper.[109] Director Clapper's opening paragraph in his 2015 annual Worldwide Threat Assessment report to the Senate Armed Services Committee reinforces our findings in this monograph very well:

> Cyber threats to U.S. national and economic security are increasing in frequency, scale, sophistication, and severity of impact. The ranges of cyber threat actors, methods of attack, targeted systems, and victims are also expanding. Overall, the unclassified information and communication technology (ICT) networks that support U.S. Government, military, commercial, and social activities remain vulnerable to espionage and/or disruption. However, the likelihood of a catastrophic attack from any particular actor is remote at this time. Rather than a "Cyber Armageddon" scenario that debilitates the entire U.S. infrastructure, we envision something different. We foresee an ongoing series of low-to-moderate level cyberattacks from a variety of sources over time, which will impose cumulative costs on U.S. economic competitiveness and national security.[110]

We believe that Director Clapper's conclusions are spot on as far as they go, but also believe that his report does not develop them nearly far enough to represent adequately how cyber-enabled economic warfare is evolving or how strategies for pursuing it vary among major threat actors. This monograph was never intended to be the end of this project. Rather, it was meant to be a springboard for further research by both these authors and others. Cyber-enabled economic warfare is, unfortunately, only beginning. For the defense of the country, a broader community of policymakers, academics, strategists, technologists, analysts, and operators must

enter into the discussion to both frame the problem and create the solution set. Consider this work the clarion call.

---

[1] Mandiant. (2014) "CyberSecurity's Maginot Line: A Real-World Assessment of the Defense-in-Depth Model," Mandiant FireEye report; p. 3. http://www2.fireeye.com/rs/fireye/images/fireeye-real-world-assessment.pdf

[2] David E. Sanger, Michael S. Schmidt and Nicole Perlroth (2014) "Obama Vows a Response to Cyberattack on Sony," *New York Times*, Dec. 19. http://www.nytimes.com/2014/12/20/world/fbi-accuses-north-korean-government-in-cyberattack-on-sony-pictures.html?_r=0

[3] Mandiant. (2015) "M-Trends: A View from the Front Lines," Mandiant FireEye report, p. 1.

[4] James R. Clapper (2015) "Worldwide Threat Assessment of the U.S. Intelligence Community," U.S. Senate Armed Services Committee, Feb. 26. http://www.dni.gov/files/documents/Unclassified_2015_ATA_SFR_-_SASC_FINAL.pdf

[5] Ponemon Institute (2012) "2012 Cost of Cybercrime Study," Ponemon Institute, Oct. 8. http://www.ponemon.org/library/2012-cost-of-cyber-crime-study

[6] Michael McCaul. (2014) "McCaul Statement on State Department's Cyber Breach," Nov. 17. http://homeland.house.gov/press-release/mccaul-statement-state-department-s-cyber-breach

[7] As reported by Matthew Rhoades, testimony to the House Committee on Homeland Security, Subcommittee on Cybersecurity, Infrastructure Protection, and Security Technologies: Subcommittee Field Hearing: "Protecting Your Personal Data: How Law Enforcement Works With the Private Sector to Prevent Cybercrime" Apr 16, 2014. http://docs.house.gov/meetings/HM/HM08/20140416/102141/HHRG-113-HM08-Wstate-RhoadesM-20140416.pdf

[8] Ponemon Institute, "2014 Cost of Cybercrime Study: United States," Hewlett-Packard, October 9, 2014; p. 9. http://resources.idgenterprise.com/original/AST-0136623_2014_Cost_of_Cyber_Crime_Study_United_States.pdf

[9] Jai Vijayan. (2014) "Cyberattacks Longer, More continuous Than Before," *Information Week*, Dec. 12. http://www.darkreading.com/perimeter/cyberattacks-longer-more-continuous-than-before-/d/d-id/1318109

[10] Mandiant, op cit. at # 1.

[11] Ibid. We note the hyperbole of the concluding estimation: "…stopping virtually none of them." This is a bias that one needs to recognize when vendors do surveys for public consumption relating to the need for their products.

[12] Channel NewsAsia (2015) "Japan Sees 25 Billion Cyberattacks in 2014: Government Agency," Channel NewsAsia, Feb. 17. http://www.channelnewsasia.com/news/technology/japan-sees-25-billion/1665272.html

[13] Vijayan, op cit at # 8.

[14] Tiffany Hsu (2014) "2 Arrested in Connection with Target Hack," *Los Angeles Times*, Jan. 20. http://www.latimes.com/business/la-fi-target-arrests-20140121-story.html

[15] Sharone Tobias, 2014: The Year in Cyberattacks," *Newsweek*, Dec. 31, 2014. http://www.newsweek.com/2014-year-cyber-attacks-295876

[16] Chris Smith, "Expert who first revealed massive Target breach tells us how it happened," 16 January 2004, http://bgr.com/2014/01/16/how-was-target-hacked/

[17] Reuters (2014) "Target, Neiman Marcus Not Only Victims of Cyberattacks: Sources," *Daily News*, Jan. 13. http://nydn.us/1aWCmax

[18] Nicole Perlroth (2015) "U.S. Finds 'Backoff' Hacker Tool Is Widespread," *New York Times*, Aug. 22. http://bits.blogs.nytimes.com/2014/08/22/secret-service-warns-1000-businesses-on-hack-that-affected-target/?_r=0

[19] eBay Announcements (2014) "eBay to Ask eBay Users to Change Passwords," eBay Announcements, May 21. http://announcements.ebay.com/2014/05/ebay-inc-to-ask-ebay-users-to-change-passwords/

[20] eBay inc Blog (2014) "eBay to Ask eBay Users to Change Passwords," eBay inc Blog, May 21. http://blog.ebay.com/ebay-inc-ask-ebay-users-change-passwords/

[21] Reuters (2014) "JP Morgan Hack Exposed Data of 83 Million, Among Biggest Breaches in History," Reuters, Oct. 2. http://www.reuters.com/article/2014/10/03/us-jpmorgan-cybersecurity-idUSKCN0HR23T20141003

[22] Goldstein, Matthew; Perlroth, Nicole; Sanger, David E. (2014-10-03). "Hackers' Attack Cracked 10 Financial Firms in Major Assault", *New York Times*.

[23] Woodyard, Chris (4 October 2014). "Report: Russian hackers behind JPMorgan Chase attack". *USA Today*.

[24] Tobias, op cit at # 16.

[25] Riley, Michael (9 October 2014). "JPMorgan Hackers Said to Probe 13 Financial Firms". *Bloomberg*.

[26] Nicole Perlroth and David Gelles (2014) "Russian Hackers Amass Over a Billion Internet Passwords," *New York Times*, Aug. 5. http://www.nytimes.com/2014/08/06/technology/russian-gang-said-to-amass-more-than-a-billion-stolen-internet-credentials.html

[27] Sharone Tobias, 2014: The Year in Cyberattacks," *Newsweek*, Dec. 31, 2014. http://www.newsweek.com/2014-year-cyber-attacks-295876

[28] Robin Sidel, 2014, "Home Depot's 56 Million Card Breach Bigger Than Target's," *Wall Street Journal*, Sept. 18, http://www.wsj.com/articles/home-depot-breach-bigger-than-targets-1411073571

[29] Michael Cieply and Brooks Barnes (2014) "Sony Cyberattack, First a Nuisance, Swiftly Grew Into a firestorm," New York Times, Dec. 30. http://www.nytimes.com/2014/12/31/business/media/sony-attack-first-a-nuisance-swiftly-grew-into-a-firestorm-.html

[30] Warwick Ashford (2015) "FBI reiterates claim North Korea is behind Sony cyber hack," *ComputerWeekly.com*, Jan. 8; http://www.computerweekly.com/news/2240237746/FBI-reiterates-claims-North-Korea-is-behind-Sony-cyber-attack ; David E. Sanger and Martin Fackler (2015) "N.S.A. Breached North Korean Networks Before Sony Attack, Officials Say," New York Times, Jan. 18 ; http://www.nytimes.com/2015/01/19/world/asia/nsa-tapped-into-north-korean-networks-before-sony-attack-officials-say.html?ref=topics

[31] Louise Esola (2014) "North Korea's Sony Hack Seen as Cyber Security Game-Changer," Business Insurance.com, Dec. 21. http://www.businessinsurance.com/article/20141221/NEWS07/312219980

[32] Amelia Smith (2014) "Sony Cyberattack One of Worst in Corporate History," Newsweek, Dec. 4. http://www.newsweek.com/sony-cyber-attack-worst-corporate-history-thousands-files-are-leaked-

289230 ; for a timeline, see USA Today report: http://www.usatoday.com/story/news/nation-now/2014/12/18/sony-hack-timeline-interview-north-korea/20601645/

[33] Cieply and Barnes, op cit. at # 21.

[34] Esola, op cit. at # 22.

[35] Anna Wilde Mathews (2015) "Anthem: Hacked Database Included 78.8 Million People," Wall Street Journal, Feb. 24. http://www.wsj.com/articles/anthem-hacked-database-included-78-8-million-people-1424807364?KEYWORDS=medicare

[36] Priya Anand (2015) "5 Things Consumers Should Do About the Anthem Hack," MarketWatch.com, Feb. 5. http://www.marketwatch.com/story/5-things-consumers-need-to-know-about-the-anthem-hack-2015-02-05

[37] BloombergBusiness: http://www.bloomberg.com/news/articles/2015-02-24/fbi-is-close-to-finding-hackers-in-anthem-health-care-data-theft

[38] Bill Gertz (2015) "'Deep Panda' Chinese Cyber Espionage Gang Linked to Hack of 80 Million Anthem Health Care Records," FlashCritic.com, Feb. 7. http://flashcritic.com/chinese-cyber-espionage-suspected-hack-health-care-provider-anthem/

[39] Anand, op cit. at # 28.

[40] Priya Anand (2015) TurboTax Halts E-Filing for State Returns due to Fraud, Stealing of Refunds," *MarketWatch*, Feb. 6. http://www.marketwatch.com/story/turbotax-halts-e-filing-of-state-tax-returns-due-to-potential-fraud-2015-02-06

[41] Robert W. Wood (2015) "TurboTax, Phishing, E-Filing, and IRS Security," *Forbes*, Feb. 19. http://www.forbes.com/sites/robertwood/2015/02/19/turbotax-phishing-e-filing-and-irs-security/

[42] Laura Saunders (2015) "Digging Into the TurboTax ID Thefts," *Wall Street Journal*, Mar. 13. http://blogs.wsj.com/totalreturn/2015/03/13/digging-into-the-turbotax-id-thefts/

[43] Anna Wilde Mathews and Danny Yadron (2015) "Premera Blue Cross Says Cyberattack Could Affect 11 Million Members," *Wall Street Journal*, Mar. 17. http://www.wsj.com/articles/premera-blue-cross-says-cyberattack-could-affect-11-million-members-1426627752

[44] Letter from Premera to its customers affected by the breach, dated March 17, 2015.

[45] CBS Moneywatch (2015) "Health Insurer Premera Hit by 'Sophisticated Cyberattack'," CBS News, Mar. 17. http://www.cbsnews.com/news/health-insurer-premera-hit-by-sophisticated-cyberattack/

[46] Ibid.

[47] David Inserra and Paul Rosenzweig (2014) "Continuing Federal Cyber Breaches Warn Against Cybersecurity Regulation," Heritage Foundation, Issue Brief #4288, Oct. 27. http://www.heritage.org/research/reports/2014/10/continuing-federal-cyber-breaches-warn-against-cybersecurity-regulation

[48] Michael S. Schmidt, David E. Sanger, and Nicole Perlroth (2014) "Chinese Hackers Pursue Key Data on U.S. Workers," *The New York Times*, July 9. http://www.nytimes.com/2014/07/10/world/asia/chinese-hackers-pursue-key-data-on-us-workers.html?_r=0

[49] DW (2014) "NATO Websites Hit by DDoS Cyberattacks, Ukraine Group Claims Responsibility," DW.de, Mar. 16. http://www.dw.de/nato-websites-hit-by-ddos-cyber-attacks-ukraine-group-claims-responsibility/a-17499561

[50] RT.com (2014) "Ukrainian CyberBerkut Takes Down NATO Websites," RT.com, Mar. 16. http://on.rt.com/vm48nl

[51] Adrian Croft and Peter Apps (2014) "NATO Websites Hit in Cyberattack Linked to Crimea Tension," Reuters, Mar. 16. http://www.reuters.com/article/2014/03/16/us-ukraine-nato-idUSBREA2E0T320140316

[52] Ibid.

[53] Eric Walsh (2014) "U.S. Homeland Security Contractor Reports Computer Breach," Reuters, Aug. 7. http://www.reuters.com/article/2014/08/07/us-usa-security-contractor-idUSKBN0G62N420140807

[54] Aliya Sternstein (2014) "Will the Government Shred Your Contract After a Hack?" Nextgov.com, Aug. 8. http://www.nextgov.com/cybersecurity/2014/08/will-government-shred-your-contract-after-hack/91049/

[55] Ellen Nakashima (2014) "Hackers Breach Some White House Computers," *Washington Post*, Oct. 28. http://www.washingtonpost.com/world/national-security/hackers-breach-some-white-house-computers/2014/10/28/2ddf2fa0-5ef7-11e4-91f7-5d89b5e8c251_story.html

[56] Ibid.

[57] Ellen Nakashima (2014) "China suspected of breaching U.S. Postal Service computer networks," Washington Post, Nov. 10. http://www.washingtonpost.com/blogs/federal-eye/wp/2014/11/10/china-suspected-of-breaching-u-s-postal-service-computer-networks/

[58] AFP, op cit. at # 4.

[59] Ellen Nakashima (2014) "Hackers breach some White House computers," *Washington Post*, Oct. 28. http://www.washingtonpost.com/world/national-security/hackers-breach-some-white-house-computers/2014/10/28/2ddf2fa0-5ef7-11e4-91f7-5d89b5e8c251_story.html

[60] *Washington Post*, Jan. 12, 2015. http://www.washingtonpost.com/news/checkpoint/wp/2015/01/12/centcom-twitter-account-apparently-hacked-by-islamic-state-sympathizers/

[61] "British Hacker Suspected of Cyberattack on U.S. Central Command Twitter Account," Mirror, Jan. 13, 2015. http://www.mirror.co.uk/news/world-news/british-hacker-suspected-cyber-attack-4974855

[62] Vincent R. Stewart (2015) Director, Defense Intelligence Agency: Statement for the Record, "Worldwide Threat Assessment," Armed Services Committee, U.S. House of Representatives, Feb. 3. http://docs.house.gov/meetings/AS/AS00/20150203/102880/HHRG-114-AS00-Wstate-StewartUSMCV-20150203.pdf

[63] See, for example, Dawn Cappelli (2012) *The CERT Guide to Insider Threats: How to Prevent, Detect, and Respond to Information Technology Crimes (Theft, Sabotage, Fraud)* (New York: Addison-Wesley Professional), Jan.; CERT and Software Engineering Institute (n.d.) CERT Insider Threat Research and Insider Threat Database, Software Engineering Institute, Carnegie Mellon University and CERT; http://www.cert.org/insider-threat/research/database.cfm ; PricewaterhouseCoopers LLP (2014) "U.S. Cybercrime: Rising Risks, Reduced Readiness," co-sponsored by PricewaterhouseCoopers, The CERT Division of the Software Engineering Institute at Carnegie Mellon University, CSO magazine, and the U.S. Secret Service; http://www.pwc.com/us/en/increasing-it-effectiveness/publications/assets/2014-us-state-of-cybercrime.pdf ; or Infosecurity Magazine (2014) "Insider Threats Top Infosecurity Europe Attendees' Cyber Fears," Infosecurity Magazine, June 26; http://www.infosecurity-magazine.com/news/insider-threats-top-infosecurity/

[64] Public Service Announcement (2014) "Increase in Insider Threat Cases Highlight Significant Risks to Business Networks and Proprietary Information," Homeland Security, Sep. 23. https://www.ic3.gov/media/2014/140923.aspx

[65] Stewart, op cit. at # 59.

[66] Dustin Volz (2015) "Obama Is Creating a New Agency to Combat Cyberthreats," *National Journal*, Feb. 10. http://www.nationaljournal.com/tech/obama-is-forming-a-new-agency-to-combat-cyber-threats-20150210

[67] Bill Gertz (2015)

[68] Schmidt et al, op cit. at # 45; for the background U.S. House intelligence committee investigation report documenting China's use of telecommunications firms such as Huawei for "malicious purposes," see: House Permanent Select Committee on Intelligence (2012) "Investigative Report on the U.S. National Security Issues Posed by Chinese Telecommunications Companies Huawei and ZTE," U.S. House Permanent Select Committee on Intelligence, 112th Congress, Oct. 8. https://intelligence.house.gov/sites/intelligence.house.gov/files/documents/Huawei-ZTE%20Investigative%20Report%20(FINAL).pdf

[69] Barton Gellman and Ellen Nakashima (2013) "U.S. spy agencies mounted 231 offensive cyber-operations in 2011, documents show," *Washington Post*, Jan. 9. http://cyber-peace.org/wp-content/uploads/2013/06/'Black-budget'-summary-details-U.S-Part2.pdf

[70] Mandiant, op cit. at # 1; p. 13.

[71] Matthew Rhoades, testimony to the House Committee on Homeland Security, Subcommittee on Cybersecurity, Infrastructure Protection, and Security Technologies: Subcommittee Field Hearing: "Protecting Your Personal Data: How Law Enforcement Works With the Private Sector to Prevent Cybercrime" Apr 16, 2014. http://docs.house.gov/meetings/HM/HM08/20140416/102141/HHRG-113-HM08-Wstate-RhoadesM-20140416.pdf

[72] Percy W. Bidwell (1942) "Our Economic Warfare," *Foreign Affairs*, 20(3): pp. 421-437. http://www.jstor.org/stable/20029165

[73] Edward S. Miller. (2007) *Bankrupting the Enemy: The U.S. Financial Siege of Japan Before Pearl Harbor* (Annapolis, MD: Naval Institute Press).

[74] See, for example, Robert Loring Allen (1960) *Soviet Economic Warfare* (Public Affairs Press); Norman A. Bailey (1998) *The Strategic Plan that Won the Cold War: National Security Decision Directive 75* (McLean, VA: Potomac Foundation); http://www.iwp.edu/news_publications/book/the-strategic-plan-that-won-the-cold-war ; and Thomas Reed (2004) *At the Abyss: An Insider's History of the Cold War* (Presidio Press).

[75] See for example Rhonda L. Callaway and Elizabeth G. Matthews (2008) *Strategic U.S. Foreign Assistance* (Burlington, VT: Ashgate Publishing Co.) ; and Jeremy M. Sharp (2014) "Egypt: Background and U.S. Relations," Congressional Research Service, RL33003; http://fas.org/sgp/crs/mideast/RL33003.pdf .

[76] Robert K. Brigham (2014) *The United States and Iraq Since 1990: A Brief History with Documents* (West Sussex, UK: Wiley-Blackwell) ; and Sasan Fayazmanesh (2008) *The United States and Iran: Sanctions, Wars and the Policy of Dual Containment* (New York: Routledge).

[77] Juan Zarate (2013) *Treasury's War: The Unleashing of a New Era of Financial Warfare* (New York: PublicAffairs).

[78] See for example Jeffrey T. Richelson (2013) "National Security Agency Tasked with Targeting Adversaries' Computers for Attack Since Early 1997, According to Declassified Document," National Security Archive, Apr. 26; http://nsarchive.gwu.edu/NSAEBB/NSAEBB424/?utm_source=Sinocism+Newsletter&utm_campaign=5b8e2a7f18-Sinocism04_28_13&utm_medium=email

[79] For example, see reporting on the U.S.'s Trojan horse sabotage of pipeline control software the Soviets stole that in 1982 caused their Siberian pipeline to experience "the most monumental non-nuclear explosion and fire ever seen from space"; Thomas Reed (2004) *At the Abyss: An Insider's History of the Cold War* (New York: Ballantine Books): p. 267.

[80] In the fall of 2012, Secretary Panetta still "carefully avoided using the words 'offense' or 'offensive' in the context of American cyberwarfare, instead defining the Pentagon's capabilities as 'action to defend the nation'" (see Elisabeth Bumiller and Thom Shanker (2012) "Panetta Warns of Dire Threat of Cyberattack on U.S.," *New York Times*, Oct. 11; http://www.nytimes.com/2012/10/12/world/panetta-warns-of-dire-threat-of-cyberattack.html?_r=0 . But other U.S. government officials were beginning to discuss offensive cyber capabilities, and by early 2013 General Alexander was very explicitly describing and advocating U.S. offensive cyberwarfare capabilities. For examples, see Cheryl Pellerin (2013) "Cybercom Builds Teams for Offense, Defense in Cyberspace," DoD News, U.S. Department of Defense; http://www.defense.gov/news/newsarticle.aspx?id=119506 ; and see Shaun Waterman (2013) "U.S. Cyberwar Offense 'Best in the World,': NSA's Gen. Keith Alexander," *Washington Times*, Aug. 26; http://www.washingtontimes.com/news/2013/aug/26/us-cyberwar-offense-best-world-nsas-gen-keith-alex/

[81] For examples, see the relevant work of journalists such as Michael Joseph Gross in *Vanity Fair*, David Sanger in the *New York Times*, Ellen Nakashima in the *Washington Post*, Cheryl Pellerin in DoD News, and Kim Zetter in *Wired* and elsewhere, among others.

[82] For example, see Martin C. Libicki (2013) "Brandishing Cyberattack Capabilities," RAND National Defense Reseaarch Institute (Santa Monica: RAND Corporation). http://www.rand.org/pubs/research_reports/RR175.html

[83] Some interesting exceptions include: Joseph S. Nye Jr. (2011) "Nuclear Lessons for Cyber Security?" Strategic Studies Quarterly, Winter: pp. 18-38; http://www.au.af.mil/au/ssq/2011/winter/nye.pdf ; Kris E. Barcomb (2013) "From Sea Power to Cyber Power: Learning from the Past to Craft a Strategy for the Future," Joint Forces Quarterly, 2nd Quarter: pp. 78-83; Alison Lawlor Russell (2014) Cyber Blockades (Georgetown University Press); and Christopher Paul, Issac R. Porche III, and Elliot Axelband (2014) "The Other Quiet Professionals: Lessons for Future Cyber Forces from the Evolution of Special Forces," RAND Research Reports RR-780-A, (Santa Monica: RAND Corporation).

[84] D.T. Jack (1940) *Studies in Economic Warfare* (London: P.S. King & Son); Pumphrey, Lowell, M., *Planning For Economic Warfare*, Military Affairs, Vol. 5, No. 3 (Autumn, 1941), pp. 145-151; Wu, Yuan-li (1952) *Economic Warfare* (New York: Prentice-Hall); Nicholas A. Lambert (2012) *Planning Armageddon: British Economic Warfare and the First World War* (Cambridge, MA: Harvard University Press); Robert Higgs (2012) "How U.S. Economic Warfare Provoked Japan's Attack on Pearl Harbor," *The Freeman* 56 (May 2006): 36-37; http://mises.org/library/how-us-economic-warfare-provoked-japans-attack-pearl-harbor .

[85] See for example Mark D. Young (2010) "National Cyber Doctrine: The Missing Link in the Application of American Cyber Power," *Journal of National Security and Law Policy*, Vol. 4: pp. 173-196; http://jnslp.com/wp-content/uploads/2010/08/12_Young.pdf ; U.S. Government Accountability Office (2011) "Defense Department Cyber Efforts: DOD Faces Challenges in Its Cyber Activities," GAO Report to Congressional Requesters, July; http://www.gao.gov/assets/330/321818.pdf ; Ellen Nakashima (2012) "Pentagon Proposes More Robust Role for Its Cyber-Specialists," *Washinton Post*, Aug. 9; http://www.washingtonpost.com/world/national-security/pentagon-proposes-more-robust-role-for-its-cyber-specialists/2012/08/09/1e3478ca-db15-11e1-9745-d9ae6098d493_story.html ; Ellen

Nakashima (2012) "Obama Signs Secret Directive to Help Thwart Cyberattacks," *Washington Post*, Nov. 14; (http://www.washingtonpost.com/world/national-security/obama-signs-secret-cybersecurity-directive-allowing-more-aggressive-military-role/2012/11/14/7bf51512-2cde-11e2-9ac2-1c61452669c3_story.html ; Zachary Fryer-Biggs (2012) "DoD's New Cyber Doctrine," DefenseNews, Oct. 13; http://archive.defensenews.com/article/20121013/DEFREG02/310130001/DoD-8217-s-New-Cyber-Doctrine ; Chairman of the Joint Chiefs of Staff (2013) Joint Publication 3-12: Cyberspace Operations (Washington, DC: The Joint Staff), Feb. ; Joel Hruska (2013) "U.S. Cyber Command Admits Offensive Cyberwarfare Capabilities, Fundamental Shift In U.S. Doctrine," HotHardware.com, Mar. 13; http://hothardware.com/News/U.S.-Cyber-Command-Admits-Offensive-Cyberwarfare-Capabilities-Fundamental-Shift-In-U.S.-Doctrine/

[86] National Archives (2015) "Records of the Foreign Economic Administration (RG 169)," U.S. National Archives and Records Administration, Holocaust-Era Assets. http://www.archives.gov/research/holocaust/finding-aid/civilian/rg-169.html

[87] W.W. Rostow (1991) "Waging Economic Warfare from London," Central Intelligence Agency, Center for the Study of Intelligence, Studies Archive Indexes, Vol. 35(4). https://www.cia.gov/library/center-for-the-study-of-intelligence/kent-csi/vol35no4/html/v35i4a06p_0001.htm

[88] Ibid.

[89] See for example Director Comey's 2014 House testimony: "We face cyber threats from state-sponsored hackers, hackers for hire, global cyber syndicates, and terrorists. They seek our state secrets, our trade secrets, our technology, and our ideas—things of incredible value to all of us. They seek to strike our critical infrastructure and to harm our economy," FBI Director Comey's written testimony to the House Homeland Security Committee, Sep. 17, 2014; http://www.fbi.gov/news/testimony/worldwide-threats-to-the-homeland

[90] CNN (2004) "Bin Laden: Goal is to Bankrupt U.S.," CNN, Nov. 1; http://www.cnn.com/2004/WORLD/meast/11/01/binladen.tape/ ; Jon Basil Utley (2009) "How Bin Laden Bankrupted America," AntiWar.com, Jan. 19 ; http://www.antiwar.com/utley/?articleid=14081 ; Gal Luft (2005) "Al Qaeda's Economic War Against the United States," *Energy Security* (Institute for the Analysis of Global Security); Jan. 24; http://www.iags.org/n0124052.htm ; Ezra Klein (2011) "Bin Laden's War Against the U.S. Economy," *Washington Post*, May 3 ; http://www.washingtonpost.com/blogs/wonkblog/post/bin-ladens-war-against-the-us-economy/2011/04/27/AFDOPjfF_blog.html ; Daveed Gartenstein-Ross (2011) "Don't Get Cocky, America: Al Qaeda is Still Deadly Without Osama bin Laden," *Foreign Affairs*, May 2; http://foreignpolicy.com/2011/05/02/dont-get-cocky-america-2/ ; Daveed Gartenstein-Ross (2011) *Bin Laden's Legacy: Why We're Still Losing the War on Terror* (Hoboken, NJ: John Wiley & Sons).

[91] Clapper, op cit. at # 4.

[92] Michael S. Rogers (2015) Statement of Admiral Michael S. Rogers, Commander U.S. Cyber Command, before the Senate Committee on Armed Services, Mar. 19. http://www.armed-services.senate.gov/imo/media/doc/Rogers_03-19-15.pdf

[93] David E. Sanger (2015) "U.S. Must Step Up Capacity for Cyberattacks, Chief Argues," *New York Times*, Mar. 19. http://www.nytimes.com/2015/03/20/us/us-must-step-up-capacity-for-cyberattacks-chief-argues.html?ref=topics

[94] Office of the President (2015) "Executive Order – 'Blocking the Property of Certain Persons Engaging in Significant Malicious Cyber-Enabled Activities,'" The White House, Apr. 1. https://www.whitehouse.gov/the-press-office/2015/04/01/executive-order-blocking-property-certain-persons-engaging-significant-m

[95] Michael Daniel (2015) "Our Latest Tool to Combat Cyberattacks: What You Need to Know," The White House Blog, Office of the President, Apr. 1. https://www.whitehouse.gov/blog/2015/04/01/our-latest-tool-combat-cyber-attacks-what-you-need-know

[96] Siobhan Gorman and Julian E. Barnes (2012) "Iran Blamed for Cyberattacks," *Washington Post*, Oct. 12; http://www.wsj.com/articles/SB10000872396390444657804578052931555576700 ; Terry Pattar (2013) "Cyberattacks in the Middle East," *Current Intelligence*, Jul. 29 ; http://www.currentintelligence.net/analysis/2013/7/29/cyber-attacks-in-the-middle-east.html

[97] Ellen Nakashima (2012) "Iran Blamed for Cyberattacks on U.S. Banks and Companies," *Washington Post*, Sept. 21; http://www.washingtonpost.com/world/national-security/iran-blamed-for-cyberattacks/2012/09/21/afbe2be4-0412-11e2-9b24-ff730c7f6312_story.html ; Nicole Perlroth and Quentin Hardy (2013) "Bank Hacking Was the Work of Iranians, Officials Say," *New York Times*, Jan. 8. ; http://www.nytimes.com/2013/01/09/technology/online-banking-attacks-were-work-of-iran-us-officials-say.html ; Michael Joseph Gross (2013) "Silent War," *Vanity Fair*, July. http://www.vanityfair.com/news/2013/07/new-cyberwar-victims-american-business

[98] Nicole Perlroth (2014) "Report Says Cyberattacks Originated Inside Iran," *New York Times*, Dec. 2. http://www.nytimes.com/2014/12/03/world/middleeast/report-says-cyberattacks-originated-inside-iran.html

[99] ISIS Study Group (2014) "Iran Steps Up Cyberattacks Against the U.S. and Its Allies," ISIS Study Group, Dec. 7. http://isisstudygroup.com/?p=3560

[100] Stewart, op cit. at # 63; Clapper, op cit. at # 4.

[101] "Many cyber-attacks targeting the U.S. can be traced to state-sponsored groups in Russia and China but it is difficult to connect the countries to the attacks directly, except by circumstantial evidence such as the attack's required monetary and computing resources." Jess Jacob McMurdo (2014) "Cybersecurity Firms – Cyber Mercenaries?" Social Science Research Network, Dec. 12. http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2556412

[102] Gross, op cit. at # 95.

[103] McMurdo, op cit. at # 99.

[104] Lillian Ablon, Martin C. Libicki, and Andrea A. Golay (2014) Markets for Cybercrime Tools and Stolen Data (Santa Monica, CA: RAND Corporation), Research Report RR-610-JNI. http://www.rand.org/pubs/research_reports/RR610.html

[105] Kaspersky Lab press release (2013) "Kaspersky Lab Exposes 'Icefog': a New Cyber-espionage Campaign Focusing on Suppy Chain Attacks," Kaspersky Lab, Sep. 26. http://www.kaspersky.com/about/news/virus/2013/Kaspersky_Lab_exposes_Icefog_a_new_cyber-espionage_campaign_focusing_on_supply_chain_attacks

[106] See for example, Andrew Colarik (2006) *Cyber Terrorism: Political and Economic Implications* (Idea Group Publishing); Irving Lachow (2009) "Cyber Terrorism: Menace or Myth?" chapter 19 in F.D. Kramer, S.H. Starr, and L.K. Wentz (eds.), *Cyberpower and National Security* (NDU Press and Potomac Books): pp. 437-464) ; S. Macdonald, A. Aly, T. Chen, L. Jarvis, D. Mair, L. Nouri, and A. Whiting (2014) "Terrorists' Use of the Internet: A Symposium – Final Report," Cyberterrorism Project Research Report (No. 4). http://www.cyberterrorism-project.org/wp-content/uploads/2014/06/2014-Symposium-Report.pdf

[107] See Shane Harris (2015) "Justice Department: We'll Go After ISIS's Twitter Army," *The Daily Beast*, Feb. 23, http://www.thedailybeast.com/articles/2015/02/23/justice-department-we-ll-go-after-isis-twitter-army.html ; and Emerson Brooking (2014) The ISIS Propaganda Machine is Horrifying and

Effective. How Does It Work?" Council on Foreign Relations blog, Aug. 21, http://blogs.cfr.org/davidson/2014/08/21/the-isis-propaganda-machine-is-horrifying-and-effective-how-does-it-work/

[108] Michael S. Schmidt (2015) "Naming U.S. Service Members ISIS Asks They Be Killed," *New York Times*, Mar. 22. http://www.nytimes.com/2015/03/22/world/middleeast/isis-urges-sympathizers-to-kill-us-service-members-it-identifies-on-website.html

[109] Clapper, op cit. at # 4.

[110] Ibid.

ABOUT THE AUTHORS

Mark Dubowitz is executive director of the Washington think tank Foundation for Defense of Democracies, and director of the foundation's Center on Sanctions and Illicit Finance. A former venture capitalist and technology executive, he has advised the U.S. administration, Congress, and numerous foreign governments on sanctions issues. Dr. Dubowitz is the co-author of more than a dozen studies on economic sanctions against Iran and teaches courses on sanctions and international negotiations at the Munk School of Global Affairs at the University of Toronto.

Annie Fixler is a policy analyst at the Foundation for Defense of Democracies' Center on Sanctions and Illicit Finance (CSIF). She contributes to CSIF's work on offensive and defensive tools of economic coercion and the application of financial sanctions. She also works closely with FDD's government relations team and executive leadership on a range of issues including Iran sanctions.

Michael Hsieh is a program manager in the Information Innovation Office at the Defense Advanced Research Projects Agency (DARPA). His focus is on quantitative and cryptographic techniques for establishing provable security in big data and software. Dr. Hsieh earned his bachelor's degrees in economics and mathematics at the University of California, Berkeley and his Ph.D. in chemistry at Princeton University.

Tiffany Rad, BS, MA, MBA, JD, is an attorney, computer security analyst and Adjunct Professor at the University of Maine where she teaches computer security, cyber law and ethics. She has presented at conferences such as Black Hat, Defcon, South by Southwest, and the *Washington Post's* Cyber Security Forum, and keynoted the U.S. Cybercrimes Conference in 2014. Her research on industrial control systems was #4 in "Top 10 White Hat Hacks" by Bloomberg news. She is co-author of the book *Security in 2020* and her work has been featured in publications and media such as 60 Minutes, *Washington Times*, NPR, *PC World*, *Popular Mechanics*, *Ars Technica*, *Der Spiegel*, CNN, *Wired Magazine*, Reuters, Huffington Post and others.

Samantha Ravich is CEO of A2P, LLC, a social media analysis firm. She previously was Co-Chair of the Congressionally-mandated National Commission for Review of R&D Programs in the U.S. Intelligence Community. From 2009-2011, Ravich was Senior VP at IPS, a global analysis firm; she also was Deputy National Security Advisor to Vice President Cheney and served in the White House for 5½ years. Dr. Ravich received her Ph.D. from the RAND Graduate School and her MCP/BSE from the University of Pennsylvania/Wharton School. She is a member of the Council on Foreign Relations and serves as an advisor to numerous U.S. Intelligence Agencies.

Abram N. Shulsky is a Senior Fellow at the Hudson Institute. He served as an advisor to the Under Secretary of Defense for Policy from 2001 to 2009, dealing primarily with issues related to Iraq and the Global War on Terrorism. His previous positions include director of Strategic Arms Control Policy in the Office of the Secretary of Defense, Minority Staff Director of the Senate Select Committee on Intelligence, and legislative assistant to Senator Daniel Patrick Moynihan on intelligence issues. Dr. Shulsky is the author of the first edition of a college textbook on intelligence, *Silent Warfare: Understanding the World of Intelligence*, and co-editor, with Gary J. Schmitt, of the second and third editions.

Juan C. Zarate is Chairman and Co-Founder of the Financial Integrity Network and Chairman and Senior Counselor for the Foundation of Defense of Democracies' Center on Sanctions and Illicit Finance. A former federal prosecutor, Zarate previously served as Deputy Assistant to the President and Deputy National Security Advisor for Combating Terrorism from 2005 to 2009, and was the first ever Assistant Secretary of the Treasury for Terrorist Financing and Financial Crimes. He is the author of *Treasury's War: The Unleashing of a New Era of Financial Warfare* (2013), *Forging Democracy (1994)*, and numerous other publications.

Hudson Institute is an independent research organization promoting new ideas for the advancement of global security, prosperity and freedom.

Founded in 1961 by strategist Herman Kahn, Hudson Institute challenges conventional thinking and helps manage strategic transitions to the future through interdisciplinary studies in defense, international relations, economics, health care, technology, culture, and law.

Hudson seeks to guide public policy makers and global leaders in government and business through a vigorous program of publications, conferences, policy briefings and recommendations.

Hudson Institute
1015 15th Street, N.W.
Sixth Floor
Washington, D.C. 20005

P: 202.974.2400
info@hudson.org
www.hudson.org