Hudson Institute

Cyber-Enabled Economic Warfare: An Evolving Challenge (Vol. 2)

Conference Summary, Survey Results, and Policy Recommendations

Samantha F. Ravich, Ph.D.
Principal Investigator

November 2015
Research Report
Cyber-Enabled Economic Warfare: An Evolving Challenge (Vol. 2)

CONFERENCE SUMMARY, SURVEY RESULTS, AND POLICY RECOMMENDATIONS

Samantha F. Ravich, Ph.D.
Principal Investigator
© 2015 Hudson Institute, Inc. All rights reserved.

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
Cyber-Enabled Economic Warfare: An Evolving Challenge
Conference Summary, Survey Results, and Policy Recommendations

On Monday, August 3, 2015, Hudson Institute hosted the launch of a new report, “Cyber-Enabled Economic Warfare: An Evolving Challenge,” edited by Samantha Ravich, principal investigator on the project that produced the report. The report examines the United States’ economic cybersecurity vulnerabilities and identifies specific steps American government agencies and private-sector actors should take to better recognize, monitor, and defend themselves against such warfare.

Along with Ravich, three of the authors of chapters in the report—Juan Zarate, Mark Dubowitz, and Michael Hsieh—assembled at the Hudson event to present brief summaries of their papers. They were joined by fellow expert panelists Steve Chabinsky, Mike Rogers, and Mark Tucker, as well as by an audience of approximately 125 invited policymakers, business people, scholars, and journalists to discuss the report’s findings. Together with the Hudson Institute, the event was co-hosted by the Foundation for Defense of Democracies’ Center on Sanctions and Illicit Finance. All those in attendance were invited to complete a survey on cyber-enabled economic warfare constructed by Ravich, and approximately half did so. The results are discussed later in this report.

Sections I and II of this paper provide synopses of the panelists’ presentations at each of two panel sessions comprising the event. (The CSPAN broadcast is available at http://www.cspan.org/video/?327438-1/juan-zarate-former-representative-mike-rogers-cybersecurity-threats). Section III provides a brief summary of the survey and its findings. Finally, Section IV offers a recap of the main conclusions from this project, including policy recommendations and suggested topics for further research.

I. SUMMARY OF FIRST SESSION ON THREATS

A. Samantha Ravich’s Introduction. Samantha Ravich is CEO of A2P, LLC, a social media analysis firm. She was Co-Chair of the congressionally-mandated National Commission for Review of R&D Programs in the U.S. Intelligence Community. Previously she was Deputy National Security Advisor to Vice President Cheney and served in the White House for 5½ years. She has served as an advisor to numerous U.S. intelligence agencies and was the principal investigator for this project.
This 18-month project has sought 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 investigated five fundamental questions regarding the contemporary evolution of cyber-enabled economic warfare:

- **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 are they evolving? How do the new, cyber-enabled methods link to more traditional forms of economic warfare?

- **Which actors pose the main threat to the U.S.**? Which adversarial states or non-state actors do, or could, have the intentions to pursue such a cyber-enabled economic warfare strategy against the U.S.? 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.?

- **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 homeland defense. But have these changes gone far enough to identify and counter the emerging new threats from economic warfare, particularly to U.S. critical infrastructure and the U.S. financial system?

- **How can the USG recognize, monitor, deter, defend, and defeat such warfare?** What additional skill sets would the U.S. government 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?

- **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 purpose of this project was not to provide definitive answers to these questions, but rather to initiate a robust, much needed debate. We hope that the monograph we produced will, along with the conference and other formal and informal briefings on the subject matter, serve that purpose.

The first speaker, Juan Zarate, contributed the chapter in the monograph on cyber-enabled economic warfare in the financial sector. His phenomenal book, *Treasury’s War*, explores the evolution and importance of this new era of economic warfare.
**B. 1st Speaker: Juan C. Zarate.** 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.

Zarate’s chapter within the monograph 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 smart sanctions campaign, Zarate is intimately familiar with the offensive “financial war” the U.S. 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 financial 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” through hacking, cyber-espionage, cyberfraud, 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.”

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, Zarate develops with substantial detail a provocative “new cyber-privatizing 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 one of the more thoughtfully provocative comments, Zarate suggested that, “Perhaps some tailored hack back capabilities, in particular instances, with cyber warrants when the government gives license to the private sector to protect its systems, go and destroy data that’s been stolen or maybe even something more aggressive” should be examined. During the Q&A, Zarate expanded upon this by adding that:

> A cyber privateering model frankly takes straight from our Constitution. The founding of our republic came at a time when there was much unease about maritime security. We have a provision in the Constitution for letters of mark and reprisal for the government to actually leverage privateers in the maritime security domain, precisely because there was
this blend of threats and this blended environment. I think we need to look a little more aggressively because the environment itself doesn't differentiate between public and private. We don't want to do damage to our Constitution or the way we foster the private sector and protect it, but we also can't ignore the fact that the private sector whether it's Sands, Sony, JPMorgan are a part of our national resilience and economy.

Zarate concluded his prepared remarks by advocating the improvement of U.S. deterrence capabilities, potentially to include offensive and retaliation strategies, as well as developing the redundancy of our systems so it becomes less attractive as a strategic tool for our adversaries.

C. 2nd Speaker: Steven Chabinsky. Steve Chabinsky is General Council and Chief Risk Officer for the cybersecurity firm CrowdStrike. Prior to joining CrowdStrike, he had a distinguished 17-year career with the FBI, culminating in his service as Deputy Assistant Director of the FBI's Cyber Division. Prior to that role, he was the cyber advisor to the Director of National Intelligence, after having organized and led the FBI’s Cyber Intelligence program and serving as the FBI’s top cyber lawyer.

Chabinsky confirmed the main points of Zarate's analysis and added at the outset his assessment that the U.S.'s current strategy for responding to cyber-enabled economic warfare threats is failing. He then provided a brief overview of the numerous alternative ways in which adversaries can attack U.S. economic systems, including methods that entail stealing confidential information as well as those that rely upon data transformation and sabotage. Such attacks may occur via remote access; via supply, distribution, or service relationships; or via hostile insiders, among others. The scope and complexity of the rapidly expanding threat possibilities mean that U.S. vulnerabilities are enormous.

Chabinsky argued that the U.S. response has been terribly misguided and ineffectual. The focus has been to spend vast amounts of resources on a single model of protection, vulnerability mitigation. But this is a fool’s errand because determined adversaries can almost always find a way to defeat virtually any vulnerability mitigation scheme. Much of the U.S.‘s expenditure has simply encouraged adversaries to become more sophisticated, and hence more dangerous. So the currently dominant mitigation model has actually become counter-productive and rendered the U.S. more vulnerable.

What is needed instead is to adopt a new model—to refocus U.S. efforts so that in addition to continued progress on vulnerability mitigation, the U.S. also focuses on penalty-based deterrence. This includes technical dimensions of enhanced detection of hostile cyber activities and attribution of their source. It also requires development and imposition of penalties that matter. So the predominant focus of the new model has to be threat deterrence, and the U.S. needs to use all elements of national power in its pursuit, including diplomatic, informational, military, economic, and law enforcement.

Chabinsky ended his remarks with this clarion call:

The economy that's being driven through technology can face a consumer confidence backlash and unfortunately citizen confidence, if we feel that the country cannot protect
us and is actually subject to extortion at any given time. In this country, we have police forces who routinely are being extorted through ransomware in which organized criminals are breaking into police force computers and telling them, “If you don’t pay us our ransom fee, we’ll delete or destroy or just not allow you ever to have access again to all of your records,” and police forces are paying extortion to foreign criminals. What happens when that happens at a nation-state level against us? Is it already happening and you just haven’t been apprised of it?

D. 3rd Speaker: Chairman Michael Rogers. Mike Rogers, currently a CNN National Security Commentator, previously served seven terms in Congress from Michigan’s 8th congressional district, and was Chairman of the House Permanent Select Committee on Intelligence. He has also served as a special agent in the FBI and in the U.S. Army, and is widely recognized as a foremost expert on cybersecurity, counterterrorism, and national security policy.

Rogers began by stating there are two problems that have developed in the past decade that Americans do not talk much about: the U.S. has had a strategic erosion in its dominance in both space and cyberspace. In space, China and other countries have ended the U.S.’s uncontested dominance, particularly vis-à-vis satellites. In cyberspace, the situation is worse: the U.S. is in a cyber war, and is not winning.

For example, the U.S. financial system is under constant attack. U.S. critical infrastructure has been penetrated repeatedly and proven vulnerable. Autos and airplanes have been hacked. Everywhere Americans are adopting upgraded technologies tied into the Internet of Things that render products and systems even more vulnerable. In 2014, there was a year-over-year 54% increase in targeted economic espionage against American businesses. Why? Because there are no consequences.

Rogers asked rhetorically, what is the U.S. government doing about it? One area where there is broad agreement on a need for improvement is business-government cooperation. Yet dysfunction among the House, the Senate, and the White House is so great that they have been unable to agree upon a solution despite trying for several years. He asserted that cooperation among the intelligence agencies is not much better.

In the meantime, the Russians, the Chinese, the Iranians, and unfortunately now the North Koreans—and up to at least 15 other nation states—are already on our networks. They’re stealing our information pretty much daily with ease, and again, with no consequence. In 2014, two nation states, Iran and North Korea, launched devastating attacks for political reasons on two businesses operating in the U.S. (the Sands Resort Casino and Sony Pictures). And as other panelists have stated, there was no deterrence.

Rogers concluded:

It’s not going to stop, and our adversaries are only increasing their cyber capabilities to do harm. And the massive thefts of personal data that they are routinely perpetrating, such as those at the Office of Personnel Management (OPM), will continue to greatly facilitate their ability to use spear phishing emails to penetrate our systems. Yet we mostly continue to yawn and look the other way. We have really serious problems brewing.
II. SUMMARY OF SECOND SESSION ON VULNERABILITIES AND PATHS FORWARD

A. Ravich Introduction. Ravich and the audience thanked the first set of panelists for an excellent discussion of the threats dimensions of the problem. While the second group of panelists were getting seated, Ravich read a quote from a 1959 treatise by Bernard Brodie called *Strategy and the Missile Age*. The quote called for new ideas and scholarship to deal with the new problems posed by the Atomic Age. “There's an intellectual no man’s land where military and political problems meet. We have no tradition of systematic study in this area and thus few intensely prepared experts.”

Ravich pointed out that a similar gap exists today at the intersection of military, political, and economic problems posed by the Cyber Age. The ‘kill chain’ of needed capabilities, so to speak, may have to be thought about differently. Nonetheless, she suggested, it’s basic elements—intelligence and warning, deterrence, detection, forensics, interdiction, battle management, consequent management and recovery—can serve as a useful way to gauge our current capabilities and create the doctrine and technologies that we need going forward.

Ravich then introduced the three speakers for the second panel session on Vulnerabilities and Paths Forward: Mark Dubowitz, Michael Hsieh, and Mark Tucker.

B. 1st Speaker: Mark Dubowitz. 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. He has advised the U.S. administration, Congress, and numerous foreign governments on sanctions issues. 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.

Together with Annie Fixler, Dubowitz co-authored the project monograph’s first chapter entitled, “Cyber-Enabled ‘Swift’ Warfare: Power, Blowback, and Hardening American Defenses.” The chapter addresses the U.S.’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 U.S.’s 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.”4 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 the 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.” Dubowitz and Fixler explain why expulsion from the SWIFT system is such a powerful instrument, and how the U.S. successfully employed it against Iran in a particularly important case.

During his remarks at the conference, Dubowitz discussed how the U.S. may have opened Pandora’s box and pondered whether we are prepared for the follow-on actions as other nation states use SWIFT-like offensive tools:

We’ve seen our adversaries try to take our playbook on Iran and use it in other ways. In Russia, the Russians are using economic warfare (through energy) against our allies in central Europe and Eastern Europe, leveraging the dependence that our European allies have on Russian national gas. There have been a whole series of escalatory measures—offensive measures against Russia because of its annexation of Crimea and invasion of Eastern Ukraine, retaliatory measures by the Russians against our allies and against the United States, and the recognition of the need for defensive measures. In the Asia Pacific region, the Chinese have used economic warfare and political warfare against Taiwan, for example, for years to persuade the international community that Taiwan should not be recognized as an independent state. The Chinese cut off the export of rare earth minerals for a couple of months when there was a dispute with the Japanese. Those rare earth minerals are critical to key industries of the Japanese economy. In the South China Sea, there have been significant territorial dispute between China and the Philippines and Vietnam and Japan and other countries. The Chinese have matched their naval maneuvers with economic coercion. It is becoming clear that our adversaries are learning from us the power of economic warfare, the power of economic coercion as a dominant instrument in the course of statecraft.

In response to a question regarding how the USG should be organized to deal with a problem where boundaries between and among public and private, state and non-state, legal and illegal, all blur, Dubowitz responded that he believes the USG has begun to take some tentative steps but has not done nearly enough to create a “defense of economy shield.” He applauded the creation of CyberCommand but stressed that, in this area, the responsibility for the analysis and thoughtful creation of policy should reside at the Treasury Department. He specifically recommended the creation of an Office of Policy Planning at Treasury and, more provocatively, an actual Economic Warfare Command, “with all the powers to work at an inner agency level, to actually think through both on the cyber side and on the traditional economic warfare side.”

C. 2nd Speaker: Michael Hsieh. 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. Previously, he was a research scientist at SAIC and a scientific consultant at Booz Allen Hamilton. The ideas he expressed both at the conference and in the monograph were solely his own and did not reflect the thinking or policy of DARPA or the USG.
In Chapter 3 of the project monograph, “Intellectual Property Piracy as Economic Privateers,” 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 seriousness of 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 readers through a quick case study of the U.K.’s analogous difficulty, and ultimate inability, to protect the intellectual property assets underlying its economic pre-eminence during the Industrial Revolution and afterwards. Ironically for readers of this monograph, it was the U.S. that 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.”6 Hsieh uses the U.K. case to illuminate core difficulties for the U.S.’s attempts to protect its vital intellectual property interests today. In so doing, 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 U.K.’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 in past epochs of IP theft.”7

Hsieh 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.”8 He stresses that U.S. policymakers must take advantage of the ingenuity of the American economic system that has produced so many value creating, world-changing ideas and help focus it as a means of defense to protect those very ideas.

Hsieh poses two questions regarding this idea: Can we use technology and economics to deter economic decision makers from deciding to steal as opposed to not steal? Can we raise the technical cost of stealing to such high levels that it no longer becomes worthwhile to do so? He answers his own questions in the following way:

Today, commercial software is effectively defenseless against being robbed of its deep IP by reverse engineers because the state of the art in defending software against such theft largely consists of inserting passive code to inveigle the attacker by essentially giving him more code to read and to understand. However, this security through obscurity approach can almost always be defeated in under a day with standard software tools. It’s almost universally regarded as ineffectual among software security experts.
Hsieh continues that:

The good news is that a recent mathematical breakthrough by UCLA computer scientist Amit Sahai and collaborators has opened up the door to making new kinds of software that can baffle even the best resource reverse engineers. The new approach entails writing the source code in such a way that unraveling its inner commercial secrets is equivalent to computing a mathematical problem whose solution provably requires lifetimes of effort even with the most powerful supercomputers and algorithms known today. This is exciting because this is the kind of technological breakthrough that could be the impetus for imagining a future where IP rights are protected not by the laws of governments or nations but the laws of mathematics.

D. 3rd Speaker: Mark Tucker. Mark Tucker is the founder and CEO of Temporal Defense Systems and founding board member of the Cyber Insurance Company of America. At TDS, he leads a team of experienced white hat hackers and technologists that are redefining the technology and security paradigm to safeguard competing devices and networks in the cyber war era.

Tucker began by reviewing some basics of the problem, which he noted is still somewhat elusive. First he focused on what is meant by “cyber-enabled economic warfare” and emphasized that it really is about warfare, not crime. Second, it is not some speculative future possibility, but rather a reality that has already commenced. Tucker pointed to Stuxnet as the launch point because it was the first time a cyberattack actually caused major physical damage. Third, he compared the dynamics of cyber-enabled economic warfare to low intensity conflict as a type of warfare, and not, for example, to the nuclear war era. For example, cyber warfare capabilities are much easier to acquire and have already proliferated.

Tucker then assessed the stage of development of this low-intensity conflict and compared it to events in Iraq in 2004: after the U.S. invasion, there was a power void. Criminal gangs were forming and there was sporadic violence, but it was not until the next stage that the violence began to become coordinated, escalated, and pervasive. Tucker stated that we currently are moving out of the cyber crime era; as increased coordination within and among state and non-state actors is rapidly developing, the attack curve is steepening. The attacks are escalating on the financial system, on infrastructure systems, and corporations’ and government organizations’ critical data. But the transition to a much more profound state of cyber conflict has not yet occurred—we stand on the cusp of it, still in a relative power void where the conflict is as yet barely formed.

The U.S. should be using this interim to get ahead of the conflict curve. This entails planning in order to anticipate and redirect the next stage of cyber conflict.

At this point, Tucker strongly took issue with the comments of some of the previous speakers, particularly Steve Chabinsky. Chabinsky had argued persuasively that the U.S. paradigm was almost completely, and wrongly, focused on vulnerability mitigation. Both he and some other panelists specifically asserted that, in this regard, it is wrong-headed to try to hold information technology manufacturers responsible for the cyber vulnerabilities within their products. But Tucker strongly disagreed. He made a
compelling case for taking actions that would, in effect, use the market mechanism to
induce manufacturers to invest significantly more resources in greatly strengthening the
cybersecurity of their products.

Tucker raised an excellent point: currently we lack a practical way to rate the degree of
cybersecurity (or extent of vulnerability) built into various information technology
products and services. This is because there has been so little focus upon it, and therefore
very little effort to produce a practical system of reliable, quantifiable security ratings. But
this is a hurdle that can, and should, be surmounted. Tucker asserted that his firm, as well
as others, are working to develop the metrics necessary for quantification of cybersecurity
ratings to succeed. Once that begins to catch on, the market will then adopt it as a
purchase criterion. That will then initiate a virtuous cycle of dramatic reductions in
products’ and services’ cyber vulnerabilities, especially if insurance companies adopt it as
a cornerstone of the fast growing market for cyberattack insurance products.9

Finally, Tucker emphasized that this improvement does not require a change in liability
laws and regulation, as some have called for, but rather simply capitalizing on the power
of the market.

E. Ravich Conclusion. Before moving to the Q&A period, Samantha Ravich offered a
couple of clarifications. First, she reminded the audience that from the outset of this
project, the intention was to call attention to today’s rapidly advancing dynamics of cyber-
enabled economic warfare and to help create a larger group of people that are interested
in this topic so that they can take on different pieces of the research and move it forward.
This project was never intended to be definitive.

Second, the project has in fact identified numerous areas where policy change and
additional research are urgently needed (these are summarized below in the final section
of this paper). Both of the panels during the conference showcased several places where
policy and new technologies come to bear. One in particular is deterrence.

Hudson Institute co-founder Herman Kahn once identified six desirable characteristics
of a deterrent: “A deterrent, to be successful, must be frightening, inexorable, persuasive,
cheap, non-accident prone and controllable.”10 Ravich mused:

If we just even start with those six things—you can imagine having the policy makers, the
war fighters, the technologists around a table saying, “All right, look. Here’s the problem.
How do we create a deterrent that both rests with sound policy doctrine and the
technologies to be able to do what Kahn recommended?” I think we would really move this
conversation ahead.

III. Questionnaire Results

As a means to gain some measure of the validity of this project’s findings and the extent
to which its concerns are publicly shared, Samantha Ravich constructed a brief survey (16
questions, most close-ended) regarding the project’s principal research questions. (For those interested in reviewing it, the brief survey is available here: https://fdd.wufoo.com/forms/cyberenabled-economic-warfare-survey/). Hudson Institute distributed the survey in advance to all of the approximately 125 attendees at the August 3 event.

The survey began with a formal definition of the key term “cyber-enabled economic warfare”:

“Cyber-enabled economic warfare” refers to a hostile strategy involving non-kinetic attacks upon a nation’s economic targets via cyber technology with the intent to degrade the target nation’s security capacity.11

Respondents were instructed to use that definition throughout the survey.

A. Demographics and Limitations. Nearly half of the audience in attendance at the August 3 Hudson event completed the survey. Of these, 45% work in government (all but one in the federal government); 41% in the private sector; and the rest in a think tank or academia.

Half assessed themselves as either “very informed” or “expert” about cybersecurity, while 37% indicated they were “somewhat informed” about it and 13% identified themselves as “not very informed.” In discussing the survey results, where germane we therefore include examination of differences between well-informed (i.e. “very informed” and “expert”) versus less informed (i.e. “somewhat informed” and “not very well informed”) respondents.

It should be noted that both the limited size and convenience nature of the sample prevent anyone from drawing statistically valid results from it. Moreover, because the survey was completed by those attending the conference, it is likely that the results contain some selection bias—e.g. respondents are more likely to take cybersecurity matters seriously, view them as more threatening, be concerned about U.S. vulnerabilities, etc. We thus report the findings not as definitive, but rather as suggestive. Nonetheless, the results are strong enough and consistent enough that they do lend some credibility to many of this project’s main findings.

B. Threat Assessment. Five questions within the survey pertained in different ways to threat assessment; the three with the most interesting results are summarized below. The first of these was the broadest. It asked individuals to rate how serious a threat does cyber-enabled economic warfare by other state and/or non-state actors currently pose to the U.S. There was a very widely shared perception that the threat is real. 95% of respondents said it was either “moderately serious” or “very serious,” with fully 70% of those knowledgeable about cybersecurity rating the threat “very serious.” No one said it was “not serious,” and only 5% said it was only “somewhat serious.”

A second question asked respondents to rate how serious is the threat posed by each of the following types of actors:
Hostile states were rated as posing the greatest threat, both individually and in collaboration with other states. Consistent with the results of the previous question, 68% rated hostile states as a “very serious” threat, while only one person rated them as “not serious.” Collaborating hostile states were considered almost as dangerous, with 64% rating collaboration among hostile states as a “very serious” threat and only 5% rating it as “not serious.”

The ratings fell substantially for the threat posed by terrorist groups and criminal groups. Only 28% rated the threat of cyber-enabled economic warfare posed by terrorist groups as a “very serious” threat, while 38% regard it as “moderately serious” and 28% regard it as “somewhat serious.” Similarly only one third of respondents rated the threat of cyber-enabled economic warfare posed by criminal groups as “very serious,” while 34% rated it as “moderately serious.”

The threat ratings rose substantially, however, when terrorist and criminal groups were evaluated as potential collaborators with hostile states. 82% rated hostile states collaborating with terrorist groups as posing either a “serious” or “very serious” threat, with more than half rating the threat as “very serious.” The ratings for hostile states collaborating with criminal groups were virtually identical. Moreover, 60% of those claiming to be cybersecurity experts rated the threat of cyber-enabled economic warfare posed by hostile states collaborating with criminal groups as “very serious.” These results suggest that there is a public perception that the threat of cyber-enabled economic warfare posed by both terrorist and criminal groups is much greater when they operate in collaboration with hostile states.

A third question asked respondents to rate how serious is the cyber-enabled economic warfare threat posed by each of the following specific state and non-state actors. The list below is reorganized in terms of the strength of the perceived threat:

<table>
<thead>
<tr>
<th>Not Serious</th>
<th>Moderately Serious</th>
<th>Very Serious</th>
</tr>
</thead>
<tbody>
<tr>
<td>China</td>
<td>0%</td>
<td>10%</td>
</tr>
<tr>
<td>Russia</td>
<td>0%</td>
<td>25%</td>
</tr>
<tr>
<td>Iran</td>
<td>3%</td>
<td>41%</td>
</tr>
<tr>
<td>North Korea</td>
<td>3%</td>
<td>33%</td>
</tr>
<tr>
<td>ISIS</td>
<td>11%</td>
<td>30%</td>
</tr>
<tr>
<td>Al-Qaeda</td>
<td>15%</td>
<td>25%</td>
</tr>
</tbody>
</table>

Nearly everyone (95%) rated China as a serious threat, with Russia not far behind. These are very high ratings and consistent with the findings of this project that the U.S.
urgently needs to upgrade its defenses against cyber-enabled economic warfare threats. They are also consistent with the fact that “classified National Intelligence Estimates over the past five years have identified Russia and China as the United States’ most sophisticated, and prolific, adversaries in cyberspace.”

On the other hand, it is perhaps surprising that only 31% of respondents consider Iran’s threat “very serious.” It seems that many do not understand the resources Iran has dedicated and the progress it has made in developing its offensive cyberattack capabilities in the past four years or the extent of the attacks it has already launched on the U.S. banking and financial services community as well as on many other targets in the U.S. and abroad. This record is particularly alarming because of the Iranian regime’s profound animosity to the U.S.; its extensive record of supporting terrorist attacks against the U.S. and its allies; and its proven willingness to go beyond cyber reconnaissance, theft and nuisance attacks to serious cyber destruction. So the consensus of the authors contributing to this project’s monograph is that despite its inferior technical capabilities, Iran, like China and Russia, poses a very serious threat of waging cyber-enabled economic warfare (as well as cyber terrorism) against the U.S.—and indeed, probably has been conducting a low-grade version of it for much of the past four years.

About half of respondents rated North Korea’s cyber-enabled economic warfare threat to the U.S. as either “moderately serious” or “very serious.” Clearly North Korea’s offensive cyberattack capabilities are not to be taken lightly. For example, many believe it was responsible for the sizeable March 2013 cyberattack against South Korea’s commercial and media networks that damaged tens of thousands of computer workstations and disrupted online banking and ATM services. North Korea has also been officially identified by the U.S. as responsible for the highly destructive cyberattack on Sony Pictures last November, which DNI Director James Clapper early this year called “the most serious and costly cyberattack against U.S. interests to date.”

Respondents provided a similar assessment of ISIS as they did North Korea, with Al-Qaeda regarded as a somewhat weaker threat. Regarding the cyber threat from these two terrorist groups, U.S. law enforcement officials have indicated that they view them with more alarm, although more for their aspirations and potential capabilities than their current skills. For example, last July, senior Justice Department cybersecurity official John Carlin stated that: “Terrorists are also using cyberspace to further their goals. They are using it to communicate and plan. They are using it for propaganda and recruitment. And they are intent on getting to the point where they can conduct cyberattacks themselves.”

In a similar vein, FBI Director Comey testified last fall to the House Homeland Security Committee: “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.”

Additionally, while we did not ask further specific questions about collaboration between any particular hostile states and non-state actors, we note that the respondents’ concerns
about such collaboration, discussed above, are supported by assessments from the U.S. intelligence community as well as numerous independent researchers. Findings produced last summer by the former members of the 9/11 Commission provide a noteworthy example:

Security officials are concerned that terrorist groups’ skills in computer technology—and in particular in manipulating offensive cyber capabilities—will increase in the years ahead. Terrorists may also seek to acquire malicious software from adversary nations or from hackers who are proficient at malware coding. This will make an already unpredictable and dangerous cyber realm even more so.20

C. Vulnerabilities and Areas for Improvement. The survey contained five questions about various aspects of U.S. cybersecurity vulnerabilities and areas in need of improvement. Rather than cover each in detail, we summarize the findings and offer a few more specific highlights.

First, to the most general question, no-one said that the U.S. is “very well prepared” to address existing threats of cyber-enabled economic warfare, and only 5% said it is “well prepared.” Rather, fully 95% of respondents rated the U.S. as either “somewhat prepared” (47%) or “not well prepared” (47%). This is a pretty dismal indictment, but no more so than has been provided on many occasions by leading U.S. Intelligence officials. 21

Second, almost 80% of respondents indicated that the U.S. has done a poor job of designating who—or even which agency—in the government bears primary responsibility for “identifying, assessing and responding to existing threats of cyber-enabled economic warfare against the U.S.” Recall that almost half the respondents are federal employees, and approximately half of them consider themselves to be very informed or expert about cybersecurity. So this response points to an ominous problem with how the U.S. government has organized to combat cyber threats.

Moreover, the problem is not simply organizational. It also entails serious staffing and training deficiencies. 72% of respondents indicated that the U.S. is not adequately staffed to cope with the threat of cyber-enabled economic warfare. Regarding training, 90% rated the need for improved training of government personnel for responding to the threat as “serious” or “very serious.”

The evaluation of U.S. capabilities was even worse. 97% of respondents rated the need for new government capabilities for responding to the threat of cyber-enabled economic warfare as either “serious” or “very serious,” with almost 60% rating the need “very serious.”

To gain a somewhat different perspective on these issues as well as to try to confirm the reliability of these very negative ratings of U.S. preparedness, the survey contained a question that asked respondents to evaluate the need for each of eleven possible corrective actions. The options are listed below in order of their rated need for improvement:22
<table>
<thead>
<tr>
<th>Action</th>
<th>Not Serious</th>
<th>Moderately Serious</th>
<th>Very Serious</th>
</tr>
</thead>
<tbody>
<tr>
<td>Increase U.S. capabilities to deter cyber-enabled economic warfare</td>
<td>0%</td>
<td>25%</td>
<td>68%</td>
</tr>
<tr>
<td>Improve government and private sector cybersecurity cooperation</td>
<td>2%</td>
<td>25%</td>
<td>67%</td>
</tr>
<tr>
<td>Increase training for government experts on cyber-enabled economic warfare</td>
<td>0%</td>
<td>29%</td>
<td>58%</td>
</tr>
<tr>
<td>Create more accountability for government cybersecurity failures</td>
<td>0%</td>
<td>30%</td>
<td>53%</td>
</tr>
<tr>
<td>Develop and apply lessons from U.S. experiences with economic warfare</td>
<td>2%</td>
<td>30%</td>
<td>52%</td>
</tr>
<tr>
<td>Reorganize cybersecurity responsibility within the government</td>
<td>7%</td>
<td>23%</td>
<td>51%</td>
</tr>
<tr>
<td>Strengthen the international legal regime for cybersecurity</td>
<td>5%</td>
<td>36%</td>
<td>46%</td>
</tr>
<tr>
<td>Improve cooperation with allies on cybersecurity</td>
<td>2%</td>
<td>40%</td>
<td>42%</td>
</tr>
<tr>
<td>Hire more specialists on cyber-enabled economic warfare</td>
<td>2%</td>
<td>36%</td>
<td>41%</td>
</tr>
<tr>
<td>Increase government spending on cybersecurity</td>
<td>5%</td>
<td>35%</td>
<td>31%</td>
</tr>
<tr>
<td>Create a new entity focused on cyber-enabled economic warfare</td>
<td>14%</td>
<td>16%</td>
<td>34%</td>
</tr>
</tbody>
</table>

Improved deterrence and improved business-government cooperation were rated as the top priorities, with approximately two-thirds of respondents indicating the need for each was “very serious.” The latter has been a major focus of cybersecurity policy in the U.S. for the past several years, though with limited success to show for it. The former—improved deterrence—has become an increasingly recognized major shortcoming in the past year or so especially, and is one of the major policy recommendations of this project.

Increased training for government experts on cyber-enabled economic warfare, and more accountability for government cybersecurity failures followed closely as the next highest rated needs; approximately 84% rated the need for these as “moderately serious” or “very serious.” One other action was regarded by more than half of respondents as a very serious need: Develop and apply lessons from U.S. experiences with economic warfare. This is a unique recommendation to arise from this project and one we explain further in the next section of this paper.

Two international dimensions—strengthen the international legal regime for cybersecurity, and improve cooperation with allies—were rated similarly, with both
viewed as moderately or very serious needs by 82% of respondents. Respondents gave just a little less support for hiring more specialists on cyber-enabled economic warfare, 77% rating it as a moderately serious or very serious need.

Finally, of the eleven possible action items, increased government spending on the problem and ‘create a new entity’ were rated lowest. Most respondents seem convinced that throwing money at the problem is not the main solution, but that much more specific fixes are needed instead. Given the proliferation of government cybersecurity entities in the past few years, it is not surprising that few respondents were enthusiastic about the need to create yet another one.

In summary, then, this survey is admittedly a limited instrument, yet its findings do provide some support for many of the major findings of this project. The threat of cyber-enabled economic warfare to the U.S. is very serious. While individual hostile states pose the greatest threat (most notably Russia, China, and Iran), collaboration between hostile states as well as collaboration between at least some of these same states and either criminal or terrorist groups are also major concerns.

Additionally, it is broadly recognized that the U.S. is currently not at all well prepared to handle these threats. Most seem to acknowledge that our cyber adversaries are currently winning. And there is no shortage of opportunities for substantial improvements.

Having reviewed the main findings of the survey of event participants, we turn now to the final section of this report, wherein we summarize the main policy lessons and research findings from this project.

IV. CONCLUSIONS, POLICY RECOMMENDATIONS, AND SUGGESTIONS FOR FURTHER RESEARCH.

Initial research on this project commenced in the summer of 2014. Its purpose was to investigate whether the U.S. is at serious risk of being blindsided by what we term cyber-enabled economic warfare. Since then the chapter authors did a considerable amount of work, first researching and drafting their chapters; then revising them for presentation at a two-day Hudson Institute conference last November; then revising them again after receiving feedback from the conference participants and PI Samantha Ravich; and then adding final revisions and submitting the chapters in April. The chapters were then edited by Ravich, who added her own introductory and concluding chapters before turning over the monograph to Hudson Institute staff for final copyedits, formatting, and printing.

Meanwhile, Ravich and other chapter authors continued to share and discuss their work with interested researchers and practitioners in cybersecurity, intelligence, and related fields. Based on those discussions, Ravich constructed the survey discussed in Section III of this paper, above. Hudson Institute staff managed the distribution and data collection processes for the survey. On August 3, the Institute hosted a half day seminar to help
publicize the monograph and provide a final opportunity for those interested in the subject to convene and exchange ideas.

From all this work and reflection, PI Ravich has drawn together her final conclusions from the project. These conclusions are largely a product of informal joint consensus among the project’s chapter authors and are generally, though not necessarily unanimously, shared by them. They are presented below in two parts: first, policy lessons; and second, priorities for future related research.

A. Policy Lessons. No one doubts that the U.S., in general, has greatly increased its awareness of very serious threats arising from a wide variety of potential and ongoing 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, however, 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. Tenth year anniversary findings from the former commissioners of the 9/11 Commission lend credence to this conclusion. The report that they issued last July specifically pointed to the growing significance of cyber threats to the U.S. government and private sector. They noted ominously: “We are at September 10th levels in terms of cyber preparedness.” They added, “American companies’ most-sensitive patented technologies and intellectual property, U.S. universities’ research and development, and the nation’s defense capabilities and critical infrastructure, are all under cyberattack.”

A senior Department of Justice official recently offered a reinforcing depiction of the economic magnitude of cyber crime and the rate at which it is growing: “A study from last summer estimated that cybercrime costs the global economy approximately $400 billion annually. A study from this past May projects that, by 2019, cybercrime will cost businesses worldwide $2 trillion per year.”

In their report, the former 9/11 Commissioners concluded: “One lesson of the 9/11 story is that, as a nation, Americans did not awaken to the gravity of the terrorist threat until it was too late. History may be repeating itself in the cyber realm.”

Below we discuss eight areas where corrective policy actions are urgently needed.

1. Recognize that cyber-enabled economic warfare is happening and that the U.S. is not prepared for it. It is readily apparent that the private, government, and academic sectors are all devoting a considerable amount of resources to improving U.S. defenses against cyberattacks from state and non-state threat actors. Usually, the problem is framed either as cyberattacks in general, cyber warfare, or cyber terrorism. 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 state entities use cyber-enabled means to implement attack strategies (e.g. espionage, IP theft, sabotage, etc.) on economic targets designed to weaken an adversary’s economy; 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 terrorist groups, either independently or with state support, use cyber-enabled means to sabotage financial systems and other critical infrastructure within an adversary’s economy in order to weaken it; these circumstances likely constitute cyber-enabled economic warfare and need to be analyzed as such.

These types of scenarios, as well as others like them, are in fact already occurring, with the U.S. and its allies as targets. We recognize that it is fast becoming common for experts to acknowledge that cyberattacks pose a threat to the U.S. economy and thus to U.S. national security. Yet almost no one is analyzing cybersecurity events or threats in terms of economic warfare, much less economic warfare strategy. As Dubowitz and Fixler note in the monograph’s first 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.”

The fundamental drivers of the new economic warfare dynamic are easily identified. Quite simply, cyber-enabled economic warfare is escalating because the opportunities for conducting it are evolving so rapidly and because the potential gains from its successful pursuit are enormous. Both the U.S. and its adversaries are responding to, and also shaping through their choices, those opportunities. Yet little is being done to analyze the emerging dynamics in terms of economic warfare strategies.

The U.S. needs to deepen its understanding of how traditional economic warfare is being overtaken by cyber-enabled economic warfare and its accompanying strategies. This is an extremely important subject: in a competitive dynamic, changed possibilities almost inevitably lead to changes in practice. If the U.S. is to prepare for the latter, it would help greatly to understand the former.

2. Learn and apply lessons from the history of economic warfare. The U.S. has extensive experience with traditional economic warfare, both defensively and offensively. One need look back 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 and used economic warfare strategies extensively against Japan. 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. handily won. After the Cold War ended, the U.S. continued to use traditional economic warfare strategies to nurture and reward strategic allies as well as to punish foes, whether state or non-state actors.
It seems strange, therefore, that there is so little use of this rich 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 the cyber-enabled versions that are emerging today.

The U.S. needs to do a better job of learning from its own long history of experience with both offensive and defensive dimensions of economic warfare. The chapters by Zarate and by Dubowitz and Fixler in this monograph provide examples of how lessons can be drawn from recent U.S. offensive experience with cyber-enabled sanctions. Similarly, the study of sanctions more generally and their targets’ responses to them seems likely to offer fruitful ground for analyzing potential responses to cyberattacks.32 To note but one more example, the U.S. would probably be doing much better today in combating cyber theft if it had set out a few years ago to really study the problem in terms of economic warfare instead of uncritically assuming it to be essentially a problem of crime.

Moreover, the history of economic warfare is much broader than just U.S. experiences. The broader global history of economic warfare offers a bedrock of cases that similarly 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 3 in this monograph is a perfect example of how economic warfare lessons from prior campaigns (e.g. he examines U.S. theft of IP from Great Britain during the Industrial Age) can provide valuable insights into today’s challenges.

The U.S. government, as well as interested private foundations, should invest in research on lessons to be gleaned from this history. They should support studies within the analytic units of various government agencies, the War Colleges, think tanks, academia, etc. and help ensure the output is disseminated to policymakers in an appropriate fashion. It is unfortunate and unwise that 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. cyber security.33 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 prior to, and during, WWI and especially WWII—when both countries had important central government economic warfare bureaucracies, plans, strategies and initiatives.34

Another ancient Greek, Polybius, wrote that “it is by applying analogues to our own circumstances that we get the means and basis for calculating the future.”35 And the best analogies are historical ones.

3. Conduct rigorous threat analyses of hostile state actors, hostile non-state actors, and alliances among them—specifically in terms of cyber-enabled economic warfare strategy (e.g. intentions, interests, capabilities, perceptions, actions, alliances, etc.). One of the biggest reasons why it is essential to apply the language of economic warfare to today’s cyber security problems is that without it one is unlikely to be able to understand adequately the strategies that various threat actors are pursuing or the important differences amongst them. Currently, the U.S.
policy analysis community seems to lack a clear awareness that adversaries’ strategies for capitalizing on the changing cyber threat opportunity set will vary by adversaries’ individual circumstances and characteristics. China, Russia, Iran, North Korea, Syria, etc. all have different characteristics that are driving their own choices. The same is also true for the relevant non-state actors and for the interactions that are developing across these state and non-state entities.

So far there seems to be limited capacity for U.S. government understanding of these issues, and, therefore, no sound basis for adequate, properly coordinated response to the threats they are generating. For example, it is well known that Russia has extensive and very well developed cyber reconnaissance, espionage, criminal, and sabotage capabilities, both in the government and within a shadowy network of apparently private actors. Yet who has a clear understanding of Russia’s cyber intentions and how they fit into Putin’s grand strategy? How has Putin’s cyber theft of U.S. data and capabilities affected his planning and operations within Syria?

Similarly, the U.S. and China have just reached an agreement that “neither of their governments would conduct or condone economic espionage in cyberspace.”36 But how does President Xi’s tactical move fit within China’s larger (cyber-enabled economic warfare) strategy? How do China’s massive personal data thefts in the past two years fit into that strategy? Or the voluminous amount of malware that Chinese hackers have left lingering, apparently dormant for now, in U.S. private and government organizations’ IT systems across the nation? How do these issues connect to China’s ambition to dethrone the U.S. dollar as the world’s reserve currency? To their economic diplomacy?37 Where in the U.S. government are these and many additional related factors all being analyzed comprehensively, in terms of economic warfare strategy?

Similar types of questions must be asked about Iran and North Korea, at the very least. Did President Obama and his negotiators in the State Department have well-developed briefings on Iran’s cyber-enabled economic warfare strategy as they negotiated the recent nuclear arms agreement with Iran? If not, why not?

We see little evidence that the U.S. research, policy, or intelligence communities are conducting serious analyses of these issues, framed in terms of economic warfare. We believe this needs to change. To do so, it seems likely that a new threat analysis framework for cyber-enabled economic warfare must be developed. The U.S. certainly has the capacity for this work, and we hope that this project helps bring attention to the need for it.

4. **Commit to remedying major U.S. cybersecurity vulnerabilities faster.** As noted above, it is becoming common knowledge among informed individuals that the U.S. remains vulnerable to a wide variety of cyberattacks and cyber threat strategies. Obviously it is very dangerous to allow these vulnerabilities to persist, yet it seems the U.S. currently is failing to remedy them faster than the rate of progress being made by U.S. cyber adversaries’ in developing their threat capabilities.
It is beyond the scope of this project to examine these vulnerabilities in detail. But it is clear that many of them are already well known. The repeated thefts during the past two years of huge volumes of critical personal information from the Office of Personnel Management is a particularly glaring example of the inadequacy of U.S. progress on cyber security.\textsuperscript{38} We list below two of the areas where existing systemic U.S. cyber security shortcomings render the nation particularly vulnerable to cyber-enabled economic warfare:

- **Organization:** Who in the government bears primary responsibility for identifying, assessing and formulating responses to existing threats of \textit{cyber-enabled economic warfare} against the U.S.? Who is conducting such analyses? Where is the “whole-of-government” approach for addressing this problem? It appears that there is some thought of assigning this type of holistic, integrative threat analysis and dissemination function to CTIIC (Cyber Threat Intelligence Integration Center), the new cyber entity announced in February by President Obama.\textsuperscript{39} However, CTIIC is very small, has not been funded by Congress, is not really up-and-running yet, and may not possess either the appropriate personnel or the management mindset needed to conduct this work.

If CTIIC either cannot or will not be designated as the primary locus for analyzing, planning, and communicating the government’s response to cyber-enabled economic warfare threats, what is the alternative? Dubowitz and Fixler advocate a thoughtful solution that would unfold in two phases and entail establishing new economic warfare units within Treasury and the NSC.\textsuperscript{40} Their plan is worthy of serious consideration. Ultimately, however, even if their suggestions are rejected, the point that needs to be addressed is that responsibility for addressing cyber-enabled economic warfare threats needs to be formally tasked to an agency capable of performing it.

- **Staffing and Training:** Many experts have expressed concerns about the shortage of qualified cybersecurity professionals in U.S. government and industry.\textsuperscript{41} We add that experts on cyber-enabled economic warfare are undoubtedly rarer. Such individuals need a good understanding of not only the technical dimensions of cybersecurity, but also the economic, geopolitical, cultural, and strategic dimensions.

We believe that individuals with such expertise are needed in all of the major branches of government tasked with responsibility for ensuring the nation’s security from cyber threats. This would seem to include at a minimum the NSC within the Office of the President; the NCCIC within DHS; Cyber Command within the DoD and NSA; probably also the CIA as well as the NSA within the intelligence agencies; some unit within the State Department; and perhaps the FBI and the DoJ as well. We believe that most, if not all, of these entities, either lack the expertise to perform the proper analysis of cyber-enabled economic warfare threats; or have not assigned the personnel who could perform this work to the task; or more often both. This needs to be rectified.
Creating the types of teams that can both analyze the human and technical components of the threat of cyber-enabled economic warfare may require building new human-computer interfaces. Such cognitive computing and artificial intelligence are already being explored in the fields of medicine and big data analytics. The challenges of cyber warfare, however, may be particularly suited to a capability that leverages the mental dexterity and emotional intelligence of humans as well as the higher order processing speed of computers.\textsuperscript{42}

Other major shortcomings exist as well (e.g. cultural, technological, legal, behavioral, etc.), not least of which is the dysfunctional state of relations among the nation’s major political parties. What is needed is a major campaign to educate the public of the seriousness of the threat, and an “all hands on deck” commitment to address major vulnerabilities. As the former 9/11 Commissioners have warned, it would be tragic if it takes some type of cyber catastrophe to spur such change.

5. Use the free market to accelerate vulnerability mitigation. In the course of the two Hudson seminars for this project, it became clear that the dominant U.S. paradigm for addressing cyber security threats—vulnerability mitigation—is inadequate at best. As we discuss next, vulnerability mitigation cannot be effective without being accompanied by meaningful deterrence. Nonetheless, vulnerability mitigation as practiced currently can be substantially improved. One path that has been discussed extensively is through increased cooperation between business and government. Though some progress in this direction has been made, as Chairman Rogers noted, U.S. politicians have not yet found a way to overcome all political obstacles despite numerous attempts to do so over the past several years. As he emphasized, this needs to change.

But a second path for reducing vulnerabilities has received much less attention. As Mark Tucker pointed out, the U.S. could create a dynamic that likely would greatly accelerate systemic technological and organizational progress on vulnerability mitigation. How? By using one of the U.S.’s greatest strengths: the competitive market.

Companies generally have not been motivated yet to prioritize building a high degree of cybersecurity into their products and services. In addition to legal and regulatory deficiencies,\textsuperscript{43} this is due in no small part, as Tucker explained, to the fact that there does not yet exist a reliable, well-established system to quantify cyber “security.” In its absence, customers have a difficult time making security/vulnerability a major criterion within their purchase decisions.

What is Tucker’s proposed solution? Develop the metrics for quantifying a product’s or service’s degree of cyber security/vulnerability, then disseminate that system for public adoption. Consider for a moment how rapid technological innovation is adding to the consumer’s challenge of avoiding victimization from cyberattack:

In just the last few years, we have seen the dramatic growth of social networks, mobile, and the cloud, the emergence of the Internet-of-Things, wearable, 3D printing and the sharing economy, and in the near future we are likely to see drones and self-driving cars. These new products, services, business models, and interdependencies impact both the
form and likelihood of a cyber-attack occurring, and the nature and severity of the resulting loss.\textsuperscript{44}

It clearly seems both unreasonable and impractical to expect the consumer to bear the brunt of the responsibility for figuring out how to use these new innovations without becoming exposed to cyberattacks. Instead, more of this burden needs to be built into the design and maintenance of companies’ products and services. Cyber security ratings metrics (assuming they are practical and reliable) can help induce this outcome by spurring market demand for more secure products and thereby inducing companies to compete on this dimension much more transparently. The resulting innovations would feed through the marketplace and directly increase U.S. cybersecurity via mass adoption of a wide variety of accelerated cybersecurity improvements.

Tucker’s insight also extends to a second, and perhaps even more important, way that the market can be used to upgrade U.S. cyber security: by developing reliable metrics for assessing not just individual products and services, but an entire organization’s cyber security/vulnerability, and then applying those metrics in the mushrooming market for cyberattack insurance.\textsuperscript{45} Creating metrics for assessing the cyber vulnerability of an organization’s complete IT systems and practices as a whole instead of simply its individual products and services would enable insurance companies to assess risk more accurately, offer more appropriately priced liability insurance against cybersecurity failures, and thus increase the efficiency of that market. For example, while demand for cyber liability insurance is rapidly growing, insurers currently rely upon a considerable amount of \textit{ad hoc} and case-by-case risk evaluation methods when pricing cyber liability products.\textsuperscript{46}

Securing a cyber-liability policy will not be a simple task. Insurers writing this coverage will be interested in the risk-management techniques applied by the business to protect its network and its assets. The insurer will probably want to see the business’ disaster response plan and evaluate it with respect to the business’ risk management of its networks, its website, its physical assets, and its intellectual property. The insurer will be keenly interested in how employees and others are able to access data systems. At a minimum, the insurer will want to know about antivirus and anti-malware software, the frequency of updates and the performance of firewalls.\textsuperscript{47}

Currently, less than 20 percent of large companies have cyber insurance while less than 6 percent of small- and medium-sized companies have it.\textsuperscript{48} But:

The largest barrier to growth is lack of actuarial data about cyberattacks, but this is quickly changing with continued cyber assaults. Currently, insurers are finding it difficult to assign the proper value to data or systems, or to determine appropriate policies since they are unable to scope the cyber risk environment of an organization.\textsuperscript{49}

The lack of widely accepted benchmarks and scores make it difficult to measure the relative risks between one organization and another, or to rank different organizations with respect to their cyber security posture in a repeatable and independent manner.\textsuperscript{50}
So the lack of a reliable set of metrics for assessing organization cyber security risk is gaining recognition as a major impediment for enabling potentially virtuous cycle of the cyber liability insurance market to function well. Tucker’s company has created one entrant into this space, and others are beginning to enter it as well:

There are some tools being developed, but they are still new and unproven, and not standardized. For example, BitSight rolled out a security ratings service for cyber insurers based on its Security Ratings Platform, which analyzes publicly available data from its global sensors that track security events and malware behavior daily for organizations, specifically looking for botnet communication, malware distribution, and email server configuration. The scoring model is akin to consumer credit ratings, comparing how a company compares with other companies security-wise. For example, if a company gets breached, how many days did it take for them to mitigate the problem compared to other companies? Also, re-insurance broker Willis Re launched a tool (PRISM-Re) to help insurance companies gauge their portfolios’ exposure to cybersecurity risks.51

Taken together, improved cyberattack risk metrics, both for products and for organizations, can provide a powerful means for enabling the market to produce more rapid innovation and dissemination of more secure products and practices. We see this as a very promising path for accelerating U.S. cybersecurity improvements. U.S. government authorities should monitor these developments to determine whether legal or regulatory changes could facilitate the process.

6. Prioritize enhanced deterrence. As noted above, the U.S. clearly needs to do a much better job of deterring cyber threats: vulnerability mitigation must be complemented by enhanced deterrence. This is not a new discovery. The Bush administration identified it as a priority as long ago as 2008 as part of its Comprehensive National Cybersecurity Initiative (CNCI). The Obama administration concurred with this finding by at least as early as May 2009:

Initiative #10. Define and develop enduring deterrence strategies and programs. Our Nation’s senior policymakers must think through the long-range strategic options available to the United States in a world that depends on assuring the use of cyberspace. To date, the U.S. Government has been implementing traditional approaches to the cybersecurity problem—and these measures have not achieved the level of security needed. This Initiative is aimed at building an approach to cyber defense strategy that deters interference and attack in cyberspace by improving warning capabilities, articulating roles for private sector and international partners, and developing appropriate responses for both state and non-state actors.52

Looking back, it seems clear that while there was recognition of the need for deterrence, it was not accompanied by much insight into how to achieve the objective. Perhaps not surprisingly, this became yet another U.S. systemic cybersecurity problem that languished without much progress for the next few years.

More recently, at least some top U.S. officials responsible for cyber security have acknowledged this deficiency. DNI Director James Clapper analyzed the problem concisely in 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.53

Other senior officials share this concern and are trying 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.54 Pressed to explain how the U.S. could deter cyberattacks, Rogers explained his view:

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 cyber capability, jumped in to say, “But right now, the level of deterrence is not deterring.”

“That is true,” Admiral Rogers responded.55

Admiral Rogers has confirmed that U.S. Cyber Command is developing capabilities to use cyber counterattacks in order to punish those who initiate major cyberattacks on the U.S. The Obama Administration also is pursuing enhanced deterrence for cyberattacks through additional, non-military means. For example, in May 2014, the U.S. Department of Justice indicted five officers from the Chinese People’s Liberation Army on charges of hacking U.S. companies. This was intended as a warning shot across the bow and explicitly framed as a deterrence measure, though whatever fruit it may eventually bear does not yet seem visible.56

Very recently the president took a further step to strengthen U.S. cyberattack deterrence 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.57 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.”

The retaliatory sanctions EO was designed to deter in two ways:

First, imposing sanctions on an aggressive state may deter that country from engaging in additional belligerent behavior; and second, imposing sanctions on that state may also signal to other countries that, should they engage in similar activities, they too will be subject to punishing economic penalties.

Substantively, however, there are clearly reasons for concern about whether the enhanced development of offensive cyber capabilities by U.S. Cyber Command, or attempts at criminal prosecution by the U.S. justice system or the authorization of the limited types of sanctions contained in the president’s new EO, will serve as the intended deterrent. So far at least, it seems a case of the bark being bigger than the bite, and this kind of bluster does not generally succeed. Of the three, it is perhaps tempting to latch onto the power of retaliatory offensive cyberattacks—while the public does not really know what damage they could produce, few knowledgeable observers doubt that they have real potential ‘bite.’

As the U.S. moves further down the path of constructing and operationalizing deterrence, it is crucial to have a full awareness 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 described above, first on Saudi and Qatari oil and gas facilities in 2012, then on a number of large U.S. banks in a series of attacks from 2012 at least through 2013, 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.” Some have gone even further and speculated that the Iranian program has established functional links to enhance North Korean and Syrian cyber warfare programs. 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.

So while we encourage continued progress on building an effective set of cyberattack deterrents, we also believe that such tools require sound doctrine in order to be used effectively. To this, we turn next.

7. **Develop suitable 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 as well as for defensive dimensions essential for effective deterrence. The Department of Defense and U.S. Cyber Command seem to be moving in both these directions as they work to
establish doctrine specifically for cyber warfare, though their work needs to be better informed specifically by economic warfare concerns.

The need to develop new doctrine extends as well to non-military applications outside the Department of Defense, such as Treasury, State, certain intelligence agencies, and the NSC, etc. The current focus only on cyber warfare 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.

Applying our previous points about learning from relevant history, we provide 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. One small but important office within these bureaucracies was the Enemy Objectives Unit (EOU), 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....

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.65

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? Again we emphasize, the U.S. currently lacks any clear designation of this responsibility, and probably also lacks the personnel and intellectual tools to conduct this work effectively. Until this is remedied, solving the problem of creating clear and comprehensive doctrine will probably continue to fall through the cracks.

8. **Stop ignoring U.S. offensive cyber-enabled economic warfare initiatives.**

We noted at the beginning of our list of policy recommendations the somewhat surprising omission within U.S. policy communities of consideration of the history of conventional economic warfare and its relevance to understanding the emerging dynamics of cyber-enabled economic warfare. This blind spot is worsened 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,66 and perhaps even well back into the Cold War.67 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 methods and sources, and thus damage very valuable programs and capabilities, as seems to have happened following some of Edward Snowden’s unlawful disclosures about U.S. covert and clandestine 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 public discussion of the U.S.’s offensive cyber warfare and cyber-enabled economic warfare capabilities and initiatives. Certainly there has been significant authorized government acknowledgement of U.S. offensive cyber warfare 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.68 There has also been a significant amount of journalistic coverage of these issues in the past four years, particularly following the discovery of the Stuxnet malware and the extensive Snowden leaks.69 Nonetheless, these revelations have been limited, as fragmented exceptions, with the public discourse about the topic shrouded in mystery and speculation.

The relative paucity of public discussion of U.S. offensive cyber capabilities is damaging to U.S. interests in three 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 the U.S. poses to them. The chapters in this monograph produced by Zarate and by Dubowitz and Fixler are noteworthy exceptions, and doubtless there are others as well. 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 that 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.

Finally, it is difficult if not impossible to have a robust deterrent without the adversary grasping the pain they will suffer if they attack. If, how, and to what extent we should open the curtain on some of our offensive capabilities should be considered as part of our overall deterrence doctrine.

B. Future Research. Having developed eight policy lessons at some length, we complete the findings from this project with a more concise summary of a few of the many topics we see as needing near-term follow-up research.

1. Conceptual Work. One task we established for this project from the outset was to explore the construct, cyber-enabled economic warfare, and to identify a sound definition for it. An unanticipated problem was that the more general term, economic warfare, did not itself seem to have a consensus definition within the broad literature that pertains to it. Nonetheless, we adopted a working definition and used it in the survey described earlier in this paper. Upon further reflection, we would amend that definition somewhat, borrowing some of the language from George Shambaugh’s definition of economic warfare: “Cyber-enabled economic warfare refers to a hostile strategy involving non-kinetic attacks upon a nation’s economic targets via cyber technology with the intent to weaken its economy and thereby reduce its political and military power.” We think this captures the essence of the matter but have no doubt that others can improve upon it. So we invite others to pursue that task.

Perhaps more importantly, we believe the policy community needs better intellectual tools and framework(s) for investigating this subject further. For example, do appropriate U.S. government agencies even possess an adequate understanding of the intelligence requirements for properly identifying and assessing adversaries’ cyber-enabled economic warfare strategies? In the aftermath of WWII as the U.S. entered a new era of Cold War, the U.S. State Department and other relevant members of the U.S. government formally conducted a serious study of “intelligence for economic warfare” in order to accomplish three well-specified objectives: “The problem under discussion is: (1) to determine economic intelligence requirements under conditions of economic warfare, (2) to appraise the resources now available to meet them, and (3) to recommend the steps necessary to mobilize these resources to meet economic warfare requirements.”
We hope others will help develop these in a practical manner that will be conducive to adoption by practitioners.

Third, the policy community needs improved doctrine for guiding decisions about how to defend and conduct cyber-enabled economic warfare. Practitioners doubtless could use help from academic and think tank researchers in developing and testing such doctrine.

2. **History.** We believe strongly that current analyses of cyber threat topics could benefit enormously by development and application of lessons from relevant history. Identifying that history and developing sound lessons from it should not be a task only, or even principally, for the government. Academic and think tank research communities could provide valuable contributions here as well.

3. **Threat Actor Strategy Studies.** We have no doubt that the U.S. government expends considerable resources studying the cyberattacks in the U.S., current U.S. systemic vulnerabilities to those attacks, and cyber threats posed by the major threat actors identified in this paper (e.g. Russia, China, Iran, North Korea, Al-Qaeda, and ISIS). We also know that private sector researchers conduct a considerable amount of very good research on cyberattacks and related matters. We are skeptical, however, that this body of work either inside or outside the U.S. government adequately addresses the concerns we have raised in this project about cyber-enabled economic warfare. Most fundamentally, the focus of this work typically is on the cyberattack as the unit of analysis, rather than upon the strategy of the attacker. Consequently, the U.S. has been very slow to come to terms with the damage being done by years of escalating cyberattacks on U.S. assets. Worse, the failure to comprehend threat actors’ strategies means that the U.S. does not possess a good understanding of where the war is going. We are locked in a sustained reactive mode, slow to respond and continually behind the rapidly escalating behaviors of our adversaries. This is extremely dangerous and must change.

4. **Deterrence.** Again, it seems strange that the U.S. at the highest level of government identified deterrence as a critical shortcoming seven years ago with President Bush’s CNCI initiative, yet apparently completely failed to develop and apply vital lessons about deterrence learned in other critical national security contexts. Deterrence was absolutely foundational to the Cold War and to the U.S.’s ability to navigate the Atomic Age successfully. How did we miss asking the obvious questions, what can we learn and apply from what we’ve learned before? What is different that we must address in the cyber threat context? The way that the current administration seems to be tentatively lurching and blustering in the past two years to come up with some plan that will actually begin to deter the avalanche of cyberattacks being launched against the U.S. suggests that we still have not conducted this analysis or applied the important lessons.

There are plenty of academics who could outline the essential conditions for effective deterrence. What is needed is to apply these to the cyber warfare and cyber-enabled economic warfare contexts, and then develop an action plan for how to develop whatever capacities are currently missing from the equation. Some researchers are pursuing this already. But someone in government needs to shine a light on the problem and energize
a serious initiative to prioritize the research, develop the plan for implementation, and shepherd the plan through to completion.

What we have instead is seemingly wishful recitations like the one DNI Director Clapper provided to the Senate Armed Service Committee in September 2015:

Clapper and other top U.S. military officials said cyber threats were increasing in frequency, scale, sophistication and severity, and the United States needed the same kind of deterrent capability in cyberspace that it maintains for nuclear weapons. Attacks by countries such as Russia, China, Iran and North Korea, as well as non-state actors, would increase and likely grow more sophisticated in coming years, expanding to include manipulation of data, he said.

"Such malicious cyber activity will continue and probably accelerate until we establish and demonstrate the capability to deter malicious state-sponsored cyber activity," he said. Establishing a credible deterrent requires agreement on norms of cyber behavior by the international community, he said.75

5. **Collaboration between Hostile States and Non-State Actors.** Until fairly recently, the major threat actor posing a serious cyber security threat to the U.S. was the hostile or adversarial state. But that is rapidly changing as non-state actors are increasingly collaborating in a variety of ways with sponsoring states.76 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.”77

In addition to hactivists 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.78 (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 cyber crime, and cyber-enabled economic warfare, strategies.79 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.”80

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.81 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.82 To date, ISIS seems to have had little interest in developing and implementing plans for cyber-enabled economic warfare. But that may be changing. The *New York Times* 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. 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.

Thus, future research is needed to track which non-state actors are collaborating with which adversarial states on cyberattacks; what are the roles they play; how do they affect the states’ cyber-enabled economic warfare strategies; how do these roles and strategies evolve over time; etc. The cyber threat matrix is quickly getting more complicated, and new research is needed to understand what these trends signify for protecting vital U.S. interests at home and abroad.

ENDNOTES

3 Zarate, ibid, p. 3.
5 Dubowitz and Fixler, ibid, p. 2.
7 Hsieh, ibid, p. 74.
8 Hsieh, ibid, p. 89.
11 Near the end of the survey, respondents were asked to evaluate the definition by indicating the extent to which they agreed or disagreed with the statement, “The definition of cyber-enabled economic warfare used in for this survey is good.” 79% either said they agreed or strongly agreed; only 4% said they disagreed or strongly disagreed, and the remaining 17% said they were “undecided.”
12 For presentation purposes, the response category “Somewhat Serious” is omitted from this table. Also, a few respondents listed Pakistan, Yemen, and/or Mexico as posing a “moderately serious” threat.
13 We note that early this year, DNI Director James Clapper listed Russia as the number one cyber threat actor confronting the U.S., stating that “While I can’t go into detail here, the Russian cyber threat is more severe than we’ve previously assessed.” See James R. Clapper (2015) “Worldwide Threat Assessment of the U.S. Intelligence Community,” written testimony to the Senate Armed Services Committee (Washington, D.C.), Feb. 26. http://www.dni.gov/files/documents/Unclassified_2015_ATA_SFR - SASC_FINAL.pdf


James R. Clapper (2015) “Worldwide Threat Assessment of the U.S. Intelligence Community,” op cit. at #12. We expect that Clapper would now regard Chinese hackers’ repeated breaches and massive extractions of personal data from OPM, which only came fully to light this summer, as far more costly and serious.


For presentation purposes, the response category “Somewhat Serious” is omitted from this table.

24 Former 9/11 Commission Members (2014), op. cit. at #19.
25 For a “proof of concept” demonstration, see for example Hamas supported cyberattacks upon Israeli targets El Al (the national airline) and the Tel Aviv stock exchange, described in Paul Rosenzweig (2013) Cyber Warfare: How Conflicts in Cyberspace Are Challenging America and Changing the World (Denver: Praeger): p. 184.
26 Mark Dubowitz and Annie Fixler (2015), op. cit. at #4: p. 32.


For the details, see Dubowitz and Fixler (op. cit), pp. 33-37.


Panzar and Dave (2015), op. cit. at #9.


Schutzer (2015), op. cit. at #43.

Ibid.


James R. Clapper (2015) op. cit. at #12.


65 Ibid.


36
For example, see reporting on the U.S.’s Trojan horse sabotage of pipeline control software that the Soviets had previously stolen, 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.


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.

For example, here is a formal definition adopted by the U.S. government in conducting its own formal economic warfare planning more than sixty years ago on the cusp of the Cold War: “Economic warfare means: The use of economic, diplomatic, military or other measures to injure an enemy’s economic support of his war effort or a possible enemy’s economic potential. It includes such measures as shipping controls, naval interceptions, export controls, proclaimed listing, preclusive buying, financial precautions, war trade agreements, alien property control, foreign exchange control, and military attack on enemy economic targets” Joint Logistics Plan Committee, Mar. 6, 1950, available in the CIA Library, [http://www.foia.cia.gov/document/cia-rdp800r0173r000400140002-2](http://www.foia.cia.gov/document/cia-rdp800r0173r000400140002-2).


“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.”

77 Gross, op cit. at # 95.
78 McMurdo (2014), op cit. at #66.
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. P: 202.974.2400
Sixth Floor info@hudson.org
Washington, D.C. 20005 www.hudson.org