FOUNDATION FOR DEFENSE OF DEMOCRACIES

The Cyber Financial Wars on the Horizon:

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

Juan C. Zarate

Foreword by Stewart Baker

Center on Sanctions & Illicit Finance
FOUNDATION FOR DEFENSE OF DEMOCRACIES

July 2015

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

Juan C. Zarate

Foreword by Stewart Baker

July 2015

FDD PRESS

A division of the
FOUNDATION FOR DEFENSE OF DEMOCRACIES
Washington, DC

This report is included in the monograph, "Cyber-Enabled Economic Warfare: An Evolving Challenge," edited by Dr. Samantha Ravich and published by the Hudson Institute.

Table of Contents

Foreword

It's a pleasure to introduce Juan Zarate's thoughtful and innovative monograph on the convergence of financial and cyber warfare. The convergence of the two has elements of irony. The United States has long used financial sanctions to pressure other states. Now, other states are exercising power through cyberattacks on U.S. financial institutions. And U.S. efforts to protect banks through international "law of cyberwar" norms have only encouraged our adversaries to attack us where it seems to hurt most.

What should the United States do about this new threat? Judging from recent history, neither international norms nor stronger network defenses are a complete answer. We can't defend our way out of this mess any more than we can defeat street crime by requiring pedestrians to buy better body armor every year.

We need to do a better job of deterring attacks, first by identifying the attacker more reliably and then by moving from attribution to retribution. This is the core of Juan Zarate's insight, and the great value of his paper is how it combines a sophisticated appreciation of financial regulatory tools with an aggressive creativity in their use. He recognizes that government alone lacks the resources, the knowledge, and the incentives to track and identify those who are attacking financial institutions.

Much of that knowledge is in the hands of private forensics firms and network defenders. I agree with Juan Zarate that we should draw on the defenders' expertise and resources. Instead of threatening to prosecute defenders who follow attackers beyond the boundaries of their own networks, the U.S. government should encourage responsible private sector countermeasures. With characteristic panache, Juan calls this "cyber-privateering." While the free-for-all battle in cyberspace that the image conjures up is daunting, it's worth remembering that some of our most aggressive adversaries have already empowered what amount to their own privateers to attack our systems. With formerly socialist nations showing enthusiasm for privatized attack, it seems odd for the American government to insist that our companies should step back and leave the fight to their government. Especially when their government is losing that fight so ignominiously.

Organizing the retribution, in contrast, is likely to remain a task for government. And here too Juan's creativity and experience point to opportunities, especially in the financial sector. Very few nations want to encourage financial attacks that almost certainly cannot be contained inside one nation's borders. Those who attack financial institutions are the enemies of bankers everywhere. Just as the Financial Action Task Force set standards to combat money laundering and gradually ostracized the nations that violated those standards, it may be possible to exclude those who launch network attacks on the financial system from the benefits of that system. That's in the interest of every country that participates in the system. And if we hope to set "norms" in cyberspace, high-minded appeals to the law of armed conflict can't hold a candle to invoking the self-interest of bankers.

For anyone seeking practical but innovative solutions to one of the great international challenges of the twenty-first century, Juan Zarate's monograph offers an excellent place to start. Indeed, it may offer something even rarer in this field: Hope.

Stewart Baker
Steptoe & Johnson LLP
Former Assistant Secretary of Homeland Security for Policy
Former General Counsel, National Security Agency

Introduction

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

On Thursday, October 2, 2014, JPMorgan Chase & Co., the largest American bank by assets, announced that a cyberattack it had detected in mid-August 2014 had compromised the accounts of 76 million households and seven million small businesses. The JPMorgan attack—which began in June and is believed to have originated from Russia—went unnoticed for two months, despite the $250 million in cybersecurity that the bank expected to spend by year's end. Hackers had gained access to the bank's servers containing the names, email addresses, phone numbers, and addresses of both current and former customers. The same group of overseas hackers appears to have attempted to infiltrate at least twelve other financial institutions, including Fidelity Investments.[1]

JPMorgan maintains that the hackers were unable to gather detailed information that would be particularly damaging to consumers and that no fraudulent activity has been reported. Passwords, account numbers, social security numbers, dates of birth, and other information valuable to any cyber attacker looking for financial gain remain unperturbed. In a statement to its customers, the bank insisted that customer money was "safe."[2]

Some have rightly noted that if the attackers were good enough to compromise JPMorgan's network, they may have left themselves backdoors into its servers that remain undetected. Cybersecurity experts have opined that there is a possibility that "ghost" or undetected intrusions may still be of concern.[3] It remains unclear exactly how much information the hackers accessed, but the number of those affected makes the breach one of the largest ever. Indeed, the hackers may have also been sending a message to the bank, industry, and U.S. government about their capabilities with the extent and reach of their intrusion.

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

The U.S. government understood the potential significance of this attack and watched the forensics unfold over the summer—concerned this could be a new stealth attack from a state actor. When briefed by national security officials on the ongoing JPMorgan breach, President Obama reportedly asked his team whether this could be Putin's retaliation for Western sanctions. The U.S. government could not provide a definitive answer.[4] Joel Brenner, a former inspector general and senior counsel of the National Security Agency, wrote that Russia's likely use of proxies in the JPMorgan case "is what the gray space between war and peace looks like."[5]

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

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

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

The frequency and sophistication of attacks on banks are increasing, with each attack representing a more dangerous intrusion and demonstration of systemic vulnerabilities. CitiBank reports ten million cyberattacks on its system a month.[6] Banks are prime targets for sophisticated, organized cybercriminals. Banks not only hold money and customer accounts but also collect and centralize sensitive customer data and some clients' intellectual property.

More importantly, banks have been pulled into a more serious and sustained cyber financial battle. Nation states and their proxies realize that banks serve both as key systemic actors important for the functioning of the global economy and as chief protagonists in the isolation of rogue regimes and actors from the financial system. Thus, the financial community finds itself drawn into combined financial and cyber battles—neither of which it controls. This has led cybersecurity experts in the banking community to admit openly, "We are at war."[7]

In some cases, the threat may stem from within. In late November 2014, the security firm FireEye released a special report on a group it had dubbed "FIN4." Operating since at least mid-2013, FIN4 targeted individuals at over 100 companies with access to sensitive, not-yet-public information regarding merger and acquisition (M&A) deals and announcements with major ramifications for markets.[8] With native-English language skills and nuanced knowledge of corporate practices, the group used spear-phishing techniques to manipulate financial markets to its advantage using insider information. In a December 25, 2014 op-ed in *The Wall Street Journal*, Congressman Mike Rogers, then chairman of the House Intelligence Committee, warned that FIN4 was a harbinger of the kind of cyber and financial threat to come.[9]

Western banks and the financial system are now encountering the convergence between economic and cyber warfare. We have entered a new era of financial influence where financial and economic tools have taken pride of place as instruments of national security. The conflicts of this age are likely to be fought with markets, not just militaries, and in boardrooms, not just battlefields. Geopolitics is now a game best played with financial and commercial weapons.[10]

And those weapons now include cyber tools, used by non-state and state actors alike to attack banks and financial systems. The new geo-economic game may be more efficient and subtle than past geopolitical

competitions, but it is no less ruthless and destructive. Major and minor state powers, along with super-empowered individuals and networks, can harness economic interdependence and cyber weapons to increase their global power status at the expense of their geopolitical rivals. The danger emerging is the coalition of actors—perhaps states using non-state proxies in cyberspace—launching financial and cyber assaults.

So far, the United States has been at the cutting edge of this competition. But the fact that it was first to develop innovative and powerful financial and cyber tools to pursue its interests is no guarantee of continued success. Indeed, there is the potential for greater U.S. vulnerability and decreased financial and economic leverage. Although the United States has had a near monopoly on the use of targeted financial pressure over the past decade, this edge is likely to erode, leaving the United States both more vulnerable to external financial pressure and less able to use financial suasion as a lever of foreign policy.[11]

The need for urgent attention to this convergence within the financial community and among Washington policymakers is clear. Benjamin Lawsky, superintendent for New York's Department of Financial Services, the city's top banking regulator, said, "The cyber threat has to become urgent, one of the most important issues facing financial sector chief executives. It's got to be at the chief executive level. It is not an IT problem. It is a bank problem."[12] The failure of Washington lawmakers to innovate and enable relationships and cyber capabilities between the private sector and government—long understood to be essential to cybersecurity—has become even more problematic.

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

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

The Evolution of the Cyber Financial Threat

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

Perhaps the biggest source of U.S. vulnerability is not in terms of physical resources, but rather in virtual systems. As former Director of National Intelligence Mike McConnell noted before the Senate, "If we were in a cyberwar today, the United States would lose. This is not because we do not have talented people or cutting-edge technology; it is because we are simply the most dependent and the most vulnerable."[13] The Internet contributed an estimated 15 percent to the U.S. GDP between 2004 and 2009, and U.S. companies captured

35 percent of total Internet revenues earned by the top 250 Internet-related companies in the world.

In a 2013 speech, General Keith Alexander, the former head of the National Security Agency and Cyber Command, pointed to a seventeen-fold increase in attacks against U.S. infrastructure between 2009 and 2011, and graded U.S. preparedness to withstand a cyberattack against its critical network infrastructure as "around a 3" on a 10-point scale.[14]

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

Given the criminal opportunities that abound globally, it is no surprise that cyber intrusions and attacks are increasing at a devastating rate—with billions of dollars' worth of intellectual property and value stolen digitally every year. It is estimated that the cost of cybercrime to the global economy could be more than $500 billion annually.[15] Over the past few years, economic cyber intrusions and targeted searches and attacks have hit the International Monetary Fund, Lockheed Martin's information systems (via stolen SecurID data), Google's mainframes, Sony's Playstation data, Bank of America, and Citibank.

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

On August 3, 2011, the computer security firm McAfee issued a report revealing the largest "cyber-attack to date," which had targeted the data and systems of seventy-two organizations and companies around the world for over five years—enabled by an unidentified state actor presumed to be China. According to McAfee's former vice president of threat research, Dmitri Alperovitch, "What is happening to all this data is still largely an open question. However, if even a fraction of it is used to build better competing products or beat a competitor at a key negotiation (due to having stolen the other team's playbook), the loss represents a massive economic threat."

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

The Chinese government—likely in coordination with the People's Liberation Army—continues to pose a threat to U.S. industry. As recently as October 15, 2014, the FBI issued a private warning to American companies that "a group of highly skilled government hackers is in the midst of a long-running campaign to steal valuable data from U.S. companies and government agencies."[16] This latest announcement is just one in an ongoing series of cyberattacks against

U.S. industry; however, the source of the threat appears to have evolved since security firm Mandiant revealed in February 2013 that the People's Liberation Army Unit 61398 was stealing corporate and government secrets. The FBI warning said that the state-sponsored group was "exceedingly stealthy and agile by comparison with PLA unit 61398."[17]

The United States is not alone in experiencing attacks from China's Advanced Persistent Threat (APT1) malware. According to an October 13, 2014 blog post from technology security firm FireEye, China has also taken advantage of its new bilateral economic partnerships with Australia to threaten key sectors, including data theft from its mining and natural resource firms.[18] The group's patience and ability to identify four "zero-day" vulnerabilities in Microsoft's Windows operating system while maintaining a low profile point directly to a state-sponsored entity.

It should come as no surprise that the bulk of cyberattacks today come from China, Russia, Iran, and North Korea. As James A. Lewis, a cybersecurity expert at the Center for Strategic and International Studies, has written, "These countries are our military rivals. Cyberspace creates opportunities to exercise national power, and these nations have seized these opportunities."[19] Yet cyber warfare is not "war" in the Clausewitzian sense, although hacking is often conducted as "the continuation of politics by other means." Our opponents rely on the reliable functioning of international economic infrastructure, and therefore—to date—appear constrained not to conduct systemic or catastrophic attacks on the United States that might collapse international systems or prompt a massive retaliation.

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

On August 9, 2012, the Moscow-based security firm Kaspersky Lab announced that it had discovered a new "Gauss" virus (named after a file name in its codebase). Kaspersky Lab has historical connections to Russian intelligence and has made a practice of outing and analyzing computer viruses—often using crowdsourcing to help break codes. The Gauss virus had infected approximately 2,500 computers, the majority of which—1,660, to be exact, including 483 in Israel and 261 in the Palestinian territories—are tied to Lebanese banks, with the first attacks going back to at least September 2011. Once the infection took hold, Gauss was capable of capturing and transmitting detailed records of information, such as browser histories, cookies, profiles, and system configurations. Once the virus was discovered, its communications were shut down, but not disabled. Apparently, they are still lying dormant, awaiting activation by an unknown controlling source.

Gauss's complexity and sophistication have led Kaspersky's experts to conclude that the virus is a state-sponsored descendant of Stuxnet, coming from the same "factory." It is able to track flows of money and tap into infected computers. But it also carries an encrypted "payload" that targets specific systems, much like the Stuxnet virus. Perhaps most revealing is that Gauss shares critical coding and platform features with the Flame virus, another data-mining virus and Stuxnet

family member capable of extensive surveillance of infected computers that was discovered on Iranian computers in May 2012. But whereas Flame, which infected only seven hundred computers, cast a wide net toward all types of data, Gauss's focus is more attenuated, capturing primarily transaction data from a handful of specific Lebanese banks. Indeed, unlike typical non-state cyber-criminal malware, which tends to target a large number of small banks, Gauss targets a small number of large banks.

Gauss is so complex that Kaspersky has not been able to determine the function of its payload (what it has designated "resource 100"), though the firm suspects that it could trigger the destruction of critical infrastructure or some other high-profile target. For more details, Kaspersky crowd-sourced the solution on August 12, 2012, asking freelance hackers to crack the payload encryption and publishing the first 32 bytes of each encrypted section in Gauss to facilitate the process. By December 27, just a few months later and responding to Kaspersky's call, a well-known hacker posted open-source software he called "Gauss cracker," which represented a "major breakthrough" toward solving the encrypted Gauss payload.[20] Previously, Kaspersky successfully used crowd-sourcing to identify the programming language used in the state-sponsored DuQu malware, as well.[21]

In light of the target, the claim of state sponsorship makes sense. Lebanon is "something like the Switzerland of the modern Middle East," wrote Katherine Maher, a digital rights security expert, in *The Atlantic*. "More than 60 banks manage nearly $120 billion in private deposits in a country of 4.3 million people, and account for roughly 35 percent of the country's economic activity."[22] Lebanese banks have been among the most secretive in the world, and their opacity has long been a concern for United States and international financial regulators seeking to disrupt money launderers and terrorist financiers. The Lebanese banking system has come under direct fire as a financial way station for Iran, Syria, Hezbollah, and illicit financial flows.

With Stuxnet and Flame, the target was a rogue regime's nuclear program. With Gauss, the target seems to be the banks of an important financial center in the Middle East, where rogue elements leverage the banking facilities. Western states' interest in Lebanon's private sector has traditionally focused on "know your customer" and transaction data rules. Gauss now ups the ante with aggressive information collection and destructive payload delivery.[23]

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

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

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

transparency, and legal constraints may place it at a disadvantage on this type of cyber-battlefield.

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

The Iranian government has entered the fray in response to the financial assault on its economy and currency. In September 2012, a Middle Eastern hacker group identifying itself as Izz ad-Din al-Qassam Cyber Fighters conducted a massive denial-of-service attack against the electronic banking operations of JPMorgan Chase, Citigroup, PNC Bank, Wells Fargo, U.S. Bancorp, and Bank of America. By increasing fake demands on the banks' sites at a rate some ten to twenty times higher than average denial-of-service attacks, the new group was able temporarily to suspend access to checking accounts, mortgages, and other bank services.[24] Perhaps more troubling is that the mysterious group warned these financial institutions that an attack was imminent, but the banks proved unable to stop it.

Though Izz ad-Din al-Qassam is also the name of the military wing of Hamas, Senator Joseph Lieberman, then chairman of the Homeland Security Committee, argued that the attacks were connected to the Iranian Islamic Revolutionary Guard Corps–Qods Force.[25] Major banks, including non-U.S. banks, continue to be attacked by intense denial-of-service operations.

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

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

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

In what is described as a "race to zero," trading is moving faster and faster—and further away from the gaze and capacity of national regulators. According to trade negotiator Harald Malmgren and Mark Stys, it has gone "from trading in milliseconds (thousandths of a second) a couple of years ago to trading in microseconds (millionths of a second) now, and for cutting edge traders, pursuit in trading in picoseconds (trillionths of a second)."[26] High-frequency trading firms "represent approximately 2 percent of the 20,000 or so trading firms operating in the U.S. markets … [but] account for 73 percent of all U.S. equity trading volume," according to one trading technology consultant.[27]

During the "Flash Crash" episode of 2010, a trading algorithm dumped 75,000 futures contracts valued at $4.1 billion on the market in a twenty-minute period. The losses were staggering, causing a 600-point fall in the Dow and erasing $862 billion from the value of equities before an automatic circuit breaker paused trading.[28] Though the mass volume of such trading provides a buffer against manipulation, the sheer speed and anonymity of the cross-border trading across asset classes increase the risks and the potential for markets to be manipulated and cornered by savvy criminal and nefarious actors—for profit or other purposes.

According to the World Economic Forum's Global Risks 2015 report, cyberspace will be increasingly at the center of both our geopolitical and economic worlds, representing a new frontier that will pose unprecedented challenges. This new variable in the geopolitical equation, the report says, "will [make] it difficult for decision-makers to predict the development of such situations as sanctions and other instruments of economic coercion, thus raising the risk of unintended consequences."[29] As cyberattacks threaten the financial system with greater frequency, the threat to the financial order and traditional geopolitical relationships increases.

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

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

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

The Cyber Financial Battles Underway

Cybersecurity experts today identify four kinds of primary threat to the financial sector. First, sophisticated cyber actors—usually states—use espionage to steal intellectual capital and data from banks and destabilize them. Second, banks can be targeted for systemic disruption by a range of cyber actors who view them as symbols of Western capitalism or have reason to threaten the financial system. Third, "hacktivists" take advantage of vulnerabilities to break into banks' IT networks, usually in order to gain publicity for their cause. Finally, organized criminal organizations and cyber fraudsters have shifted from stealing money through traditional bank heists to using other means (online, telephone, card fraud) that are harder to detect.[30]

As recent attacks have made clear, no business, critical infrastructure, or private consumer—big or small, poorly- or well-protected—is completely immune to cyber threat. While the Syrian Electronic Army defaced prominent American media websites, a group of hackers known as "Dragonfly" inserted malware into the legitimate software of three industrial control systems manufacturers. 2013 saw a 91 percent increase in targeted attack campaigns. A co-authored report from the Center for Strategic and International Studies (CSIS), a prominent Washington think tank, and security firm McAfee, estimated the annual global cost of digital crime and intellectual property theft at $445 billion.[31] On nearly every front, the number, creativity, and effectiveness of attacks continue to go up.

There is evidence, however, that gaining notoriety in the cyber realm for its own sake is losing appeal. In

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

The most recent Office of the Comptroller of the Currency's Semi-Annual Risk Perspective shows alarming accelerated risk of cyberattacks in financial institutions. The problem is that criminals seeking information are getting better at accessing bank information as technology becomes cheaper and the barriers for entry to cybercrime drop.[32] Those historically rejected by the international financial system find themselves increasingly embraced by unscrupulous nation states willing to use their expertise to exploit weaknesses, and the line between state and non-state actors further blurs. Online markets for cyber hacking expertise allow for states and non-state actors to recruit front-line cyber proxies. Like never before, state-sponsored cyberattacks pose a threat to financial institutions.

The nexus between the financial sector and cybercrime is growing as never before. In July 2014, Bloomberg's *Businessweek* magazine reported that Russian hackers had "stolen the Nasdaq" back in October 2010.[33] An FBI internet traffic monitor had picked up signals indicating that malware had infiltrated the company's central servers. The event quickly prompted both the National Security Agency (NSA) and the National Cybersecurity and Communications Integration Center (NCCIC)—the latter one of the Department of Homeland Security's many information sharing and coordination centers—to get involved. Over a period of five months, an array of government agencies struggled to characterize and counter the state-sponsored cyberattack. For weeks, it remained unclear whether the attackers had compromised the trading platform, whether the breach was part of a larger attack, and which government agency was responsible for addressing which weakness.

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

State-sponsored attacks are not limited to a particular region or type. The Advanced Persistent Threat 1 (APT1) was described by Mandiant in a 2013 report as "one of the most prolific cyber-espionage groups in terms of the sheer quantity of information stolen" and stated that the group had stolen terabytes of data from at least 141 organizations in 20 major industries, estimating that it was an organization with at least dozens, potentially hundreds, of human operators."[34] In its report, Mandiant claimed that APT1 is Unit 61398 of the Chinese People's Liberation Army, though China's Ministry of Defense has previously stated that it is "unprofessional and groundless to accuse the Chinese military of launching cyberattacks without any conclusive evidence."[35] Still, in over 97 percent of the 1,905 times Mandiant observed APT1 intruders connecting to their attack infrastructure, APT1 used IP addresses registered in Shanghai and systems set to use the Simplified Chinese language.

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

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

On August 5, 2014, Hold Security reported that a Russian crime ring had amassed the largest known collection of stolen Internet credentials, including 1.2 billion user name and password combinations and more than 500 million email addresses.[36] The attack was not specifically targeted. The hackers targeted any website they could get, ranging from Fortune 500 companies to very small websites. On September 10, the passwords and email addresses for close to 5 million Gmail accounts were posted to a Russian Bitcoin forum in a text file. While forum administrators were quick to remove all passwords from the file, there is no doubt some accounts are now compromised.

Cyber Tools and Actors

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

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

Financial Trojans represent one of the newest and fastest-growing threats to banks. Financial institutions have dealt with targeted malware for more than a decade, evolving their security measures to stay one step ahead of fraudsters. Security firm Symantec reports that these security solutions—often customized—were ineffective in protecting banks from the threat they faced, as cybercriminals "motivated by financial reward" outpaced them.[37] In 2013 alone, attackers using financial Trojans targeted over 1,400 financial institutions and the top 15 most targeted financial institutions were targeted by over 50 percent of known Trojans. The number of unique financial Trojans has quadrupled since January 2013, and unfortunately, the adoption rate of strong countermeasures has been too slow.[38]

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

Reports of the death of spear-phishing—in which an attacker disguises himself as a friend or known entity and asks for sensitive financial information—were greatly exaggerated. Such campaigns increased a dramatic 91 percent in 2013.[39] Attacks now, however, use a "low and slow" approach, with both the total number of emails used per campaign and the number of those targeted decreasing. Ransomware scams—in which the attacker pretends to be local law enforcement, demanding a fake fine of between $100 and $500—escalated in 2013 and grew by 500 percent over the course of the year. These attacks are highly profitable and attackers

have adapted them to ensure they remain so. Related "Cryptolocker" scams are even more vicious. An attacker drops any pretense of being law enforcement and will spontaneously encrypt a user's files and request a ransom for the files to be unencrypted.[40]

While the prevalence of mobile malware is still comparatively low, 2013 showed that the environment for an explosive growth of scams and malware attacks is here. The Norton Report 2014, a global survey of end-users, showed that 38 percent of mobile users had already experienced mobile cybercrime.[41] Although lost or stolen devices remain the biggest risk, mobile users continue to engage in dangerous habits—such as storing sensitive files online and sharing account logins with family—that leave them open to attack.

Despite crackdowns by authorities, illicit or problematic online networks prove resilient. Last November, administrators from the shuttered Silk Road online black market, led by a new pseudonymous Dread Pirate Roberts (DPR), re-launched the site. Dubbed "Silk Road 2.0", it recreated the original site's setup and promised improved security. The new DPR took the precaution of distributing encrypted copies of the site's source code to allow the site to be quickly recreated in the event of another shutdown.[42] In mid-September 2014, online black market Silk Road 2.0 experienced a DDoS attack, which forced the site's administrators to temporarily shut down service. News of the attack broke on Bitcoin forums hours after it started. There is speculation that the attack was launched by law enforcement trying to locate the Silk Road 2.0 servers, while others believe criminals or competitors launched the attack.[43]

In early July 2014, security company Symantec revealed that the group of hackers known as "Dragonfly" had inserted malware into the legitimate software of three manufacturers of industrial control systems.[44] Focused largely in the U.S. and European energy sectors, Dragonfly's targeted cyber-espionage campaign gave the attackers the ability to sabotage major power supplies. The state-sponsored group—also known as "Energetic Bear" based somewhere in Eastern Europe—had been in operation since 2011, gaining long-term access to computers through spam email and watering hole attacks.[45] Dragonfly's ability to evolve in order to target new victims and remain unnoticed made it one of the most insidious groups ever to target American economic infrastructure.

In this environment, it has become increasingly difficult to distinguish state from non-state actors, as the former may use the latter as a proxy, quietly supporting the group while feigning innocence and denying involvement. Russia, in particular, has stepped up its cyber aggression when it perceives it is under attack from foreign entities. In its war with Georgia, the Russian state deployed cyberattacks as a complement to its military campaign. Following the relocation of a prominent Soviet-era statue in Estonia's capital of Tallinn in 2007, Russia bombarded Estonian organizations with DDoS attacks, marking one of the largest instances of state-sponsored cyber warfare to date.[46] In recent months, dozens of computers in the Ukrainian prime minister's office and at least ten of Ukraine's embassies abroad have been infiltrated by a cyber-espionage weapon linked to Russia.[47]

The Russian government does not always employ these cyber groups explicitly; however, they often maintain close ties to those in power and may benefit from a degree of funding. Scott Borg, chief executive of the U.S. Cyber Consequences Unit, an independent non-profit research institute said of Russian cybercriminals, "They are tolerated and even to some degree protected by the Russian government because they regularly engage in 'patriotic hacking.'"[48] Borg added, "They will often carry out cyber-attacks that allow them to profit, while still falling in line with what they perceive to be Russia's political interests."[49] Alliances of

convenience—between autocratic regimes and proxy groups around the world—may be the new modality in the cyber domain.

Private and Public Sector Response

Both the public and private sector have reacted to the growing threat from cyberattacks and intrusions—in large part by spending more on technical systems and expertise to defend against serious attacks. In recent years, spending on cybersecurity has exploded. Gartner, a research firm, estimates that in 2013 organizations around the globe spent $67 billion on information security. According to Allied Business Intelligence, Inc., cybersecurity spending by critical infrastructure industries alone was expected to hit $46 billion in 2013, up 10 percent from a year earlier.[50]

PwC's 2014 Global Economic Crime Survey found that 7 percent of U.S. organizations lost $1 million or more due to cybercrime incidents in 2013, compared with 3 percent of global organizations. 19 percent of U.S. entities reported financial losses of $50,000 to $1 million, compared with 8 percent of worldwide respondents.[51]

Many U.S. retailers believe the risk of legal liability and costly lawsuits will escalate. Today, claims by businesses that they are unaware of cybercrime risks and the need to invest in updated cybersecurity safeguards have become increasingly unconvincing. Tom Ridge, CEO of security firm Ridge Global and first Secretary of Homeland Security, said, "I think there will be a lot more litigation than we've seen in the past. These high-profile attacks have the attention of every board of directors."[52]

Cybersecurity analysts say that retailers are spending less on cybersecurity measures than banks and healthcare providers. Retailers spend 4 percent of their IT budgets on cybersecurity, while financial services and healthcare providers spend 5.5 percent and 5.6 percent, respectively. On cybersecurity spending per employee, the banking and finance industries spend roughly $2,500 per employee, while retailers invest about $400 per employee.[53] In early September 2014, Home Depot became the latest retailer to investigate a potential major breach of customer credit or debit card data. The stolen information from Home Depot will likely be put toward a massive new collection of stolen credit and debit cards that went on sale in early September in the cybercriminal underground.

Retailers spend far less than organizations of comparable size on cybersecurity, making themselves vulnerable to attack. Neiman Marcus Group, Sally Beauty Supply, Michaels, SuperValu, and Target Corp. were targeted earlier this year. Research director for cybersecurity at Gartner Inc. Lawrence Pingree, said, "Retailers have been the low-hanging fruit for attackers since they don't spend as much as banks and government entities in cybersecurity."[54] In 2005, Gartner also said that for every $5.62 businesses spend after a breach, they could spend $1 beforehand on encryption and network protection to prevent intrusions and minimize damage.[55] Today, the ratio remains about the same. Perhaps most worrying is that companies often lack basic procedural guidelines for what to do when they are hacked. According to a PwC survey, only 49 percent of the CEOs in the study have a plan for responding to insider cybersecurity threats, despite evidence that those events are typically more damaging than those from outside.[56]

Regardless of the amounts spent, it is cheaper to hack than to defend a hack. Richard Bejtlich, chief security strategist at FireEye Inc. and a former cyber investigator for the U.S. Air Force, said he could assemble a team that could hack offensively into nearly any target.[57] But $1 million would not be nearly enough for a company to defend itself.

Thanks to the growing recognition of this threat, however, there is a greater impetus for government and private companies to cooperate and share information. On October 13, 2014, Jamie Dimon, chief executive of JPMorgan, exhorted his counterparts on Wall Street to coordinate their cybersecurity efforts while also calling on the U.S. government to help more directly. He also pledged to double the bank's spending on digital security over the next four to five years.[58]

But collaboration between the public and private sector is not new. The Information Sharing and Analysis Centers (ISAC) fora have served as important venues for information sharing, and they have gained more momentum in the financial services and technology industries. The Financial Services Information Sharing and Analysis Center (or FS-ISAC) is the first widespread not-for-profit intelligence service designed to assist with cyber defense and analysis and has recently attracted extra funding from twelve large companies—including the financial, energy, transport, and healthcare sectors.[59]

The FS-ISAC has grown more operational over time. In June 2013, Microsoft teamed up with the FS-ISAC to disrupt the "Citadel" botnet, which cybercriminals deployed to infect thousands of computers to steal banking information and identities from unwitting victims. Microsoft, working with FBI, disrupted more than 1,000 botnets, but the malware resulted in losses of more than $500 million and affected more than 5 million people.[60] Most were located in the United States, Europe, Hong Kong, Singapore, India, and Australia, but Microsoft has found evidence of Citadel in more than ninety countries.[61] More recently, Microsoft assisted law enforcement in the United Kingdom to disrupt the "Caphaw" botnet, which targeted banks and their customers across Europe.[62]

On September 29, 2014, Microsoft and FS-ISAC expanded their operational relationship and signed a deal to share threat data when combating cybercrime, in a bid to help firms defend themselves against malware.[63] This will allow participating FS-ISAC members access to Microsoft's Cyber Threat Intelligence Program feed, giving them near real-time information on known malware infections affecting more than 67 million unique IP addresses.

FS-ISAC has recently teamed up with the Depository Trust and Clearing Corporation, which provides post-trade financial services, to launch a new software platform. Beginning with a pilot of 45 organizations, it will be used to share information about attacks and attempts at attack at a real-time speed intended to prevent hackers from deploying the same cyber weapons against several companies consecutively. The joint venture, known as Soltra, has seen its membership double since January as more institutions become aware of the threat.[64]

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

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

More broadly, the U.S. government has attempted to bring more focus, coordination, and information sharing on the issue of cybersecurity. President

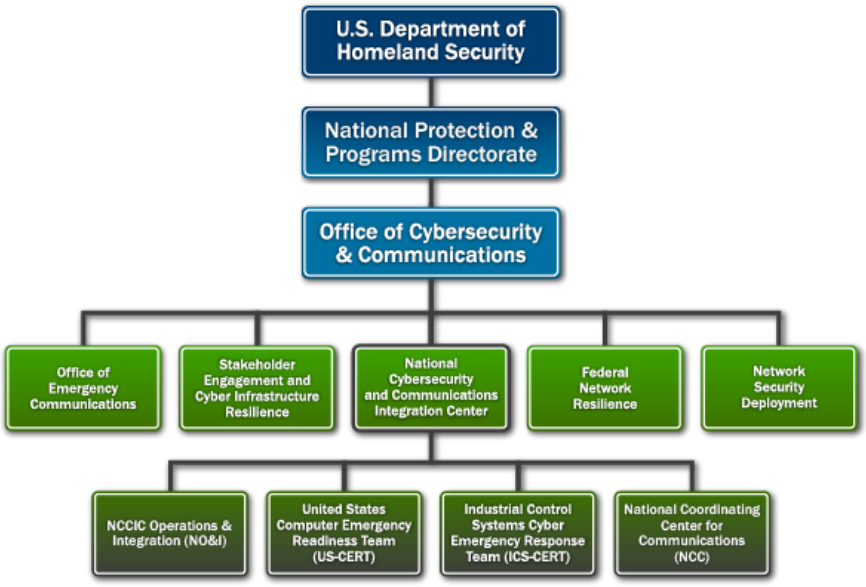
Obama has repeatedly labeled cybersecurity a priority national security issue. Executive Order 13636 signed in February 2013—"Improving Critical Infrastructure Cybersecurity"—gave rise to the National Institute of Standards and Technology's (NIST) Cybersecurity Framework, a compendium of best practices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

Cybersecurity legislation requiring heightened security protocols in the private sector and enabling better public-private information sharing has failed to pass in recent years, with cyber experts urging the Administration and Congress to pass new legislations. In his 2015 State of the Union address, President Obama urged Congress "to finally pass the legislation we need to better meet the evolving threat of cyberattacks."[65] This push, along with others from industry, has put cybersecurity information sharing at the forefront of congressional priorities.

The Obama Administration has also facilitated greater cooperation between the United States and the EU on cybersecurity issues. The new high-level U.S.-EU Cyber Dialogue announced at the 2014 U.S.-EU Summit will formalize and serve as the platform for closer U.S.-EU coordination on international cyberspace developments; the promotion and protection of human rights online; international security issues, such as norms of behavior in cyberspace, cybersecurity confidence building measures, and application of existing international law; and cybersecurity capacity building in third countries.

Within U.S. government, a range of departments, agencies, and shared initiatives is responsible for the nation's cybersecurity. The first line of defense is the U.S. intelligence community—including agencies within the NSA, FBI, and DHS—where monitoring

Exhibit 1



SOURCE: Department of Homeland Security.

systems and cyber analysts work to identify threats and disseminate information to the rest of government. At the Department of Homeland Security (DHS), the National Cybersecurity and Communications Integration Center (NCCIC) is a 24-7 cyber situational awareness, incident response, and management center that is a national nexus of cyber and communications integration for federal government, intelligence community, and law enforcement.

Within DHS, the U.S. Secret Service uses the Electronic Crimes Task Force (ECTF) to leverage the combined resources of local, state, and federal law enforcement with prosecutors, private industry, and academia to combat cyber-criminal activity. FBI's NCIJTF is its "next-generation cyber initiative" and serves as a coordination, integration, and information sharing center for nineteen U.S. agencies and cyber threat investigations. FBI's Key Partnership Engagement Unit (KPEU) manages a targeted outreach program focused on building relationships with senior executives of key private sector corporations.

There has been no lack of effort by the U.S. government to try to increase information sharing with the private sector. Indeed, the private sector—including the financial industry—often feels bombarded by different agencies of government attempting to gain access to information or serve as the principal interlocutor for the government. They also feel exposed without legislation to protect their activities.

The private sector has tried to do its part in preparing the next generation to better understand the challenges of cybersecurity. At a Wilson Center event on October 16, officials from the University of Maryland, the Department of Homeland Security, and Northrop Grumman discussed cooperative efforts to build "tomorrow's workforce" of cyber-savvy leaders. With funding from Northrop Grumman, the University of Maryland's Honors College founded the Advanced Cybersecurity Experience for Students (ACES), the first four-year undergraduate program in cybersecurity that seeks to address the current shortage of cyber-enabled graduates.[66]

Attempts to bridge the public-private sector divide are not limited to the United States. On October 5, 2012, the United Kingdom established The Centre for Global Cyber-Security Capacity Building, which hoped "to draw on the expertise generated by eight research universities, is designed to improve international co-ordination, increase access to expertise, and promote good governance online."[67] It will act as a forum for collaboration between leaders from across the world, including from think tanks and the private sector.

The British Bankers Association (BBA) is another institution working toward better sharing of cyber information between public and private entities. The BBA plans to launch the Financial Crimes Alert Service (FCAS), designed to allow banks and other financial groups to react faster to major incidents and to learn of the latest techniques used by fraudsters, cybercriminals, and terrorists.[68] BBA says it is working with BAE Systems to get the service up and running by early 2015.

The association's Chief Executive Anthony Browne called the FCAS "a powerful new weapon against fraudsters, cybercriminals and other crooks intent on stealing our clients' money," calling it "a shining example of how banks and government can work together to benefit all customers."[69] This will add onto the framework that already exists within the U.K. called the National Fraud Intelligence Bureau, which has prevented more than $163 million of fraud losses through information sharing. The new system will pool intelligence from twelve government and law enforcement agencies and share it with the teams working inside banks to combat fraud, cybercrime, terror financing, money laundering, and bribery.[70]

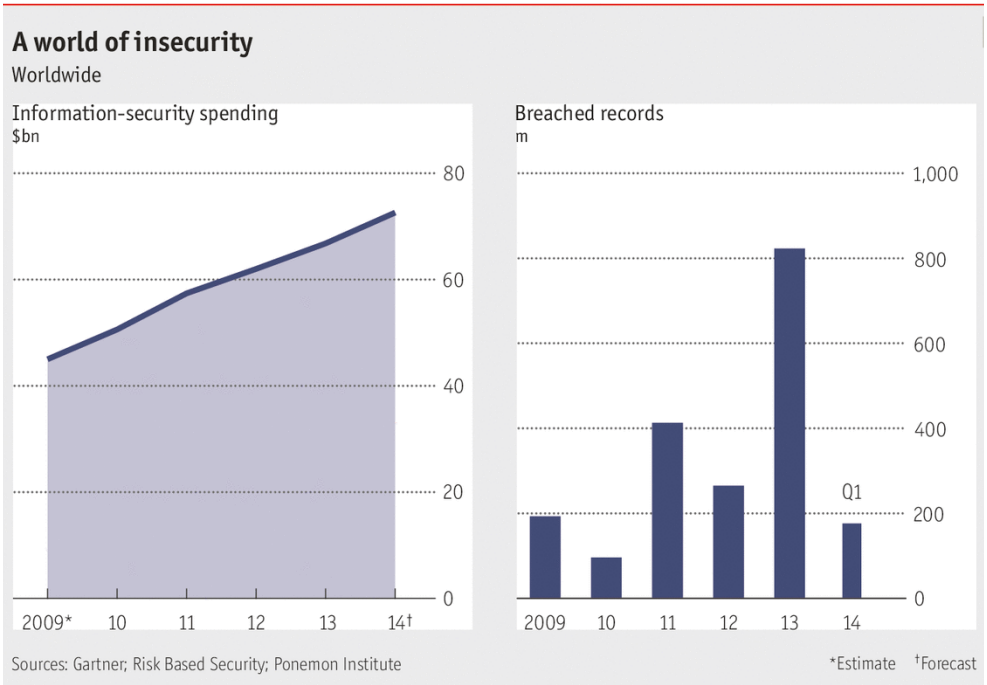
These are important attempts to foster more information sharing and real-time attempts to understand and counter breaches to key private sector data sets and systems. All of these models, however, maintain a strict divide between public and private sector actors—often with liability and risk attached to those private sector entities willing to share information or divulge openly their vulnerabilities.

The approach applied by governments to date also tends to be reactive and case-specific, with little capability to appreciate or communicate the systemic risks to key systems and infrastructure from sophisticated or even state actors. Under the current system, there is little incentive for pro-active defense of financial systems and legal restrictions on more aggressive monitoring and disruption in cyberspace by systemically relevant and important private sector entities.

Instead of fostering a culture of cooperation, the current model creates frustration as financial institutions feel more vulnerable and less able to defend their systems. They also feel less supported by the government. Indeed, in a recent speech by Ellen Richey, Visa's vice chairman for risk and public policy, she concluded, "The primary thing the government can do is number one, get out of the way. Eliminate the barriers that exist legally to sharing information, stop punishing the victim and assuming that every company that is breached is some sort of criminal and deserving of multiple investigations and lawsuits."[71]

But in light of recent attacks, federal regulation organizations have come down hard on banks, urging them to more actively share their cyber threat information. Five of the United States' banking regulators—most prominently the Federal Financial Institutions Examination Council (FFIEC)—are threatening the industry with increased oversight if

Exhibit 2



SOURCE: *The Economist*

more stringent measures to protect consumer financial data are not implemented. An FFIEC report published alongside the announcement reinforced the need for engagement beyond the board of directors and senior management. The report emphasized the benefit of routinely discussing cybersecurity issues in meetings and identifying inherent vulnerabilities.[72]

In some cases, companies are considering more self-help options to defend their systems from identified hackers, like "hacking back" or "active defense" to defend against identified cyberattacks. This remains illegal under U.S. law; however, more financial executives and experts have begun discussing this option more openly in recent months. Technology research firm Gartner Inc. projects that countermeasures on the part of the cybersecurity industry will surpass $78 billion in 2015. House Homeland Security Committee Chairman Michael McCaul has said that "some victim companies may already be conducting offensive operations without permission from government and are 'very frustrated.'"[73] Regardless, a new, more pro-active model should be considered as the financial industry finds itself in the eye of the cyber storm and as the financial system appears more and more at risk from sophisticated attackers.

A New Cyber-Privateering Framework

A new economic and cybersecurity approach requires a new paradigm of U.S. public-private engagement and collaboration. This involves an evolution from classic, state-based national security actions toward deeper involvement of the private sector in arenas previously confined to the halls of government, with a commensurate and widening appreciation within governments of the power of markets and the private sector to influence international security. In arenas such as financial sanctions and anti-money laundering and counter-terrorist financing programs, the United States has already moved in this direction, relying on the private sector and the ability of financial institutions to act as gatekeepers to the financial system by identifying, reporting, and preventing the use of financial facilities by transnational actors and criminals of concern.

The utility of this approach is that it is not based on private sector altruism or civic duty, but on the self-interest of legitimate financial institutions that want to minimize the risk of facilitating illicit transactions that could bring high regulatory and reputational costs if uncovered. In other economic arenas, this symbiosis takes hold only with great effort, particularly given the private sector aversion to increased regulatory burdens and associated costs. This means that governments need to check their regulatory practices and work closely to build consistent requirements and regimes across borders to help international financial institutions operate effectively and efficiently. The challenge of cooperation will be exacerbated as governments continue to unveil new regulatory structures and requirements in the wake of the 2008 financial crisis.

Innovation in public-private coordination is already occurring by necessity in the cyber domain, with approximately 80 percent of cyber-infrastructure in private sector hands. After the attacks on Google servers by Chinese hackers, Google and the National Security Agency began to work together in 2010 to help Google defend against future attacks.[74] In the wake of the massive attacks on U.S. banks in 2012 and continuing into 2013, the National Security Agency began a pilot project with the banks to try to track and prevent cyberattacks.[75] Other pilot projects—driven by the private sector and governments—are unfolding to help accelerate information sharing and defenses against significant cyberattacks. This kind of collaboration opens the door for more creative and widespread public-private cooperation to tackle cyber threats and

serves as a testing ground for such collaboration on broader issues of national economic security.

Indeed, the broader paradigm of leveraging financial suasion in national security involves empowering and catalyzing key private sector actors to protect the integrity of the financial system by making market and risk-based decisions. This paradigm can be the basis of this new framework to address financial cyberattacks.

In the first instance, financial and cyber intelligence need to be enhanced and driven toward the creation of useful, actionable information. Many banks are now establishing units—including internal financial intelligence units—to analyze internal data and understand and manage financial crime and sanctions compliance risk. These systems complement the cyber and technical defenses being built in all major financial institutions. Banks can build on these financial and analytic systems to better understand potential cyber intrusions and the transactions flowing through their systems.

More importantly, the private sector must be allowed to share more information with each other and government to detect and prevent cyberattacks. Secretary of the Treasury Jack Lew made the case for clearer rules of the road to allow for information sharing and protection of rights:

> As it stands, our laws do not do enough to foster information sharing and defend the public from digital threats. We need legislation with clear rules to encourage collaboration and provide important liability protection. It must be safe for companies to collaborate responsibly, without providing immunity for reckless, negligent or harmful behavior. And we need legislation that protects individual privacy and civil liberties, which are so essential to making the United States a free and open society.[76]

The current financial information sharing regime, which requires financial institutions to monitor transactions and customer behavior and submit suspicious activity and other reports (to include information sharing about cyberattacks) to the U.S. Treasury, also provides for greater information sharing within the financial community. Section 314(b) of the USA PATRIOT Act allows financial institutions to share information about suspect financial activity within their sector, without liability. This provision should be matched in the cyber intrusion and attack context, and there should be legal safe harbors for information sharing between and from private sector actors intended to inform or assist in cyber defense.

In addition to new forms of real-time and legally protected information sharing, there need to be new tools applied that accelerate the U.S. government's targeting of state actors, networks, and individuals that attempt to breach U.S. private sector systems—especially financial systems. U.S. law enforcement has consistently investigated cases of breaches, including of organized crimes rings and hackers that successfully penetrate U.S.-based systems, with indictments often following.

The most significant indictment was made public on May 19, 2014, when the U.S. government charged five Chinese People's Liberation Army officials with cyber espionage. Though the individuals may never see the inside of a U.S. federal courthouse, the indictment was significant in laying out the specifics of official Chinese cyber espionage and gave weight to the broad U.S. government accusations that the Chinese government lies behind massive cyber infiltration of the U.S. private sector for commercial advantage. These types of cases need to be pursued and networks of cybercriminals—of whatever type—exposed. Such cases, in combination with the aggressive enforcement of financial criminal statutes against those that are directing and financially benefitting from cyber

intrusions and espionage, can begin to create accountability and perhaps even a form of deterrence against those actors that want to appear legitimate.

The president should also deploy aggressively his emergency economic powers and a broader strategy for the use of multiple tools to address the reality of major cyber espionage, crime, and infiltration affecting the U.S. financial and commercial system.

On April 1, 2015, the president took an important step by signing Executive Order (EO) 13694, based on his power under the International Emergency Economic Powers Act (IEEPA), that allows the Secretary of the Treasury, in coordination with the Secretary of State and the Attorney General, to identify and isolate from the U.S. financial system those who are engaged in "significant malicious cyber-enabled activities" outside the United States. This EO allows for the blocking of assets and property of those engaged in activities "that are reasonably likely to result in, or have materially contributed to, a significant threat to the national security, foreign policy, or economic health or financial stability of the United States" and are intended, among other things, to affect or disrupt substantially critical infrastructure and systems or to cause misappropriation of financial information, trade secrets, and economic resources. This includes the targeting of those responsible for the receipt or use of any such misappropriated resources for commercial or competitive advantage.

With this new Executive Order, the U.S. government has created a cyber financial battlespace for potential targets that it can now identify and financially isolate—to include the full spectrum of actors that may be involved in significant cyber intrusions. Though hackers and those responsible for cyber intrusions are the most obvious targets of this EO, the deepest potential impact will be on the behavior of state actors like China, state-owned enterprises seeking access to American markets and Western commercial legitimacy, and corporations that may seek to leverage stolen intellectual property for commercial advantage. All those actors, including everything they own and control, and any entity or person that may support financially or benefit intentionally from such cyber activities, may be targeted and put at risk under this EO, with the potential that significant economic players will be isolated from the U.S. financial and economic system.

The U.S. government can now use the tools of economic and financial isolation—including freezing assets and blocking transactions—against those companies, entities, networks, and individuals identified as being behind major cyber infiltrations, disruptions, and espionage. As with Executive Order 13224, which formed the cornerstone of the counter-terrorist financing campaign after 9/11, EO 13694 has the potential to drive a new strategy and innovations that leverage the convergence of cyber and financial warfare.

In addition, as with the provisions of Section 311 of the USA PATRIOT Act regarding "primary money laundering concerns," Congress could amplify the effects of this new EO and craft legislation to empower the Secretary of the Treasury to identify jurisdictions, institutions, or networks that are sponsoring or willfully allowing their territory or systems to be used to attack American financial institutions. The label of "primary cybersecurity concern" could be applied to any such actor and could bring with it a range of consequences and potential countermeasures against a jurisdiction's economy, including measures to sanction or bar from any business in the United States those companies or entities are found to be benefiting or profiting from cyber espionage.

Congress could further empower the private sector—creating a 21st century cyber-privateering regime that rewards, enables, and empowers the private sector to help defend itself in concert with government. This

would require rule-setting, more active collaboration, and explicit line drawing and processes, but such a regime is imaginable. This model could be based on the tradition of congressional issuance of "letters of marque and reprisal," as provided for explicitly in Article 1, Section 8 of the U.S. Constitution. Governments provided these letters to private merchant ships, granting them the authority and monetary incentive to attack and capture enemy vessels and bring the cases before admiralty courts. In the age of piracy and maritime insecurity, this was a legitimate method of providing maritime security in the early days of the Republic.

This type of approach was proposed in part by Professor Jeremy Rabkin of the George Mason School of Law and his son, Ariel Rabkin in the *Chicago Journal of International Law* in Summer 2013. The Rabkins argue that approaching cyber conflict in the context of armed conflict is misguided; rather, they write, "Cyber conflict should be open—as naval war has been—to hostile measures short of war, to attacks on enemy commerce, to contributions from private auxiliaries."[77] Adopting this model would also force the U.S. government to resolve lingering questions of authority and responsibility within the government for assisting or acting in concert with the private sector.

This "privateering" model could take different forms. In June 2014, Irving Lachow and Evan Wolff proposed a future scenario in which a cadre of "cyber cops" could take action against hackers on behalf of private individuals and small business—those who would lack the resources to address cybercrime on their own.[78] This could include a reward program for those groups able to uncover, identify, and even "deliver" cyber hackers to U.S. courts or authorities—as security groups have done in the past. Eric Rosenbach, the Assistant Secretary of Defense for Homeland Defense and Global Security, mentioned at an October 2, 2014 event at the Center for Strategic and International Studies that the capabilities of government to track and identify organizations and individuals responsible for cyberattacks against the United States have never been greater. Rosenbach claimed that the capability for "attribution"—the technical wherewithal to accurately name and shame those who threaten us—is a key component of our cyber deterrence strategy.[79]

The capability to track and identify cyber hackers exists in the private sector, as demonstrated by Mandiant's ability to identify the specific PLA office behind certain cyberattacks against Western companies and the Information Warfare Monitor's ability to track Chinese-based infiltration of dozens of computers systems throughout the world, including the Dalai Lama's computers in India.[80] The "attribution revolution" in the private sector—with better cyber forensic technology to identify the source of cyberattacks—opens up the possibility of more aggressive tracking, detection, and targeting.

Groups pursuing these techniques already exist. Companies like CrowdStrike—staffed by former FBI cyber officials including Shawn Henry and Steve Chabinsky—provide services to help governments and companies protect themselves through attribution and active defense. By identifying zero-day vulnerabilities and quickly locating the origin of threats, CrowdStrike and other companies like it accomplish two tasks at once, both decapitating the existing threat and creating an environment that may deter others from joining in the first place. On October 28, 2014, *Bloomberg* reported that a coalition of several technology companies—led by Novetta and including Microsoft, Cisco, Symantec, and FireEye—had joined in disrupting a hacking campaign originating with Chinese intelligence.[81] Dubbed by those involved as a "first-of-its-kind effort," the efficacy of the private sector effort demonstrated its reach and the potential for future coordination on cyber threats within its own ranks and with government.

New legal actions and authorities, that unleash the

power of cyber forensic teams and private litigants and plaintiff's lawyers against those attacking U.S. systems, should be considered as well. *Qui tam* actions that allow private litigants to benefit from the identification of prosecutions should be designed to reward those building cases against cyber hackers and state-sponsors. This would incentivize further those able to attribute attacks and would deputize the private sector and lawyers to investigate significant cases.

Victims of attacks should be given the right to sue the perpetrators and those benefitting directly from any cyber infiltrations, just as victims of terrorism are provided the right to sue terrorists, state-sponsors, and terrorist financiers and facilitators. Thus, shareholders and companies could be given the right to sue those who have perpetrated, sponsored, or benefited directly and knowingly from cyberattacks. This would have the benefit of unleashing the power of the plaintiff's bar—focusing less attention on those attacked by the breaches and instead on those sponsoring or benefiting from the attacks.

Greater attribution and awareness of attacks could also lead to foreign litigation, World Trade Organization-related suits, and other forms of trade, intellectual property, and fraud causes of action in foreign and international courts. All of this would be in furtherance of allowing companies and those affected by cyberattacks the ability to use the court system and judgments to defend themselves.

Moreover, the U.S. Department of Justice, Department of Homeland Security, and Treasury Department could create and issue special cyber warrants—another type of "letter of marque and reprisal"—to allow U.S. private sector actors to track and even "hack back" or disrupt cyberattacks in certain instances to defend their systems. This would require a real-time capability to respond to targets of opportunity and evaluation of the negative externalities of any such action—especially those that affected friendly states or systems. The issuance of the warrants by the government would allow for legal, diplomatic, and systemic considerations before any preemptive or counter-attacks were approved.

The government today is in a position to enable the private sector—and even private individuals—to pursue economic warfare on its behalf vis-à-vis a new model of cyber-privateering. Individuals would be given the resources necessary to bring suits against those who threaten their assets abroad and domestically. The burden of financial integrity would move from top-down federal control to a democratized, flattened system to match the more distributed and amorphous cyber threat environment.

The U.S. government has been growing more comfortable enabling hackers working with private industry—known as "cyber-privateers"—to identify weaknesses in existing cybersecurity and build it back stronger. According to an October 2014 article from the *Financial Times*, banks say that regulators—such as the Bank of England and the Federal Reserve—have been pushing them to identify threats and testing their cyber resilience with a program of "ethical hacking" with events like "Def Con," known as "the Olympics of Hacking," where computer hackers gather annually to compete, share their knowledge, and meet like-minded hackers.[82] The Securities Industry and Financial Markets Association (SIFMA) has been trying to foster better collaboration between the government and industry for some time, organizing simulated cyberattacks dubbed "Quantum Dawn" that involve authorities, regulators, and banks.[83] Harnessing the dynamism of the private sector for purposes of cyber information sharing could provide just the lift stagnant Washington lawmakers need.

The idea of coopting hackers and enlisting them has taken hold in the private sector. Seventeen-year-old George Hotz became the world's first hacker to crack

AT&T's lock on the iPhone in 2007, the company ignored him while it scrambled to fix the bugs his work exposed. He later reverse-engineered Sony Playstation 3, and Sony summarily sued him and settled only after he agreed never to hack a Sony product again. Last year, Hotz dismantled the defenses of Google Chrome's operating system. By contrast, the company paid him a $150,000 reward for helping fix the flaws he had uncovered. Two months later, Chris Evans, a Google security engineer, followed up via email with Hotz, making him an offer to join Google's elite team of full-time hackers paid to hunt security vulnerabilities in software across the Internet.[84]

Indeed, the U.S. government and other governments around the world have grown more comfortable with enlisting the private sector in the security space—enlisting hundreds of thousands of private contractors to provide a range of defense- and security-related services over the past two decades. Former NSA General Counsel Stewart Baker—an advocate for limited "hacking back"—believes that government officials today are far likelier to enable companies burdened by cyberattacks than they are to prosecute them for considering actively defending themselves against adversaries.[85] Cyber experts are considering implementing a warning mechanism called a "beacon" that could be attached to stolen data, allowing sleuths to determine the origins of an attack.[86] In the cybersecurity context, there should be consideration for a new framework that allows for private actors to take on more of their own defense, within bounds and with clears lines of authority and responsibility.

This approach would need to be matched by new international arrangements and alliances that set standards of international conduct, principles of state control and responsibility, and allow for closer coordination to address problems of attack attribution and response coordination. The U.S. government has attempted to spur international cooperation in the cyber domain and discussions of limits on the use of cyber weapons, including reported briefings to Chinese government officials regarding U.S. capabilities and willingness to restrain U.S. cyber activities. But these efforts have not been reciprocated and the international system remains bereft of broader international standards and processes—especially in the cyber financial context.

International efforts could build on Estonia's Cyber-Defense League, intended to build multilateral and private sector capabilities to detect and react to cyberattacks. This could be replicated more broadly in a new NATO mission, especially given concerns over repeated use of cyber tools and attacks by Russian actors. Bilateral and multilateral working groups or investigations—combining key private sector actors and cyber forensic experts—could coordinate responses to sophisticated infiltrations and attacks—assuming the idea of broader cooperation and coordination among trusted actors *ab initio*. This could include a role for Interpol, perhaps creating a new "silver notice" for international attention and action against cybercriminals and sponsors.

Even the United States and China could try to collaborate on specific investigations of attacks that affect both the U.S. and Chinese financial systems. By starting with a particular investigation affecting both countries, the United States could test whether the Chinese could be enlisted to address systemic concerns about attacks on the international financial system, upon which the Chinese rely as much as the United States.

More broadly, a new collection of relevant state and private actors could be assembled to help establish international cyber norms—in particular to address questions of attribution and response. This could allow for the establishment of norms around the use of cyber warrants by the private sector and development of laws and strictures to address cyber hacking, espionage, and

crimes without squelching innovation.
This could take directly from the model of the Financial Action Task Force (FATF), which is the international body comprised of thirty-six jurisdictions that set international standards on anti-money laundering and countering the financing of terrorism and proliferation financing. The FATF, along with regional-style FATF bodies, elaborate these standards and practices and, along with the IMF and World Bank, assess countries on their implementation and effectiveness. The FATF also provides a forum to address new issues—like the emergence of digital currencies—and to engage the private sector directly.

Underlying the international development of norms, there needs to be recognition that the Internet and the cyber domain require careful tending. The cyber domain can be and is misused by nefarious actors, and the trust and legitimacy of this world can be quickly undermined and broken if the attacks increase in severity and disrupt key national systems.

In addition, this new framework might allow for doctrinal innovation in the cyber field—to include exploring new forms of a cyber deterrence strategy that take lessons from financial warfare deterrence models. In the context of a cyber arms race, there may be ultimately no way to match the cyber intrusive efforts of multiple, sophisticated actors—especially when collaborating or enabled by state-sponsors. Although the "attribution revolution" has afforded cyber sleuths—from government and the private sector—unprecedented abilities to pin responsibility on aggressors, fearing no retaliation, these actors are unlikely to change their behavior.

By using proxies for plausible deniability, nation states are increasingly emboldened to go after symbols of economic prosperity. North Korea's attack on Sony Pictures Entertainment on November 24, 2014 is a demonstration that a cyber event need not disrupt key national security systems to prove strategically relevant and induce an official government response from the U.S. But lack of clarity in what sort of "retaliation" the U.S. has planned for a country already under the burden of economic sanctions and with little technological infrastructure to speak of, may do little to deter state or non-state actors from launching similar attacks.

Perhaps in widening the scope of those actors that may be targeted with economic sanctions, legal censure, international opprobrium, or even cyber retaliation or attacks, there may begin to emerge a new form of deterrence affecting not just the hackers, but the entire spectrum of those actors willing to support, finance, or benefit from cyberattacks. This may also begin to force "responsible" state actors to curb their cyber hacking activity to avoid damaging attacks on their own systems and unwanted scrutiny in a variety of fora and from a range of non-state or private actors. A doctrine of cyber deterrence may emerge in the context of the cyber-privateering model delineated above.

Unlike in the financial context, where the U.S. Treasury and government worry about the "magnificent glass house" of the international financial system, there is little coordination and consideration of the systemic risks to the global cyber and digital domains. Other active actors in the domain—including the Chinese, Russian, and Iranian governments—have demonstrated little concern at this stage for managing the health or sustainability of either the financial or cyber systems. Yet, these actors do rely on these systems for their economic well-being and are more and more entangled in the global, commercial, and cyber systems that allow their economies and countries to function. As these actors begin to predominate in cyberspace and perhaps sponsor or direct attacks against key international financial actors, there needs to be a broader policy and international debate about how the key states and private sector actors protect the integrity of both the financial and cyber systems. Indeed, there may

be new models of both deterrence and international cooperation that emerge among the responsible state actors that rely most heavily on the uninterrupted functioning of the cyber and financial systems.

A new model of collective and local cyber defense may be necessary to address the increasing threats and risks, especially to the financial community. Banks now sit at the heart of the cyber storm—targeted by all actors in cyberspace. They are looking for more support from government and more freedom to collaborate within their sector. Given the current legal and policy constructs, these measures are likely to be reactive and represent marginal improvements to the current system.

Absent a more revolutionary approach to public-private collaboration and cyber defense, the financial community will remain at risk. The banks will spend hundreds of millions to harden and defend key systems, while sophisticated actors, including nation states, will up the ante in the cyber arms race. In so doing, the underpinnings of the financial system will remain at risk. Now is the time to address the convergence of cyber and financial warfare before a systemic breakdown and disaster occur. In so doing, we may innovate a new and more enduring model for ensuring global cybersecurity.

Endnotes

1. Kara Scannell & Tom Braithwaite, "Fidelity Hack Points to JPMorgan Link," *Financial Times*, October 9, 2014. (http://www.ft.com/intl/cms/s/0/2564f64e-4f2e-11e4-9c88-00144feab7de.html#axzz3GJX0s0Ma)

2. Emily Glazer & Danny Yadron, "J.P. Morgan Says About 76 Million Households Affected By Cyber Breach," *The Wall Street Journal*, October 3, 2014. (http://online.wsj.com/articles/j-p-morgan-says-about-76-million-households-affected-by-cyber-breach-1412283372)

3. In a *Financial Times* interviews, Frank Abagnale—inspiration for *Catch Me If You Can* and anti-fraud specialist—is dubious that the hackers would not have taken additional data. "The Benefits of Being a Real Fraudster," *Financial Times*, October 9, 2014. (http://www.ft.com/intl/cms/s/2/1e7ad07c-4ae4-11e4-839a-00144feab7de.html#axzz3GJX0s0Ma)

4. "Obama Had Security Fears on JPMorgan Data Breach," *DealBook*, accessed October 16, 2014. (http://dealbook.nytimes.com/2014/10/08/cyberattack-on-jpmorgan-raises-alarms-at-white-house-and-on-wall-street/)

5. Joel Brenner, "Nations Everywhere Are Exploiting the Lack of Cybersecurity," *The Washington Post*, October 24, 2014. (http://www.washingtonpost.com/opinions/joel-brenner-nations-everywhere-are-exploiting-the-lack-of-cybersecurity/2014/10/24/1e6e4b70-5b85-11e4-b812-38518ae74c67_story.html)

6. "Finextra: MasterCard Unveils Tool to Tackle Cyber Threat," *Finextra*, October 2, 2014. (http://ww.finextra.com/news/fullstory.aspx?newsitemid=26532&topic=sibos)

7. Charles Blauner, Global Head of Information Security for Citi Bank and the Chair of the Financial Services Sector Coordinating Council, "The Cyber Wars Escalate," *SIBOS Conference*, September 30, 2014.

8. Barry Vengerik et al., "Hacking the Street? FIN4 Likely Playing the Market," *FireEye*, 2014. (https://www2.fireeye.com/fin4.html)

9. Mike Rogers, "Stopping the Next Cyberassault," *The Wall Street Journal*, December 25, 2014. (http://www.wsj.com/articles/mike-rogers-stopping-the-next-cyberassault-1419543945)

10. Juan Zarate, *Treasury's War: The Unleashing of a New Era of Financial Warfare* (PublicAffairs, 2013).

11. Ibid.

12. Kara Scannell, "NY Bank Regulator Targets Cyber Threat," *Financial Times*, October 6, 2014. (http://www.ft.com/intl/cms/s/0/5a981338-4cdf-11e4-a0d7-00144feab7de.html#axzz3GJX0s0Ma)

13. Trudy Rubin, "It's Time to Get Serious about Cyber Attack Risk," *Sydney Morning Herald*, December 29, 2010. (http://www.smh.com.au/federal-politics/political-opinion/its-time-to-get-serious-about-cyber-attack-risk-20101228-1998p.html)

14. David E. Sanger & Eric Schmitt, "Cyberattacks Are Up, National Security Chief Says," *The New York Times*, July 26, 2012. (http://www.nytimes.com/2012/07/27/us/cyberattacks-are-up-national-security-chief-says.html)

15. "Net Losses: Esatimating the Global Cost of Cybercrime," *Center for Strategic and International Studies* June 2014. (http://csis.org/event/2014-mcafee-report-global-cost-cybercrime)

16. Ellen Nakashima & Ashkan Soltani, "FBI Warns Industry of Chinese Cyber Campaign," *The Washington Post*, October 15, 2014. (http://www.washingtonpost.com/world/national-security/fbi-warns-industry-of-chinese-cyber-campaign/2014/10/15/0349a00a-54b0-11e4-ba4b-f6333e2c0453_story.html)

17. Ibid.

18. "Double-Edged Sword: Australia Economic Partnerships Under Attack from China," *FireEye Blog*, October 13, 2014. (http://www.fireeye.com/blog/technical/2014/10/double-edged-sword-australia.html)

19. James Andrew Lewis, "The Key to Keeping Cyberspace Safe? An International Accord," *The Washington Post*, October 7, 2014. (http://www.washingtonpost.com/postlive/key-to-keeping-cyberspace-safe-international-accord/2014/10/07/ae50a35e-4812-11e4-b72e-d60a9229cc10_story.html)

20. "Hashcat's GPU-Accelerated Gauss Encryption Cracker—," *Securelist*, December 28, 2012. (https://securelist.com/blog/events/34884/hashcats-gpu-accelerated-gauss-encryption-cracker-4/)

21. Kim Zetter, "Researchers Seek Help Cracking Gauss Mystery Payload," *WIRED*, August 14, 2012. (http://www.wired.com/2012/08/gauss-mystery-payload/)

22. Katherine Maher, "Did the Bounds of Cyber War Just Expand to Banks and Neutral States?" *The Atlantic*, August 17, 2012. (http://www.theatlantic.com/international/archive/2012/08/did-the-bounds-of-cyber-war-just-expand-to-banks-and-neutral-states/261230/)

23. David Nordell, "Is the New 'Gauss' Malware a Counter-terror Finance Intelligence Tool?" *The Terror Finance Blog*, August 12 2012. (http://www.terrorfinanceblog.com/2012/08/is-the-new-gauss-malware-a-counter-terror-finance-intelligence-tool.html)

24. "Deconstructing the Al-Qassam Cyber Fighters Assault on US Banks," *Recorded Future*, January 2, 2013. (https://www.recordedfuture.com/deconstructing-the-al-qassam-cyber-fighters-assault-on-us-banks)

25. E. Scott Reckard, "Banks Fail to Repel Cyber Threat," *Los Angeles Times*, September 27, 2012. (http://articles.latimes.com/2012/sep/27/business/la-fi-bank-attacks-20120927)

26. Harald Malmgren and Mark Stys, *Computerized Global Trading 24/6: a Roller Coaster Ride Ahead?: An Article from: The International Economy*, n.d.

27. Rob Lati, "The Real Story of Trading Software Espionage," *Wall Street & Technology*, July 10, 2009. (http://www.wallstreetandtech.com/trading-technology/the-real-story-of-trading-software-espio/218401501)

28. U.S. Commodity Futures Trading Commission & U.S. Securities & Exchange Commission, "Findings Regarding the Market Events of May 6, 2010," September 30, 2010, page 13. (http://www.cftc.gov/ucm/groups/public/@otherif/documents/ifdocs/staff-findings050610.pdf)

29. "2.2 Global Risks Arising from the Accelerated Interplay Between Geopolitics and Economics," *World Economic Forum*, accessed January 30, 2015. (http://reports.weforum.org/global-risks-2015/part-2-risks-in-focus/2-2-global-risks-arising-from-the-accelerated-interplay-between-geopolitics-and-economics/)

30. Martin Arnold, "Banks Face Rising Threat from Cyber Crime," *Financial Times*, October 6, 2014. (http://www.ft.com/intl/cms/s/0/5fd20f60-4d67-11e4-8f75-00144feab7de.html#axzz3FOFcGxgh)

31. "Net Losses: Esatimating the Global Cost of Cybercrime," *Center for Strategic and International Studies* June 2014. (http://csis.org/event/2014-mcafee-report-global-cost-cybercrime)

32. New York State Department of Financial Services, Press Release, "Governor Cuomo Announces New Cyber Security Assessments For Banks," May 6, 2014. (http://www.dfs.ny.gov/about/press2014/pr1405061.htm)

33. Michael Riley, "How Russian Hackers Stole the Nasdaq," *BusinessWeek*, July 17, 2014. (http://www.businessweek.com/articles/2014-07-17/how-russian-hackers-stole-the-nasdaq)

34. "Mandiant," *Mandiant*, accessed October 28, 2014. (http://www.mandiant.com)

35. "US and China Accuse Each Other of Cyber Warfare," *RT*, February 19, 2013. (http://rt.com/usa/cyber-china-war-unit-604)

36. Nicole Perlroth & David Gelles, "Russian Hackers Amass Over a Billion Internet Passwords," *The New York Times*, August 5, 2014. (http://www.nytimes.com/2014/08/06/technology/russian-gang-said-to-amass-more-than-a-billion-stolen-internet-credentials.html)

37. Candid Wueest, "The State of Financial Trojans in 2013," *Security Response Blog*, December 17, 2013. (http://www.symantec.com/connect/blogs/state-financial-trojans-2013)

38. Ibid.

39. "2015 Internet Security Threat Report," *Symantec*, accessed October 20, 2014. (http://www.symantec.com/security_response/publications/threatreport.jsp)

40. Ibid.

41. "2013 Norton Report,"Symantec, accessed October 20, 2014. (http://www.symantec.com/about/news/resources/press_kits/detail.jsp?pkid=norton-report-2013)

42. Nermin Hajdarbegovic, "Silk Road 2.0 Hit by 'Sophisticated' DDoS Attack," *CoinDesk*, September 15, 2014. (http://www.coindesk.com/silk-road-2-0-shrugs-sophisticated-ddos-attack/)

43. Ibid.

44. "FBI Investigating Russian Cyber Attacks on US Banks," *The American Interest,* August 28, 2014. (http://www.the-american-interest.com/blog/2014/08/28/fbi-investigating-russian-cyber-attacks-on-us-banks/)

45. Candid Wueest, "The State of Financial Trojans in 2013," *Security Response Blog*, December 17, 2013. (http://www.symantec.com/connect/blogs/state-financial-trojans-2013)

46. Christian Lowe, "Kremlin Loyalist Says Launched Estonia Cyber-attack," *Reuters*, March 12, 2009. (http://www.reuters.com/article/2009/03/12/us-russia-estonia-cyberspace-idUSTRE52B4D820090312)

47. Sam Jones, "Ukraine PM's Office Hit by Cyber Attack Linked to Russia," *Financial Times*, August 7, 2014. (http://www.ft.com/intl/cms/s/0/2352681e-1e55-11e4-9513-00144feabdc0.html#axzz3DtMfpRac)

48. "FBI Investigating Russian Cyber Attacks on US Banks," *The American Interest,* August 28, 2014. (http://www.the-american-interest.com/blog/2014/08/28/fbi-investigating-russian-cyber-attacks-on-us-banks/)

49. Ibid.

50. "Defending the Digital Frontier," *The Economist*, July 12, 2014. (http://www.economist.com/news/special-report/21606416-companies-markets-and-countries-are-increasingly-under-attack-cyber-criminals)

51. "Global Economic Crime 2014 Survey," *PwC Website*, accessed October 20, 2014. (http://www.pwc.com/gx/en/economic-crime-survey/index.jhtml)

52. Ibid.

53. "Retailers Spend Less on Cybersecurity Than Other Industries, and It Shows," *Homeland Security News Wire*, September 5, 2014. (http://www.homelandsecuritynewswire.com/dr20140905-retailers-spend-less-on-cybersecurity-than-other-industries-and-it-shows)

54. "Retail Spends Less on Cybersecurity Than Banking, Healthcare," *The Wall Street Journal CIO Journal*, September 2, 2014. (http://mobile.blogs.wsj.com/cio/2014/09/02/retail-spends-less-on-cybersecurity-than-banking-healthcare/)

55. Danny Yadron, "Companies Wrestle With the Cost of Cybersecurity," *The Wall Street Journal*, February 26, 2014. (http://online.wsj.com/articles/SB10001424052702304834704579403421539734550)

56. "Global Economic Crime 2014 Survey," *PwC Website*, accessed October 20, 2014. (http://www.pwc.com/gx/en/economic-crime-survey/index.jhtml)

57. Danny Yadron, "Companies Wrestle With the Cost of Cybersecurity," *The Wall Street Journal*, February 26, 2014. (http://online.wsj.com/articles/SB10001424052702304834704579403421539734550)

58. Robert Hackett, "JPMorgan's Dimon: There Will Be Wins, Losses in Battle Against Cyber Threats," October 17, 2014. (http://fortune.com/2014/10/17/jpmorgan-jamie-dimon-data-breach/)

59. Hannah Kuchler, "US Financial Industry Launches Platform to Thwart Cyber Attacks," *Financial Times*, September 24, 2014. (http://www.ft.com/intl/cms/s/0/080092b2-437a-11e4-8a43-00144feabdc0.html?siteedition=intl#axzz3FOFcGxgh)

60. Joseph Demarest, "Taking Down Botnets," *Testimony before the Senate Judiciary Committee, Subcommittee on Crime and Terrorism,* July 15, 2014. (http://www.fbi.gov/news/testimony/taking-down-botnets)

61. Chloe Albanesius, "Microsoft, FBI Take Down 'Citadel' Botnet Targeting Bank Info," *PCMAG*, June 6, 2013. (http://www.pcmag.com/article2/0%2c2817%2c2420046%2c00.asp)

62. Richard Domingues Boscovich, "Microsoft Partners with Financial Services Industry on Fight Against Cybercrime," *Microsoft on the Issues*, September 29, 2014. (http://blogs.microsoft.com/on-the-issues/2014/09/29/microsoft-partners-financial-services-industry-fight-cybercrime/)

63. Hannah Kuchler, "US Financial Industry Launches Platform to Thwart Cyber Attacks," *Financial Times*, September 24, 2014. (http://www.ft.com/intl/cms/s/0/080092b2-437a-11e4-8a43-00144feabdc0.html?siteedition=intl#axzz3FOFcGxgh)

64. The Depository Trust & Clearing Corporation, Press Release, "FS-ISAC and DTCC Announce Soltra, a Strategic Partnership to Improve Cyber Security Capabilities and Resilience of Critical Infrastructure Organizations Worldwide," September 24, 2014. (http://www.dtcc.com/news/2014/september/24/fs-isac-and-dtcc-announce-soltra.aspx)

65. Lily Hay Newman, "In State of the Union, Obama Promotes Cybersecurity Measures 'Especially' to Protect Kids," *Slate,* January 20, 2015. (http://www.slate.com/blogs/future_tense/2015/01/20/in_state_of_the_union_obama_promotes_cybersecurity_measures_especially_to.html)

66. Noted in: "Tomorrow's Workforce: How Can America Remain Competitive?" *Event at The Wilson Center,* October 16, 2014. (http://www.wilsoncenter.org/event/tomorrow%E2%80%99s-workforce-how-can-america-remain-competitive)

67. "About," *The Global Cyber Security Capacity Centre at The Oxford Martin School Website*, accessed October 28, 2014.

(http://www.oxfordmartin.ox.ac.uk/research/programmes/cybersecurity/)

68. British Bankers' Association, Press Release, "Banks Team up with Government to Combat Cyber Criminals and Fraudsters," September 23, 2014. (https://www.bba.org.uk/news/press-releases/banks-team-up-with-government-to-combat-cyber-criminals-and-fraudsters/#.VE-nx_nF8uc)

69. Martin Arnold, "Banks Launch Fresh Drive Against Cyber Crime," *Financial Times*, September 23, 2014. (http://www.ft.com/intl/cms/s/0/15630060-433f-11e4-be3f-00144feabdc0.html#axzz3EF608RSt)

70. Ibid.

71. Dakin Campbell & Michael J. Moore, "Cyber Attacks Require Coordinated Defense, Executives Say," *Bloomberg*, October 11, 2014. (http://www.bloomberg.com/news/articles/2014-10-11/cyber-attacks-require-coordinated-defense-executives-say)

72. Cory Bennett, "Regulators Urge Banks to Share Cyber Threat Info," *The Hill*, November 3, 2014. (http://thehill.com/policy/cybersecurity/222730-regulators-urge-banks-to-share-cyber-threat-info)

73. Jordan Robertson, "It's the Government's Job to Respond to Cyber Attacks: Bloomberg Poll," *Bloomberg*, January 21, 2015. (http://www.bloomberg.com/news/articles/2015-01-21/cyber-attack-retaliation-seen-as-government-s-job-in-global-poll)

74. Shane Harris, "Google's Secret NSA Alliance: The Terrifying Deals Between Silicon Valley and the Security State," *Salon.com*, November 16, 2014. (http://www.salon.com/2014/11/16/googles_secret_nsa_alliance_the_terrifying_deals_between_silicon_valley_and_the_security_state/)

75. Ellen Nakashima, "Banks Seek NSA Help Amid Attacks on Their Computer Systems," *The Washington Post*, January 11, 2013. (http://www.washingtonpost.com/world/national-security/banks-seek-nsa-help-amid-attacks-on-their-computer-systems/2013/01/10/4aebc1e2-5b31-11e2-beee-6e38f5215402_story.html)

76. "Wall Street Confronts Cyber Threats," *Markets Media*, July 24, 2014. (http://marketsmedia.com/wall-street-faces-cyber-threats/)

77. Jeremy Rabkin & Ariel Rabkin, Navigating Conflicts in Cyberspace: Legal Lessons from the History of War at Sea, *Chicago Journal of International Law, 14*(1), September 15, 2014, pages 197-258. (Accessed via http://papers.ssrn.com)

78. Thomas E. Ricks, "When Your Computer Gets Hacked, Why Can't You Call the Police to Deal with It?" *Foreign Policy*, June 26, 2014. (http://ricks.foreignpolicy.com/posts/2014/06/26/when_your_computer_gets_hacked_why_cant_you_call_the_police_to_deal_with_it)

79. Noted in: "Cyber Leaders: A Discussion with the Honorable Eric Rosenbach," *Event at The Center for Strategic and International Studies*," October 2, 2014. (http://csis.org/event/cyber-leaders)

80. Tania Branigan, "Cyber-Spies Based in China Target Indian Government and Dalai Lama," *The Guardian* (U.K.), April 6, 2010. (http://www.theguardian.com/technology/2010/apr/06/cyber-spies-china-target-india)

81. Chris Strohm & Michael Riley, "China-Linked Hacking Foiled by Private-Sector Sleuthing," *Bloomberg*, October 28, 2014. (http://www.bloomberg.com/news/2014-10-28/china-linked-hacking-foiled-by-private-sector-sleuthing.html)

82. Hannah Kuchler, "Def Con: The 'Olympics of Hacking'," *Financial Times*, August 15, 2014. (http://www.ft.com/intl/cms/s/2/e7243fec-22e2-11e4-9dc4-00144feabdc0.html#axzz3FOFcGxgh)

83. "Cybersecurity Exercise: Quantum Dawn 2," *SIFMA Website*, accessed October 28, 2014. (http://www.sifma.org/services/bcp/cybersecurity-exercise--quantum-dawn-2/)

84. "Famous iPhone Jailbreaker Geohot Is Now Working At Google As A Project Zero Hacker," *Redmond Pie*, July 18, 2014. (http://www.redmondpie.com/famous-iphone-jailbreaker-geohot-is-now-working-at-google-as-a-project-zero-hacker/)

85. Craig Timberg, Ellen Nakashima and Danielle Douglas-Gabriel, "Cyberattacks Trigger Talk of 'Hacking Back'," *The Washington Post*, October 9, 2014. (http://www.washingtonpost.com/business/technology/cyberattacks-trigger-talk-of-hacking-back/2014/10/09/6f0b7a24-4f02-11e4-8c24-487e92bc997b_story.html)

86. Ibid.

Acknowledgments

This report was derived from Chapter 16 of my book *Treasury's War: The Unleashing of a New Era of Financial Warfare* (PublicAffairs, 2013) and is included in "Cyber-Enabled Economic Warfare: An Evolving Challenge," edited by Dr. Samantha Ravich and published by the Hudson Institute. I am grateful to Samantha for including me in her study and for her vision in leading a project on the future challenges and opportunities associated with cyber-enabled economic warfare.

I would like to thank Daniel Paltiel, from the Center for Strategic and International Studies (CSIS), who provided invaluable research and insights and without whom this piece could not have been written. I would also like to thank Denise Zheng and Jim Lewis from CSIS for their scholarship and review of this article. I am grateful to Stewart Baker for offering his guidance and support—and for crafting the Foreword to this piece—and to Mark Dubowitz, Annie Fixler, Chip Poncy, and my colleagues at FDD's Center on Sanctions and Illicit Finance for their encouragement and constant support.

About The Author

Juan C. Zarate serves as Chairman and Senior Counselor of the Center on Sanctions and Illicit Finance (CSIF) at the Foundation for Defense of Democracies. Mr. Zarate is the Chairman and Co-Founder of the Financial Integrity Network, the Senior National Security Analyst for CBS News, a Visiting Lecturer of Law at the Harvard Law School, and a Senior Adviser at the Center for Strategic and International Studies (CSIS).

Mr. Zarate served as the Deputy Assistant to the President and Deputy National Security Advisor for Combating Terrorism from 2005 to 2009, and was responsible for developing and implementing the U.S. Government's counterterrorism strategy and policies related to transnational security threats. Mr. Zarate was the first ever Assistant Secretary of the Treasury for Terrorist Financing and Financial Crimes where he led domestic and international efforts to attack terrorist financing, the innovative use of Treasury's national security-related powers, and the global hunt for Saddam Hussein's assets. Mr. Zarate is a former federal prosecutor who served on terrorism prosecution teams prior to 9/11, including the investigation of the USS Cole attack.

Mr. Zarate sits on several boards, including for the Director of the National Counterterrorism Center (NCTC), HSBC's Financial System Vulnerabilities Committee, the Coinbase Board of Advisors, and the Vatican's Financial Information Authority (AIF).

He is the author of *Treasury's War: The Unleashing of a New Era of Financial Warfare* (2013), *Forging Democracy* (1994), and a variety of articles in *The New York Times*, *Washington Post*, *Wall Street Journal*, *LA Times*, *the Washington Quarterly* and other publications.

Mr. Zarate has his own weekly national security program on CBSNews.com called "Flash Points."

About the Foundation for Defense of Democracies (FDD)

The Foundation for Defense of Democracies is a non-profit, non-partisan policy institute dedicated exclusively to promoting pluralism, defending democratic values, and fighting the ideologies that drive terrorism. Founded shortly after the attacks of 9/11, FDD combines policy research, democracy and counterterrorism education, strategic communications, and investigative journalism in support of its mission.

FDD focuses its efforts where opinions are formed and decisions are made, providing cutting-edge research, investigative journalism and public education - transforming ideas into action and policy.

FDD holds events throughout the year, including the Leading Thinkers series, briefings on Capitol Hill, expert roundtables for public officials, diplomats and military officers, book releases, and panel discussions and debates within the policy community.

About FDD's Center on Sanctions and Illicit Finance (CSIF)

The Foundation for Defense of Democracies' Center on Sanctions and Illicit Finance (CSIF) expands upon FDD's success as a leading think tank on the use of financial and economic measures in national security. The Center's purpose is to provide policy and subject matter expertise in areas of illicit finance, financial power, and economic pressure to the global policy community.

CSIF seeks to illuminate the critical intersection between the full range of illicit finance activities and national security, including money laundering, terrorist financing, sanctions evasion, proliferation financing, cyber crime and economic espionage, and corruption and kleptocracy. This includes understanding how America can best use and preserve its financial and economic power to promote its interests and the integrity of the financial system. The Center also examines how America's adversaries may be leveraging economic tools and power.

CSIF focuses on global illicit finance, including the financing of terrorism, weapons and nuclear proliferation, corruption, and environmental crime. It has a particular emphasis on Iran, Saudi Arabia, Kuwait, Qatar, Turkey, Russia, and other autocratic states as well as drug cartels and terrorist groups including Hamas, Hezbollah, al-Qaeda, and the Islamic State.

For more information, please visit www.defenddemocracy.org.

FDD
FOUNDATION FOR
DEFENSE OF DEMOCRACIES

P.O. Box 33249
Washington, DC 20033-3249
(202) 207-0190
www.defenddemocracy.org