JUNE 16, 2015

GLOBAL PERSPECTIVE ON CYBER THREATS

UNITED STATES HOUSE OF REPRESENTATIVES, COMMITTEE ON APPROPRIATIONS

ONE HUNDRED AND FOURTEENTH CONGRESS, FIRST SESSION

HEARING CONTENTS:

WITNESSES:

Frank J. Cilluffo ***[view pdf]***
Associate Vice President – George Washington University
Director – Center for Cyber and Homeland Security
Co-Director – Cyber Center for National and Economic Security

Michael Madon ***[view pdf]***
Board of Advisors Member
Center on Sanctions and Illicit Finance, Foundation for Defense of Democracies
Vice-President, Business Development – RedOwl Analytics

Richard Bejtlich ***[view pdf]***
Chief Security Strategist
FireEye, Inc.

AVAILABLE WEBCAST(S):*

Duration [01:45:23] ***[view video]*** via YouTube

COMPILED FROM:

http://financialservices.house.gov/calendar/eventsingle.aspx?EventID=399216

** Please note: Any external links included in this compilation were functional at its creation but are not maintained thereafter.*

Center for Cyber
& Homeland Security

THE GEORGE WASHINGTON UNIVERSITY

"A Global Perspective on Cyber Threats"

Testimony of Frank J. Cilluffo
Director, Center for Cyber and Homeland Security

Before the U.S. House of Representatives, Committee on Financial Services, Subcommittee on Oversight and Investigations

Tuesday June 16, 2015

GW Center for Cyber and Homeland Security
2000 Pennsylvania Avenue, NW, Suite 2210 • Washington, DC 20052
Tel: 202-994-2437 • E-Mail: cchs@gwu.edu
http://cchs.gwu.edu

Introduction

Thank you, Chairman Duffy, Ranking Member Green, and distinguished Subcommittee Members for this opportunity to testify before you today. The United States currently faces an almost dizzying array of cyber threats from many and varied actors. Virtually every day there is a new incident in the headlines and the initiative clearly remains with the attacker.

The U.S. financial services sector in particular is in the crosshairs as a primary target. To give you a sense of the magnitude of the problem, consider the following figures which were provided to me recently by a major U.S. bank on a not-for-attribution basis: just last week, they faced 30,000 cyber- attacks. This amounts to an attack every 34 seconds, each and every day. And these are just the attacks that the bank actually knows about, by virtue of a known malicious signature or IP address. As for the source of the known attacks, approximately 22,000 came from criminal organizations; and 400 from nation-states.

This pace is magnified by the speed at which technologies continue to evolve and by the fact that our adversaries continue to adapt their tactics, techniques and procedures in order to evade and defeat our prevention and response measures. Against this background, a strong detection and mitigation program is just as necessary as a strong defense. While it is important to continue to invest in technologies and procedures to prevent attacks, the reality is that nobody can prevent all attacks; but significant steps can be taken to minimize the impact and consequences of an attack. The financial services sector understands this well and should therefore serve as a model for other sectors which are simply not as far along on the learning curve. Indeed, up until recently, even the financial sector invested overwhelmingly (85%) in prevention .

While Wall Street has made significant strides and is investing heavily in shoring up their cybersecurity, Main Street—meaning small and medium sized businesses, including the regional banks—lags far behind. This issue will

become increasingly salient as the threat continues to migrate along the spectrum, shifting its focus from harder targets like big business to encompass medium-sized and smaller enterprises.

At the national level, the challenge is to understand as best we can the threat as it manifests in so many different incarnations; and to prioritize it so that our limited resources for preventing and containing the challenge are directed as efficiently and effectively as possible.

Taking a global perspective on cyber threats, the bottom line up front is as follows:

- The threat spectrum includes a wide array of actors with different intentions, motivations, and capabilities.

- Nation-states and their proxies continue to present the greatest—meaning most advanced and persistent— threat in the cyber domain.

- Foreign terrorist organizations certainly possess the motivation and intent but fortunately, they have yet to fully develop a sustained cyber-attack capability. Recent "doxing" tactics against US military and law enforcement personnel by the Islamic State in Iraq and Syria (ISIS) is troubling and indicative of an emerging threat. It is likely that ISIS, or their sympathizers, will increasingly turn to disruptive cyber attacks.

- By contrast, criminal organizations possess substantial capabilities, but their motivation and intent differs from terrorists. Rather than being motivated by ideology or political concerns, criminal organizations are driven by the profit motive. However criminals are increasingly working with or for nation-states such as Russia; and this convergence of forces heightens the dangers posed by both groups.

GW Center for Cyber and Homeland Security
2000 Pennsylvania Avenue, NW, Suite 2210 • Washington, DC 20052
Tel: 202-994-2437 • E-Mail: cchs@gwu.edu
http://cchs.gwu.edu

- Yet other entities such as "hacktivists" may also possess considerable skills and abilities; and when their special interests or core concerns are perceived to be in play, these individuals can be a significant disruptive force whether acting alone or loosely in tandem, essentially as a leaderless movement. Their motive is often to cause maximum embarrassment to their targets and to bring attention to their cause.

- In reference to any threat vector, a worst-case scenario would combine kinetic and cyber-attacks; and the cyber component would serve as a force multiplier to increase the lethality or impact of the physical attack.

- Finally, banking and financial services are primary targets for cyber-attacks and cybercrimes. Directed against this truly critical infrastructure, cyber-attacks or a concerted campaign against U.S. banks, exchanges, clearinghouses, and markets—hold the potential to undermine trust and confidence in the system itself, irrespective of the perpetrator.

Below the various categories of actors are examined in greater detail in terms of the nature of the threat they pose and how they function.

Nation-States

The most advanced and persistent cyber threats to the United States today remain nation-states and their proxies, and in particular China and Russia. In addition, Iran has increased its cyber capabilities exponentially in recent years. And with the hack of Sony Corporation—which made use of more than half a dozen exploits lest the target be patched against one or more of these vulnerabilities, North Korea too has demonstrated itself to be a significant adversary.

How do these actors function?

Our adversaries have engaged in brazen activity, from computer network exploitation (CNE) to computer network attack (CNA). CNE includes

GW Center for Cyber and Homeland Security
2000 Pennsylvania Avenue, NW, Suite 2210 • Washington, DC 20052
Tel: 202-994-2437 • E-Mail: cchs@gwu.edu
http://cchs.gwu.edu

traditional, economic, and industrial espionage, as well as intelligence preparation of the battlefield (IPB)—such as surveillance and reconnaissance of attack targets, and the mapping of critical infrastructures for potential future targeting in a strategic campaign. In turn, CNA encompasses activities that alter (disrupt, destroy, etc.) the targeted data/information. The line between CNE and CNA is thin, however: if one can exploit, one can also attack if the intent exists to do so.

Foreign militaries are, increasingly, integrating CNE and CNA capabilities into their warfighting and military planning and doctrine. These efforts may allow our adversaries to enhance their own weapon systems and platforms, as well as stymie those of others. Moreover, CNAs may occur simultaneously with other forms of attack (kinetic, insider threats, etc.).

Our adversaries are also interweaving the cyber domain into the activities of their foreign intelligence services, to include intelligence derived from human sources (HUMINT).

This said our adversaries are certainly not all of a piece. Rather, nation-states may differ from one another, or from their proxies, in their motivation and intent. Tradecraft and its application may also differ widely. From a U.S. perspective, the challenge is to parse our understanding of key actors and their particular behaviors, factoring details about each threat vector into a tailored U.S. response that is designed to dissuade, deter, and compel.[1]

China

China possesses sophisticated cyber capabilities and has demonstrated a striking level of perseverance, evidenced by the sheer number of attacks and acts of espionage that the country commits. Reports of the Office of the U.S. National Counterintelligence Executive have called out China and its cyber

[1] http://blogs.wsj.com/cio/2015/04/28/cyber-deterrence-is-a-strategic-imperative/

GW Center for Cyber and Homeland Security
2000 Pennsylvania Avenue, NW, Suite 2210 • Washington, DC 20052
Tel: 202-994-2437 • E-Mail: cchs@gwu.edu
http://cchs.gwu.edu

espionage, characterizing these activities as rising to the level of strategic threat to the U.S. national interest.[2]

The U.S.-China Economic and Security Review Commission notes further: "Computer network operations have become fundamental to the PLA's strategic campaign goals for seizing information dominance early in a military operation."[3]

China's aggressive collection efforts appear to be intended to amass data and secrets (military, commercial / proprietary, etc.) that will support and further the country's economic growth, scientific and technological capacities, military power, etc.—all with an eye to securing strategic advantage in relation to (perceived or actual) competitor countries and adversaries.

Just this month, data theft on a massive scale, affecting virtually all U.S. government employees, was traced back to China. Whether the hack was state-sponsored, state-supported, or simply tolerated through a blind eye by the government of China, is not yet clear. But military officers in China are increasingly known to moonlight as hackers for hire when off the clock; and countries are increasingly turning to proxies do their bidding in order to provide plausible deniability.[4]

Russia

Russia's cyber capabilities are, arguably, even more sophisticated than those of China. The Office of the U.S. National Counterintelligence Executive (NCIX) observes: "Moscow's highly capable intelligence services are using HUMINT, cyber, and other operations to collect economic information and technology to support Russia's economic development and security. Russia's extensive

[2]http://www.ncix.gov/publications/reports/fecie_all/Foreign_Economic_Collection_2011.pdf
[3] http://www.uscc.gov/RFP/2012/USCC%20 Report_Chinese_CapabilitiesforComputer_NetworkOperationsandCyberEspionage.pdf
[4] https://theconversation.com/massive-government-employee-data-theft-further-complicates-us-china-relations-42941; and http://www.darkreading.com/attacks-breaches/state-owned-chinese-firms-hired-military-hackers-for-it-services/d/d-id/1269102

GW Center for Cyber and Homeland Security
2000 Pennsylvania Avenue, NW, Suite 2210 • Washington, DC 20052
Tel: 202-994-2437 • E-Mail: cchs@gwu.edu
http://cchs.gwu.edu

attacks on U.S. research and development have resulted in Russia being deemed (along with China), "a national long-term strategic threat to the United States," by the NCIX.[5]

In 2009, the Wall Street Journal reported that cyber-spies from Russia and China had penetrated the U.S. electrical grid, leaving behind software programs. The intruders did not cause damage to U.S. infrastructure, but sought to navigate the systems and their controls. Was this reconnaissance or an act of aggression? What purpose could the mapping of critical U.S. infrastructure serve, other than intelligence preparation of the battlefield? The NASDAQ exchange, too, has allegedly been the target of a "complex hack" by a nation-state. Again, one questions the motivation.[6]

More recently, Russian hackers believed to be doing their government's bidding breached the White House, the State Department, and the Defense Department.[7] Similar forces were also poised to cyber-attack US banks against the backdrop of economic sanctions levied against Russia for its repeated and brazen incursions into Ukraine.[8]

Russia has also engaged in cyber operations against Ukraine (2014/15), Georgia (2008), and Estonia (2007); in the first two instances combining them with kinetic operations. Equally concerning, if not more so, Russia and China

[5] http://www.ncix.gov/publications/reports/fecie_ all/Foreign_Economic_Collection_2011.pdf
[6] http://www.bloomberg.com/bw/articles/2014-07-17/how-russian-hackers-stole-the-nasdaq
[7] http://www.cnn.com/2015/04/07/politics/how-russians-hacked-the-wh/; and http://thehill.com/policy/cybersecurity/242213-pentagon-head-russian-goals-not-clear-in-dod-hack
[8] http://thehill.com/policy/cybersecurity/241965-russian-hacking-group-was-set-to-hit-us-banks; https://www.fireeye.com/blog/threat-research/2014/10/apt28-a-window-into-russias-cyber-espionage-operations.html; http://www.newsweek.com/how-stop-putin-hacking-white-house-321857; and http://www.cnbc.com/id/102025262

GW Center for Cyber and Homeland Security
2000 Pennsylvania Avenue, NW, Suite 2210 • Washington, DC 20052
Tel: 202-994-2437 • E-Mail: cchs@gwu.edu
http://cchs.gwu.edu

recently signed a cybersecurity agreement pursuant to which they pledge not to hack one another and to share both information and technology.[9]

Over time, Russia's history has also demonstrated a toxic blend of crime, business, and politics—and there are few, if any, signs that things are changing today. To the contrary, a convergence between the Russian intelligence community and cyber-criminals has been observed as relations between Russia and the West have deteriorated as the conflict over Ukraine has unfolded.[10] Evidence of the complicity between the Russian government and its cyber-criminals and hackers became even starker when the Russian Foreign Ministry issued "a public notice advising `citizens to refrain from traveling abroad, especially to countries that have signed agreements with the U.S. on mutual extradition, if there is reasonable suspicion that U.S. law enforcement agencies' have a case pending against them."[11]

Iran

Iran has invested heavily in recent years to deepen and expand its cyber warfare capacity. Under President Rouhani, the country's cybersecurity budget has increased "twelvefold"; and the country may now be considered "a top-five world cyber power."[12]

This concerted effort and the associated rapid rise through the ranks comes in the wake of the Stuxnet worm, which targeted Iran's nuclear weapons development program. How the current international negotiations on containing that program will affect Iran's behavior in the cyber domain, moving forward, remains to be seen.

---

[9] http://www.afpc.org/files/august2012.pdf; and http://thehill.com/policy/cybersecurity/241453-russia-china-unit-with-major-cyber-pact
[10] http://www.theregister.co.uk/2015/04/16/cyber_war_keynote_infiltrate/
[11] http://www.wired.com/2013/09/dont-leave-home/
[12] http://thehill.com/policy/cybersecurity/236627-iranian-leader-has-boosted-cyber-spending-12-fold

GW Center for Cyber and Homeland Security
2000 Pennsylvania Avenue, NW, Suite 2210 • Washington, DC 20052
Tel: 202-994-2437 • E-Mail: cchs@gwu.edu
http://cchs.gwu.edu

What we do know is that Iran has engaged in a concerted cyber campaign against U.S. banks.[13] In January 2013, the Wall Street Journal reported[14] on "an intensifying Iranian campaign of cyberattacks [thought to have begun months earlier] against American financial institutions" including Bank of America, PNC Financial Services Group, Sun Trust Banks Inc., and BB&T Corp. Six leading U.S. banks—including J.P. Morgan Chase—were targeted in "the most disruptive" wave of this campaign, characterized by DDoS attacks. The Izz ad-Din al-Qassam Cyber Fighters claim responsibility for all of these incidents.

U.S. officials also believe Iran to be responsible for a cyber-attack against the Sands Casino in Las Vegas owned by politically active billionaire Sheldon Adelson. The incident appears to be a first: "a foreign player simply sought to destroy American corporate infrastructure on such a scale… PCs and servers were shut…down in a cascading IT catastrophe, with many of their hard drives wiped clean."[15]

Iran has also long relied on proxies such as Hezbollah—which now has a companion organization called Cyber Hezbollah—to strike at perceived adversaries. Iran and Hezbollah are suspected in connection with the August 2012 cyberattacks on the state-owned oil company Saudi Aramco and on Qatari producer RasGas, which resulted in the compromise of approximately 30,000 computers.[16]

In addition, elements of Iran's Revolutionary Guard Corps (IRGC) have also openly sought to pull hackers into the fold, including the political/criminal

[13] http://foreignpolicy.com/2014/02/18/forget-china-irans-hackers-are-americas-newest-cyber-threat/
[14] http://www.wsj.com/articles/SB10001424127887324734904578244302923178548
[15] http://www.bloomberg.com/bw/articles/2014-12-11/iranian-hackers-hit-sheldon-adelsons-sands-casino-in-las-vegas
[16] http://www.wired.com/2015/02/nsa-acknowledges-feared-iran-learns-us-cyberattacks/

GW Center for Cyber and Homeland Security
2000 Pennsylvania Avenue, NW, Suite 2210 • Washington, DC 20052
Tel: 202-994-2437 • E-Mail: cchs@gwu.edu
http://cchs.gwu.edu

hacker group Ashiyane; and the Basij, who are paid to do cyber work on behalf of the regime.[17]

North Korea (DPRK)

As perhaps the world's most isolated state-actor in the international system, North Korea operates under fewer constraints. For this reason, the country poses an important "wildcard" threat, not only to the United States but also to the region and to broader international stability.

South Korea's Defense Ministry estimates that North Korea possesses a force of "about 6,000 cyber agents."[18] A frequent DPRK target, South Korea has attributed a series of cyber-attacks—upon its Hydro & Nuclear Power Company (2014) and upon its banks and broadcasting companies (2013), for example—to North Korea.[19]

From a U.S. standpoint, it is the North Korean attack on Sony Pictures Entertainment late last year that looms large: "`There was disruption. There was destruction of data. There was an intent to hurt the company. And it succeeded, bringing a major U.S. entertainment company to its knees'."[20]

Where will the DPRK go from here? In the words of an Australian expert, "There's growing concern amongst analysts, and government officials alike

[17]http://cchs.gwu.edu/sites/cchs.gwu.edu/files/downloads/Testimony_Cilluffo_April_26_2012.pdf
[18] http://www.nknews.org/2015/03/n-korean-hacking-threat-leads-to-blue-house-cyber-security-office/
[19] http://thediplomat.com/2015/04/south-korea-beefs-up-cyber-security-with-an-eye-on-north-korea/
[20] http://www.cbsnews.com/news/north-korean-cyberattack-on-sony-60-minutes/

GW Center for Cyber and Homeland Security
2000 Pennsylvania Avenue, NW, Suite 2210 • Washington, DC 20052
Tel: 202-994-2437 • E-Mail: cchs@gwu.edu
http://cchs.gwu.edu

that North Korea has begun to rapidly accelerate its development of advanced offensive cyber capabilities'."[21]

The latter development is all the more disturbing when considered in tandem with the following trenchant question raised by one of my CCHS colleagues: "`Given North Korea's proclivity to provide other destructive technologies and military assistance to rogue states and non-state actors, would the DPRK also assist them with destructive cyber capabilities'?"[22]

In addition, recent reports that the United States targeted the DPRK's nuclear program with a version of Stuxnet, but without success, may—if true—further complicate the challenge posed by North Korea.[23]

On many levels, North Korea is both a troubling and unusual case. Ordinarily, it is organized crime that seeks to penetrate the state. In this case, however, it is the other way around—with the state trying to penetrate organized crime in order to ensure the survival of the regime/dynasty.

Foreign Terrorist Organizations

To date, terrorist organizations have not demonstrated the advanced level of cyber-attack capabilities that would be commensurate with these groups' stated ambitions. Undoubtedly, though, these organizations will persist in their efforts to augment their in-house cyber skills and capacities. Of particular concern are foreign terrorist organizations that benefit from state sponsorship and support, as well as the Islamic State in Iraq and Syria

[21] http://www.nknews.org/2015/03/n-korean-hacking-threat-leads-to-blue-house-cyber-security-office/

[22]https://books.google.com/books?id=oG51CAAAQBAJ&pg=PA1&lpg=PA1&dq=north+korea:+the+cyber+wild+card&source=bl&ots=i9IDOgGLS6&sig=xXyFSVkL4LslwPoO6EjWyQc77pI&hl=en&sa=X&ved=0CCYQ6AEwAWoVChMI0eet7fuHxgIVKE2MCh0L_gAv#v=onepage&q=north%20korea%3A%20the%20cyber%20wild%20card&f=false

[23] http://www.reuters.com/article/2015/05/29/us-usa-northkorea-stuxnet-idUSKBN0OE2DM20150529

GW Center for Cyber and Homeland Security
2000 Pennsylvania Avenue, NW, Suite 2210 • Washington, DC 20052
Tel: 202-994-2437 • E-Mail: cchs@gwu.edu
http://cchs.gwu.edu

(ISIS/ISIL). Given ISIS' savvy use of social media and how it has built and maintained a sophisticated propaganda machine, it is likely that the group—and their sympathizers—will turn their efforts towards developing a more robust cyber-attack capability.

The current level of cyber expertise possessed by terrorist groups should bring us little comfort, however, because a range of proxies for indigenous cyber capability exist: there is an arms bazaar of cyber weapons, and our adversaries need only intent and cash to access it. Capabilities, malware, weapons, etc.—all can be bought or rented.[24]

In terms of what we have seen recently, ISIS has invoked a new tactic against members of the U.S. military and law enforcement: "doxing"—which involves gathering personal information from sources online and then publishing that data online, which puts the victim at risk of further attack in both the physical and virtual worlds. [25] A prevalent theme in the drumbeat of ISIS propaganda videos has been repeated calls for "lone wolf" attacks against Western law enforcement and military personnel.

Terrorist organizations also use the internet in a host of ways that serve to further their ends and put the United States and its allies, and the interests of both, in danger. By way of illustration, the internet helps terrorists plan and plot, radicalize and recruit, and train and fundraise.

As terrorist cyber capabilities grow more sophisticated, one especially concerning scenario would involve terrorist targeting of U.S. critical infrastructure, using a mix of kinetic and cyber-attacks. In this scenario, the cyber component could serve as a force multiplier to increase the lethality or impact of the physical attack.

Criminal Organizations

[24]http://cchs.gwu.edu/sites/cchs.gwu.edu/files/downloads/Testimony_Cilluffo_March_20_2013.pdf

[25] http://gizmodo.com/isis-has-a-new-terrorism-tactic-doxing-us-soldiers-1693078782

GW Center for Cyber and Homeland Security
2000 Pennsylvania Avenue, NW, Suite 2210 • Washington, DC 20052
Tel: 202-994-2437 • E-Mail: cchs@gwu.edu
http://cchs.gwu.edu

Cyberspace has proven to be a gold mine for criminals, who have moved ever more deeply into the domain as opportunities to profit there continue to multiply. These criminal groups operate in layered organizations that share networks and tools. Despite reaping 30 cents on the dollar, there is a low chance that these criminals will be held accountable for their actions because they benefit from safe havens in Eastern Europe—which is, according to European Police Office (EUROPOL) Director Robert Wainwright, the source of 80 percent of all cybercrime.

The illicit activities of criminal groups in the virtual world are typically associated with the "Dark Web," a sub-set of the Internet where the IP addresses of websites are concealed. Here, "the sale of drugs, weapons, counterfeit documents and child pornography" constitute "vibrant industries."[26] Cybercriminals have also demonstrated substantial creativity, such as extortion schemes demanding payment via cryptocurrencies, such as Bitcoin. For example, most criminals demand payment for "ransomware" attacks (such as GameOver Zeus or CryptoLocker) to be made via cryptocurrencies, which are attractive to criminal organizations due to their anonymity or pseudonymity. Increasingly, more traditional organized crime groups, such as drug trafficking organizations, are also turning to virtual currencies for payment and to move their money in the black market.

According to EUROPOL whose focus is serious international organized crime, "cybercrime has been expanding to affect virtually all other criminal activities":

> The emergence of crime-as-a-service online has made cybercrime horizontal in nature, akin to activities such as money laundering or document fraud. The changing nature of cybercrime directly impacts on how other criminal activities, such as drug trafficking, the facilitation of illegal immigration, or the distribution of counterfeit goods are carried out. … General trends for cybercrime suggest

[26] http://www.wired.com/2014/11/hacker-lexicon-whats-dark-web/

GW Center for Cyber and Homeland Security
2000 Pennsylvania Avenue, NW, Suite 2210 • Washington, DC 20052
Tel: 202-994-2437 • E-Mail: cchs@gwu.edu
http://cchs.gwu.edu

> considerable increases in scope, sophistication, number and types of attacks, number of victims and economic damage. … This allows traditional OCGs [organized criminal groups] to carry out more sophisticated crimes, buying access to the technical skills and expertise they require.[27]

Cybercriminals possess substantial cyber capabilities and, increasingly, are working with or for nation-states such as Russia. This convergence of forces heightens the dangers posed by both groups (e.g., criminal organizations and nation-states). And from a monetary standpoint alone, the amounts at stake are staggering. Consider: Russia's slice of the 2011 global cybercrime market has been pegged at $2.3 billion.[28]

While the focus of this hearing is on threat rather than response, it bears mention that it is a relatively small, core group of "kingpins" that constitute the heart of the cybercrime problem. If these key figures could be extradited for prosecution, it would go a long way toward combating the problem—and would represent a much more efficient way of tackling the challenge.

"Hacktivists" and Other Entities

Cyberspace largely levels the playing field, allowing individuals and small groups to have disproportionate impact. While some "hacktivists" may possess considerable abilities, the bar here is relatively low, and virtually anyone with a measure of skills and a special interest can cause harm.

Though great sophistication may not be needed to achieve disruption and draw attention to a particular concern, individuals and entities in this category can be a significant force, whether acting alone or loosely in tandem, essentially as a leaderless movement. Recall, for example, the activities of

[27] https://www.europol.europa.eu/newsletter/massive-changes-criminal-landscape; and http://cchs.gwu.edu/counterterrorism-cybersecurity-insights-europol-director-rob-wainwright
[28] http://www.group-ib.com/?view=article&id=705

GW Center for Cyber and Homeland Security
2000 Pennsylvania Avenue, NW, Suite 2210 • Washington, DC 20052
Tel: 202-994-2437 • E-Mail: cchs@gwu.edu
http://cchs.gwu.edu

"Anonymous," whose significant impact has been felt by targets as diverse as the private intelligence firm Stratfor and opponents of the "Arab Spring."[29]

Conclusion

From the standpoint of banking and financial services in particular—a critical U.S. infrastructure sector, cyber-attacks hold the potential to undermine trust and confidence in the system itself, irrespective of the perpetrator. This is just one of many reasons that it is imperative to bolster U.S. prevention, resilience, and response efforts—in partnership with the private sector.

Moving forward, and in connection with this last point, the U.S. government must give companies who now find themselves at the tip of the spear, the framework, parameters, and tools that they need in order to engage in active defense to protect themselves.

Thank you again for this opportunity to testify on this important topic. [30] I look forward to trying to answer any questions that you may have.

[29] http://www.wired.com/2012/07/ff_anonymous/

[30] I would like to thank CCHS Associate Director, Sharon Cardash, for her help in drafting my prepared testimony.

GW Center for Cyber and Homeland Security
2000 Pennsylvania Avenue, NW, Suite 2210 • Washington, DC 20052
Tel: 202-994-2437 • E-Mail: cchs@gwu.edu
http://cchs.gwu.edu

Congressional Testimony

A Global Perspective on Cyber Threats

Michael Madon
Board of Advisors Member
Center on Sanctions and Illicit Finance, FDD
Vice President, Business Development, RedOwl Analytics

The House Committee on Financial Services
Subcommittee on Oversight and Investigations

Washington, DC
June 16, 2015

Center on Sanctions & Illicit Finance
FOUNDATION FOR DEFENSE OF DEMOCRACIES
1726 M Street NW ● Suite 700 ● Washington, DC 20036

Chairman Duffy, Vice Chairman Fitzpatrick, Ranking Member Green, and other distinguished members of the Committee, it is an honor to appear before you to discuss the global cyber threats we face and in my view, more importantly, what we can do about it.

During my time at Treasury, I was fortunate to work for and with a team of true innovators developing novel strategies and approaches to identify and mitigate the cyber risks and vulnerabilities facing both the department and financial sector more broadly. More recently, I have worked closely with Juan Zarate, a visionary and founder of that early Treasury team and who currently serves as Chairman and Senior Counselor of the Center on Sanctions and Illicit Finance (CSIF) at the Foundation for Defense of Democracies. The thoughts below are inspired by our early Treasury work and taken in no small measure from Juan's current writings on this topic.

Five Primary Cyber Threats

While cyber attacks and intrusions threaten US private sector institutions on a daily basis, cyber attacks against financial services institutions in particular are becoming more frequent, more sophisticated, and more widespread. In my view, the rise in frequency and breadth of these cyber attacks can be attributed to five primary threats:

- First, nation states striving to steal intellectual capital from banks and/or destabilize them;
- Second, cyber terrorists seeking to disrupt and destroy the transactional glue that binds our community of nations and who view our financial institutions as symbols of Western capitalism.
- Third, "hacktivists" who make opportunistic attempts to break into banks' IT networks, to draw attention to some cause or deeply held belief.
- The fourth are organized crime elements who breach systems for monetary gain.
- The fifth is the insider threat. In its most recent Data Breach Investigation Report, Verizon provided the following observation on all security incidents reported in 2014, "It may not be obvious at first glance, but the common denominator across the top four patterns - accounting for nearly 90% of all incidents - is people. Whether it's goofing up,

> getting infected, behaving badly or losing stuff, most incidents fall in the [user error category].” The uncomfortable truth here is that individuals that we bring inside the enterprise and trust with systems and data access are the root cause or unknowing enablers of most cyber incidents.

Threats against the Financial Community.

If the recent attacks against JPMorgan Chase & Co. and Citibank serve as examples, banks are prime, vulnerable targets for sophisticated, organized cyber attacks, despite a dramatic increase in cyber security spending. The frequency, sophistication, and breadth of attacks on banks are swelling in large part because banks hold not just money but also collect and centralize sensitive personally identifiable information and clients’ intellectual property.

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.”

Further, banks have been pulled into a more serious and sustained cyber financial battle. The primary cyber threats realize that banks serve as both key systemic actors important for the functioning of the global economy and as chief protagonists in the isolation of bad actors from the financial system. Thus, the financial community finds itself drawn into combined financial and cyber battles – neither of which they control. As Juan Zarate has noted,

> “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. 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.”

Our society's current response is not sufficient to address growing cyber threats. We need to have a more pro-active approach, one that shifts the paradigm away from defense to offense. We can take inspiration from the anti-money laundering and sanctions model forged at Treasury and leverage financial pressure against cyber threats to better protect the financial system. This would entail a model to promote "Cyber-Driven Targeted Financial Measures" to empower and enlist the private sector to better defend its systems in coordination with the government.

A Snapshot of Current Private and Public Sector Partnerships

Collaboration between the public and private sector, and the financial sector in particular, is not new. But the process for sharing information among the private sector and with government has been 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. Collaboration has also relied on private sector threat intelligence services that do not necessarily communicate with others. But there are some diamonds in the ruff:

- The Financial Services Information Sharing and Analysis Center (or FS-ISAC) is the primary industry forum for collaboration on critical security threats facing the global financial services sector and has grown increasingly operational. For example, the 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 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 financial sector requests.

- 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 the private sector and government.

- In February of this year, President Obama signed an Executive Order to encourage and promote sharing of cybersecurity threat information within the private sector and between the private sector and government.

- Cyber analysts within the US Intelligence Community continue working 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.

    - The US Secret Service uses the Electronic Crimes Task Force (ECTF) to leverage the combined resources of local, state, and law enforcement with prosecutors, private industry, and academia to combat 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.

There is no dearth of attempts by the US government to try to increase information sharing with the private sector. Indeed, the private sector—including the financial industry—often feels bombarded by different government agencies attempting to gain access to information or serve

as the principal interlocutor for the government. The private sector also feels exposed without legislation to protect their activities. Indeed, all of these aforementioned models 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 openly divulge their vulnerabilities.

Further, under the current system, there is little incentive for pro-active defense of financial systems and legal restrictions on more aggressive monitoring and disruption in cyber-space by systemically relevant and important private sector entities. And so 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 is increasingly at risk from sophisticated attackers.

Cyber-Driven Targeted *Financial* Measures

A new economic and cyber security approach requires a new paradigm of US public-private engagement and collaboration. This involves an evolution from classic, state-based national security actions toward deeper involvement of and reliance on the private sector in arenas previously confined to the halls of government, with a commensurate and widening appreciation within governments of the private sector to influence international security.

As Juan Zarate notes, "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." Further, as certain verticals within the financial sector increasingly become commoditized, a robust program of public-private engagement and collaboration may become the discriminator - the edge -that drives profits.

These measures seek to:

- Encourage the creation of internal Financial Intelligence Units (FIU) to enhance financial sector and augment US Intelligence Community collection and analysis efforts. Many banks have already or are now establishing FIUs 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.

- Enhance Safe Harbor Regime to Encourage Greater Information Sharing Among Financial Institutions. Secretary of the Treasury Jack Lew recently made the case for clearer rules of the road to allow for information sharing and protection of rights:

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

- Enhance Section 314(b) of the USA PATRIOT Act to allow financial institutions to share information about suspect cyber-related 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.

- Accelerate the US government's targeting of state actors, networks, and individuals that attack US private sector systems – especially financial systems. US law enforcement has consistently investigated cases of breaches, including of organized crime rings and hackers that successfully penetrate US-based systems, with indictments often following.

- Deploy the President's emergency economic powers for the use of multiple tools to address the reality of major cyber espionage, crime, and infiltration affecting the US financial and commercial system.
  - In the first instance, the President should sign a new executive order, based on his power under the International Emergency Economic Powers Act (IEEPA), that

would allow the Secretary of the Treasury, in coordination with the Secretary of State and the Attorney General, to identify cyber hackers, state sponsors, and those entities and individuals owned or controlled, who financially support such activities, or who are otherwise associated. This would allow the US government to 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 attacks to include infiltrations, disruptions, and espionage.

- Encourage Congress to 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. As with the provisions of Section 311 of the USA PATRIOT Act regarding "primary money laundering concerns," the label of "primary cyber security 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 US those companies or entities found to be benefiting or profiting from cyber espionage.

Cyber-Driven Targeted *Active-Defensive* Measures

Innovative criminals require innovative responses and Congress could enlist the private sector in participating in a cyber-driven targeted, active-defensive measures that reward, enable, and empower 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 US 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 model could take different forms to include:

- A Reward Program for those groups able to uncover, identify, and even "deliver" cyber hackers to US courts or authorities – as security groups have done in the past. Admittedly, attribution of activities carried out through the internet is extremely difficult and, in many cases, impossible to achieve. There is a large swath of grey among these groups – and the swath is just getting bigger. For example, tracing the line where a Russian hacktivist or organized criminal network ends and the Russian government begins can be dashed, missing, picked up again as a solid line, only to dissolve soon after into a suspicion or best guess. Yet, as the "attribution revolution" in the private sector – with ever better cyber forensic technology to identify the source of cyber attacks – begins to shed light on once opaque activities, the possibility of more aggressive tracking, detection, and targeting becomes a reality.

- Unleash the Power of Cyber Forensic Teams and Private Litigants and plaintiff's lawyers against those attacking US systems. 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.

- Empower Victims of Attacks 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 cyber attacks. 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 benefiting from the attacks.

- Encourage the US Department of Justice, Department of Homeland Security, and Treasury Department to consider issuing special cyber warrants – another type of "letter of marque and reprisal" -- to allow US private sector actors to track and even disrupt cyber attacks in certain instances to defend their systems. While this would not happen overnight and would require a defendable attribution regime and real-time capability to respond to targets of opportunity and evaluation of the negative externalities of any such action

The government today is in a position to enable the private sector – and even private individuals – to pursue active defensive measures on its behalf vis-à-vis a new model. 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, and usher in a new era of financial warfare.

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 sets international standards and norms on anti-money laundering, 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.

Committee members, thank you for allowing me to appear before you and discuss the global cyber threats. My colleagues at the Center on Sanctions and Illicit Finance and I look forward to collaboratively devising and implementing strategies to defeat the growing cyber-threats that confront our nation.

Statement for the Record

Richard Bejtlich

Chief Security Strategist

FireEye, Inc.

Before the

U.S. House of Representatives

Committee on Financial Services

Subcommittee on Oversight and Investigations

A Global Perspective on Cyber Threats

June 16, 2015

Chairman Duffy, Ranking Member Green, members of the Subcommittee, thank you for the opportunity to testify. I am Richard Bejtlich, Chief Security Strategist at FireEye. I am also a nonresident senior fellow at the Brookings Institution, and I am pursuing a PhD in war studies from King's College London. I began my security career as a military intelligence officer in 1997 at the Air Force Information Warfare Center. My employer, FireEye, provides software to stop digital intruders, with 3,400 customers in 67 countries, including 250 of the Fortune 500. Our Mandiant consulting service, known for its 2013 report on Chinese PLA Unit 61398, helps companies identify and recover from intrusions. In 2014, we conducted hundreds of investigations in 13 countries.

The title of this hearing includes the phrase "cyber threat." Understanding the threat is necessary, but not sufficient. We should expand our focus and discuss "risk" associated with specific damaging scenarios, and incorporate threats, vulnerabilities, and consequences. Risk is a function of these three factors, and influencing any one or more changes our overall level of security. Furthermore, while risk is a forward-looking concept -- we worry about what could happen -- some scenarios have already occurred, making a theoretical risk an actualized event.

I separate damaging scenarios into two categories: chronic and acute. Chronic scenarios occur over an extended period, with impact spread across time in ways that can be difficult to measure. Acute scenarios involve immediate and distinct impact, usually with obvious physical or virtual damage. Thankfully, we have not yet seen a combination of these two categories, i.e., long-term, highly-visible, costly damage. Hopefully that will remain the case.

The United States is currently suffering three important chronic damage scenarios. First, foreign nation state actors are stealing sensitive data and commercial secrets from private organizations, for use by their domestic industries. Second, these actors are stealing sensitive and classified data on American military and intelligence plans and technologies, to benefit their strategic interests. Third, foreign actors are stealing personally identifiable information and financial instruments from citizens and organizations, to benefit national capabilities and fuel underground crime. The theft of commercial, government, and personal data is an actualized risk, and it remains a current and future risk.

The United States is also susceptible to two acute damage scenarios. First, many security professionals worry about attacks against critical infrastructure. The electrical grid, finance sector, water supply, and

telecommunications systems are the “big four” targets. To date, according to public testimony and reporting, some foreign actors have infiltrated elements of critical infrastructure, while others have attempted to at least disrupt critical infrastructure. The second acute damage scenario involves disruption or destruction of virtual infrastructure. In two public examples, foreign actors have infiltrated American companies and destroyed data on thousands of computers.

With this understanding of risk due to specific scenarios, let’s briefly discuss threat actors. Security professionals classify threats into four broad categories: nation-states, organized criminals, terrorists, and activists. There is some overlap and mixing among the teams or individuals in these categories, along with their motivations for action. Traditional cyber security tools, tactics, and processes are generally sufficient when countering current terrorist and activist capabilities. Organized criminals are adopting more of the capabilities of nation-state groups. Nation-states are the top of the pack, and more of them are entering the digital arena. Therefore, I focus on my testimony on the top four nation-state threat actors: Russia, China, North Korea, and Iran.

Russia poses chronic and acute challenges. Russian government and affiliated forces can conduct full-spectrum information operations, and they possess top tier cyber capabilities, including the ability to preserve operational security and partially frustrate forensic analysis. According to open sources, Russian forces have infiltrated some elements of American critical infrastructure, but these forces have not used that access to inflict damage. Russian and Russian-speaking criminal actors are a major source of financial hardship for American companies and individuals. Geopolitically, Russia is a cause for worry due to the ongoing war in Ukraine.

China also poses chronic and acute challenges. Chinese government and affiliated forces can conduct full-spectrum information operations, although not at the Russian level. What they lack in top-tier sophistication they make up for in volume and persistence. Chinese theft of commercial and sensitive data from American companies is unequalled, and ongoing. According to open sources, Chinese forces have also infiltrated some elements of American critical infrastructure, but have not used that access to inflict damage. Chinese criminal actors are active but not to the degree seen by their eastern European counterparts. Geopolitically, China is a cause for worry due to the escalating tensions in the East China Sea and South China Sea.

North Korea primarily poses acute challenges. North Korean government and affiliated forces have invested heavily in developing their cyber capabilities. In contrast with their Russian and Chinese counterparts, North Korean forces have stepped beyond the espionage line in order to inflict virtual damage, first against South Korean targets, and then against an American victim, Sony Pictures Entertainment, in November 2014. Geopolitically, North Korea is a cause for worry due to their aggressive posture towards the West.

Iran primarily poses acute challenges. Iranian government and affiliated forces are enhancing their cyber capabilities. Similar to North Korea, Iranian forces have stepped beyond the espionage line in order to inflict virtual damage, first against targets in the Middle East, and then against an American victim, Sands Casino, in February 2014. Iran has also demonstrated specific interest in degrading the American financial sector, via distributed denial of service attacks in 2012. Geopolitically, Iran may be less of a cause for worry, depending on the outcome of the P5+1 nuclear talks.

Although I just outlined four nation-state threats, note that other countries are developing capabilities to harm American national interests. Furthermore, these four nation-states, and others, may collaborate with criminal groups, terrorists, and activists, sometimes obscuring the identity of the responsible party. However, advances in attribution during the last five years have enabled the American intelligence community to act with confidence when investigating strategically significant intrusions.

I will conclude by mentioning the last two elements of risk, which are vulnerabilities and consequences. American interests and infrastructure remain largely vulnerable to the chronic and acute scenarios I outlined earlier. In the private sector, financial and defense companies are best resourced and postured to counter threat actors. However, I remind the Subcommittee that even these industries are worried. Last year, Bloomberg reported a private proposal by the Securities Industry and Financial Markets Association (SIFMA) for a "cyber war council" with the US government.[1] Beyond finance and defense, the remainder of the American economy and population remains in danger. Government at federal, state, local, and tribal levels is similarly at risk, although the primary threats to the military and intelligence communities appear to those of untrustworthy insiders. It is increasingly difficult for

[1] Carter Dougherty, "Banks Dreading Computer Hacks Call for Cyber War Council," Bloomberg, July 8, 2014. http://www.bloomberg.com/news/articles/2014-07-08/banks-dreading-computer-hacks-call-for-cyber-war-council

organizations to detect and respond to intrusions on their own. In 2014, only 31 percent of organizations discovered, via their own resources, that they were breached – down from 33 percent in 2013 and 37 percent in 2012.

In terms of consequences, costs continue to increase. On the financial crime front, the 2015 Cost of Data Breach Study by IBM and the Ponemon Institute reported that "the average cost for each lost or stolen record containing sensitive and confidential information increased from $201 to $217," while "the total average cost paid by organizations increased from $5.9 million to $6.5 million."[2] Worse, the types of personally identifiable data being stolen increasingly include "permanent data," such as Social Security numbers and health care records. Although credit cards are easily replaced at minimal cost to the victim, there is no business process to recover from the theft of Social Security numbers or health records. On the national security front, we are all aware of the series of devastating breaches in the news.

I look forward to your questions, where I hope we can discuss strategies for mitigating these risks.

[2] IBM and the Ponemon Institute, "2015 Cost of Data Breach Study," http://www-03.ibm.com/security/data-breach/