A GLOBAL PERSPECTIVE ON CYBER THREATS

HEARING

BEFORE THE

SUBCOMMITTEE ON OVERSIGHT AND INVESTIGATIONS

OF THE

COMMITTEE ON FINANCIAL SERVICES

U.S. HOUSE OF REPRESENTATIVES

ONE HUNDRED FOURTEENTH CONGRESS

FIRST SESSION

JUNE 16, 2015

Printed for the use of the Committee on Financial Services

Serial No. 114–32

U.S. GOVERNMENT PUBLISHING OFFICE

96–993 PDF WASHINGTON : 2016

For sale by the Superintendent of Documents, U.S. Government Publishing Office
Internet: bookstore.gpo.gov Phone: toll free (866) 512–1800; DC area (202) 512–1800
Fax: (202) 512–2104 Mail: Stop IDCC, Washington, DC 20402–0001

HOUSE COMMITTEE ON FINANCIAL SERVICES

JEB HENSARLING, Texas, *Chairman*

PATRICK T. MCHENRY, North Carolina, *Vice Chairman*
PETER T. KING, New York
EDWARD R. ROYCE, California
FRANK D. LUCAS, Oklahoma
SCOTT GARRETT, New Jersey
RANDY NEUGEBAUER, Texas
STEVAN PEARCE, New Mexico
BILL POSEY, Florida
MICHAEL G. FITZPATRICK, Pennsylvania
LYNN A. WESTMORELAND, Georgia
BLAINE LUETKEMEYER, Missouri
BILL HUIZENGA, Michigan
SEAN P. DUFFY, Wisconsin
ROBERT HURT, Virginia
STEVE STIVERS, Ohio
STEPHEN LEE FINCHER, Tennessee
MARLIN A. STUTZMAN, Indiana
MICK MULVANEY, South Carolina
RANDY HULTGREN, Illinois
DENNIS A. ROSS, Florida
ROBERT PITTENGER, North Carolina
ANN WAGNER, Missouri
ANDY BARR, Kentucky
KEITH J. ROTHFUS, Pennsylvania
LUKE MESSER, Indiana
DAVID SCHWEIKERT, Arizona
FRANK GUINTA, New Hampshire
SCOTT TIPTON, Colorado
ROGER WILLIAMS, Texas
BRUCE POLIQUIN, Maine
MIA LOVE, Utah
FRENCH HILL, Arkansas
TOM EMMER, Minnesota

MAXINE WATERS, California, *Ranking Member*
CAROLYN B. MALONEY, New York
NYDIA M. VELÁZQUEZ, New York
BRAD SHERMAN, California
GREGORY W. MEEKS, New York
MICHAEL E. CAPUANO, Massachusetts
RUBÉN HINOJOSA, Texas
WM. LACY CLAY, Missouri
STEPHEN F. LYNCH, Massachusetts
DAVID SCOTT, Georgia
AL GREEN, Texas
EMANUEL CLEAVER, Missouri
GWEN MOORE, Wisconsin
KEITH ELLISON, Minnesota
ED PERLMUTTER, Colorado
JAMES A. HIMES, Connecticut
JOHN C. CARNEY, JR., Delaware
TERRI A. SEWELL, Alabama
BILL FOSTER, Illinois
DANIEL T. KILDEE, Michigan
PATRICK MURPHY, Florida
JOHN K. DELANEY, Maryland
KYRSTEN SINEMA, Arizona
JOYCE BEATTY, Ohio
DENNY HECK, Washington
JUAN VARGAS, California

SHANNON MCGAHN, *Staff Director*
JAMES H. CLINGER, *Chief Counsel*

SUBCOMMITTEE ON OVERSIGHT AND INVESTIGATIONS

SEAN P. DUFFY, Wisconsin, *Chairman*

MICHAEL G. FITZPATRICK, Pennsylvania, *Vice Chairman*
PETER T. KING, New York
PATRICK T. MCHENRY, North Carolina
ROBERT HURT, Virginia
STEPHEN LEE FINCHER, Tennessee
MICK MULVANEY, South Carolina
RANDY HULTGREN, Illinois
ANN WAGNER, Missouri
SCOTT TIPTON, Colorado
BRUCE POLIQUIN, Maine
FRENCH HILL, Arkansas

AL GREEN, Texas, *Ranking Member*
MICHAEL E. CAPUANO, Massachusetts
EMANUEL CLEAVER, Missouri
KEITH ELLISON, Minnesota
JOHN K. DELANEY, Maryland
JOYCE BEATTY, Ohio
DENNY HECK, Washington
KYRSTEN SINEMA, Arizona
JUAN VARGAS, California

CONTENTS

WITNESSES

TUESDAY, JUNE 16, 2015

APPENDIX

ADDITIONAL MATERIAL SUBMITTED FOR THE RECORD

A GLOBAL PERSPECTIVE ON CYBER THREATS

Tuesday, June 16, 2015

U.S. HOUSE OF REPRESENTATIVES,
SUBCOMMITTEE ON OVERSIGHT AND INVESTIGATIONS,
COMMITTEE ON FINANCIAL SERVICES,
Washington, D.C.

The subcommittee met, pursuant to notice, at 10:03 a.m., in room 2128, Rayburn House Office Building, Hon. Sean Duffy [chairman of the subcommittee] presiding.

Members present: Representatives Duffy, Fitzpatrick, Fincher, Wagner, Tipton, Poliquin, Hill; Green, Cleaver, Beatty, Heck, Sinema, and Vargas.

Ex officio present: Representative Hensarling.

Also present: Representative Royce.

Chairman DUFFY. The Oversight and Investigations Subcommittee will come to order. The title of today's hearing is, "A Global Perspective on Cyber Threats."

Without objection, the Chair is authorized to declare a recess of the subcommittee at any time.

The Chair now recognizes himself for 3 minutes for an opening statement.

The purpose of today's hearing is to identify the United States' primary cyber enemies, better understand the growing global cyber threat, and ultimately formulate more effective responses to cyber incidents.

The cyber landscape today is vastly different from that of past years, with technology an integral component of nearly all transactions, means of communication, and methods of transportation. In recent years, there has been a growing focus on protecting the cyber security of critical infrastructure.

However, in the wake of the breach of over four million personnel records at the Office of Personnel Management, it is still clear that much more needs to be done to protect Americans from cyber threats.

Cyber crime provides a clear and present danger to the United States of America. At the other end of these attacks are nation-states like Russia, China, Iran, and North Korea; terrorist groups; criminal organizations; and hacktivists. These groups can range from sophisticated cyber actors to ideological groups motivated by political or patriotic reasons.

While the motivations may vary, there remains one constant. They intend to hurt America and our interests. Not only are they

targeting the critical infrastructure of our country such as banks, power grids, and food supplies, but they also pose a much graver threat directly to the citizens of the United States.

Nearly every government agency has been a target of cyber attacks, and with the recent OPM breach, the Federal Government has now provided a channel for these criminals to access sensitive personal information.

In the wake of these incidents, the Consumer Financial Protection Bureau (CFPB) continues to collect information on consumers and their financial practices, and "Obamacare" has created a vast data hub to collect and store scores of highly sensitive personal and health information on American citizens.

This most recent cyber attack on OPM should underscore the urgency around reconsidering the need for such governmental data collection programs. The benefits do not allay the privacy risks to American citizens.

The extent to which this information is utilized to harm our government's employees is yet to be known. But what is known is that more needs to be done to mitigate these cyber risks.

I welcome our distinguished panel this morning, and I look forward to hearing more about what the Federal Government can do and should be doing to protect our country and our citizens from these cyber criminals.

With that, I yield 4 minutes to the gentleman from Texas, Mr. Green.

Mr. GREEN. Thank you, Mr. Chairman. And I thank the witnesses, as well. Mr. Chairman, there appears to be clear and convincing evidence that cyber attacks pose a clear and present danger not only to the United States' businesses but also to the U.S. Government itself.

The preponderance of the evidence shows that 2014 was a banner year for cyber criminals. According to a report from the Heritage Foundation written by Riley Walters, the list of cyber attacks in 2014 on private U.S. companies includes the following excerpts. And Mr. Chairman, in my opinion, one of the best ways to appreciate the magnitude of a problem is to examine and review some of the components. Let's review some of the components.

January 2014: Target hacked, 70 million people impacted; Neiman-Marcus hacked, 350,000 people impacted; Michaels retail store hacked, 2.6 million customers impacted; Yahoo! hacked, 273 million users impacted.

April 2014: Aaron Brothers retail store hacked, 400,000 customers impacted

May 2014, eBay hacked, 233 million customers impacted.

June 2014, Feedly Communications hacked, 15 million users impacted.

September 2014: Home Depot hacked, 56 million shoppers impacted; Google hacked, 5 million people impacted; Goodwill Industries hacked, 868,000 people impacted.

And of course, in October, JPMorgan Chase hacked, 76 million households impacted.

According to this report, in 2014 the annual average cost per company of successful cyber attacks increased to $20.8 million in

the financial services industry; $14.5 million in the technology sector; and $12.7 million in the communications industry.

These are real people. These are real concerns, and they must be addressed.

Mr. Chairman, I fear that FBI Director James Comey was right when he proclaimed there are two kinds of big companies in the United States—those who have been hacked and those who don't know that they have been hacked.

Mr. Chairman, I will yield back the balance of my time. Actually, rather than yield back, I will share it with the gentlelady that you will call next.

Chairman DUFFY. Thank you, Mr. Green.

The Chair now recognizes the gentleman from Pennsylvania, Mr. Fitzpatrick, the vice chairman of our subcommittee, for 1 minute.

Mr. FITZPATRICK. Thank you, Mr. Chairman, and I also thank the three witnesses for being here today to share your experience and your knowledge with the subcommittee.

The protection of our personal data is increasingly a critical part of our private lives, and the threat of data breaches from state or non-state actors looms heavy over security experts in nearly every sector of the American economy.

These types of attacks have real financial and emotional consequences. When families back in my hometown of Levittown learn that their information was compromised, they immediately become concerned about whether they will be able to use their debit card to purchase gas and groceries. But for our Nation's financial institutions, the risks are significant and they are systemic.

Mr. Chairman, there is a task force to investigate terror finance. I am especially interested in the possibility that this data, once stolen, could be sold to fund illicit operations, or as recent reports regarding the OPM theft have shown, be used against United States government personnel.

I look forward to hearing the witnesses' testimony, and I hope that this committee can work together to strengthen and protect this vital part of our Nation's security and infrastructure.

I yield back.

Chairman DUFFY. The gentleman yields back.

The Chair now recognizes the gentlelady from Arizona for 2 minutes.

Ms. SINEMA. Thank you, Chairman Duffy and Ranking Member Green.

Earlier this month, the Office of Personnel Management revealed that at least four million, and perhaps substantially more, current and former Federal employees from nearly every Federal agency, some of them military and defense personnel living in Arizona, may have had their personal information stolen.

While DHS and the FBI continue to investigate this incident, it is strongly suspected that Chinese hackers are responsible for the breach. Cyber attacks from state and non-state actors have increased dramatically in recent years. The U.S. Government needs a clear strategy to deter, as well as detect and defeat ever-changing cyber threats.

Federal law sets forth various requirements, roles, and responsibilities for securing Federal agencies' systems and information.

Despite these measures, according to an April 2015 GAO report, Federal agencies continue to demonstrate shortcomings in assessing risks, developing and implementing security controls, and monitoring results.

Securing our government requires strengthened security controls and information-sharing infrastructures. Educating Federal employees and contractors is also crucial if these efforts are to be successful.

I look forward to hearing more from our witnesses today about the effectiveness of actions taken by Federal agencies to address cyber vulnerabilities.

Thank you, Mr. Chairman. I yield back my time.

Chairman DUFFY. The gentlelady yields back.

We now recognize our witnesses. We have Mr. Frank Cilluffo, an associate vice president at George Washington University; director of the Center for Cyber and Homeland Security; and co-director of GW's Cyber Center for National and Economic Security. Mr. Cilluffo has published extensively on cyber and homeland security.

In addition, he has served on various national security-related committees sponsored by the government and nonprofits, including as the vice chairman of the Future of Terrorism Task Force of the Homeland Security Advisory Council and chairman of the Quadrennial Homeland Security Review Advisory Council.

Previously, Mr. Cilluffo served as Special Assistant to the President for homeland security. Immediately after the September 11, 2001, terrorist attacks, President George W. Bush appointed him to the Office of Homeland Security, where he was a principal adviser to Governor Tom Ridge. Mr. Cilluffo directed the President's Homeland Security Advisory Council.

We also have Mr. Michael Madon. He serves on the board of advisors of the Center on Sanctions and Illicit Finance at the Foundation for Defense of Democracies, and is the vice president of business development at Redowl Analytics.

Previously, Mr. Madon served as Deputy Assistant Secretary in the Office of Intelligence and Analysis of the Treasury Department, where he developed strategies to help identify and mitigate cyber risks within both the Department and the financial sector.

Mr. Madon holds an MBA from Wharton School, a master's of international affairs from Columbia, and a BA from Cornell. He is the recipient of the Bronze Star, the National Intelligence Distinguished Service Medal, and Treasury's Distinguished Service Award.

And finally, last but not least, Mr. Richard Bejtlich. Welcome. He is the chief security strategist at FireEye' a nonresident senior fellow in the Center for 21st Century Security in intelligence of the foreign policy program at Brookings; and a board member of the Open Information Security Foundation.

Mr. Bejtlich was Mandiant's chief security officer. Before that, he was the director of incident response for GE, and before that, he worked extensively in the private sector. Previously, Mr. Bejtlich was a military intelligence officer in the U.S. Air Force Computer Emergency Response Team, Air Force Information Warfare Center and Air Intelligence Agency.

He has a master's of public policy from Harvard University and a BS from the United States Air Force Academy.

So with that, gentlemen, you will each be recognized for 5 minutes for an oral presentation of your testimony. And without objection, the witnesses' written statements will be made a part of the record. Once the witnesses have finished presenting their testimony, each member of the subcommittee will have 5 minutes within which to ask questions.

Now, on your table, you have three lights—green, yellow, and red. Green means go, yellow means you have 1 minute left, and red means your time is up. The microphones are sensitive, so please make sure that you are speaking directly into them.

And with that, Mr. Cilluffo, you are recognized for 5 minutes.

STATEMENT OF FRANK J. CILLUFFO, DIRECTOR, THE GEORGE WASHINGTON UNIVERSITY CENTER FOR CYBER AND HOMELAND SECURITY

Mr. CILLUFFO. Thank you, Mr. Chairman. And thank you, Ranking Member Green, and the distinguished members of the subcommittee for the opportunity to testify before you today.

I thought "red" meant we were being hacked, given the topic, but I am glad that I have to sum up my remarks quickly.

I thought all of you did a terrific job summing up the threat, so I will try to zero in on a handful of different issues that, hopefully, we will have time to explore further during Q&A.

Clearly, the United States currently faces a dizzying array of cyber threats from many and varied actors. Virtually every day, there is a new incident in the headlines, and the initiative today clearly remains with the attacker.

The U.S. financial services sector, from banks to credit card companies to exchanges and clearinghouses, is clearly in the crosshairs and is a primary target for cyber attacks and cyber crime.

To give you a sense of the magnitude of the problem, consider the following figures, which were provided to me 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 attacks, approximately 22,000 came from criminal organizations and 400 from nation-states.

A few words on the threat itself. First, not all hacks are the same, nor are all hackers the same. The threat comes in various shapes, sizes, and forms, ranging from nation-states at the high end of the threat spectrum to foreign terrorist organizations, criminal enterprises, and hacktivists.

Just as diverse as the threat actors themselves are their intentions; capabilities; and tactics, techniques, and procedures (TTPs) and the tools they utilize to commit these crimes.

Put another way, nearly every form of conflict today and tomorrow will have a cyber dimension to it. Whereas technologies will continue to evolve and change, human nature remains consistent. If it happens in the physical world, it is happening in the cyber

world, and increasingly, you are seeing the physical and cyber worlds converge.

One factor that makes cyber unique, of course, is time and space, or speed and impact. You can commit a cyber crime without ever stepping foot in the target area or even the same country, and it would take years, say, to rob bank after bank after bank, which can now be done in a matter of nanoseconds by pointing and clicking on a mouse.

A couple of very quick top-line words on the threat actors. As I mentioned earlier, nation-states and their proxies continue to present the greatest, meaning most advanced and persistent, threat in the cyber domain. Topping the list are countries that are integrating computer network attack and computer network exploit into their war-fighting doctrine and strategy.

The most sophisticated and active countries are China and Russia. It is also worth noting that the two countries recently signed a major cyber security agreement, dubbed by a friend of mine as a new axis of e-vil. Both China and Russia are known to use proxies to do their bidding to provide plausible deniability of their attacks if they get caught.

After these two countries, come Iran and North Korea. While perhaps not up to par with Russia or China in terms of capability, both countries are investing very heavily into building out their cyber capacity, and what they may lack in capability, they more than make up for in intent.

Moreover, they are more likely to turn to computer network attack, rather than merely espionage, as demonstrated by Iran's distributed denial of service attacks on U.S. banks and North Korea's recent attack on Sony.

Next up are foreign terrorist organizations. They certainly possess the motivation and intent, but fortunately, they have yet to fully develop a sustained cyber attack capability. The recent doxing attacks, however, on our U.S. military and law enforcement personnel is a very troubling sign, with their coming up with new tactics, and I think it is 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 obviously differs from foreign terrorist organizations. Rather than being motivated by ideology, they are motivated by profit. And they are continuing—one of the trends we are seeing is working as proxies with other nation-states, as I mentioned vis-a-vis Russia.

And then, of course, you have hacktivists. And regardless of the cause, they are going to use their techniques for special interests, and some of those can be very sophisticated. And their intent is normally to embarrass to bring attention to their cause.

While I planned to say a couple of words on what we should do about all this, I hope we will have an opportunity to discuss that during Q&A.

Mr. Chairman, thank you.

[The prepared statement of Mr. Cilluffo can be found on page 41 of the appendix.]

Chairman DUFFY. Thank you, Mr. Cilluffo.

The Chair now recognizes Mr. Madon for 5 minutes.

STATEMENT OF MICHAEL MADON, BOARD OF ADVISORS MEMBER, CENTER ON SANCTIONS AND ILLICIT FINANCE, FOUNDATION FOR DEFENSE OF DEMOCRACIES

Mr. MADON. Chairman Duffy, Vice Chairman Fitzpatrick, Ranking Member Green, and other distinguished members of the subcommittee, 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 the financial sector more broadly.

The thoughts I am sharing today are inspired by that early Treasury work and the thinking spearheaded by Juan Zarate and his Center on Sanctions and Illicit Finance.

If the recent attacks against JPMorgan Chase and Citibank serve as examples, banks are prime targets for sophisticated, organized cyber attacks, despite a dramatic increase in cyber security spending. In my view, the rise in frequency and breadth of cyber attacks can be attributed to five primary threats—nation-states, cyber terrorists, hacktivists, organized criminal elements and malicious, compromised, or negligent employees—in other words, the insider threat.

So why banks? On a tactical level, banks hold not just money but also collect and centralize sensitive personally identifiable information and clients' intellectual property.

But our cyber threats see a greater purpose in hitting banks. They 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.

It is clear from watching these attacks dramatically increase in both frequency and damage, that our Nation's current defensive posture is simply not sufficient to address the threat. We need to have a more proactive 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 economic and cyber security approach requires a new paradigm of U.S. public-private engagement and collaboration, adopting language from Treasury's successful campaign. Cyber-driven targeted financial measures is, at its core, a thoughtful set of decisions that change our cyber posture from a defensive crouch to an offensive charge.

These measures can encourage the creation of internal financial intelligence units to enhance financial sector and augment U.S. intelligence community collection and analysis efforts. These measures include:

Enhancing the safe harbor regime to encourage greater information sharing among financial institutions.

Enhancing 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.

Accelerating the U.S. Government's targeting of state actors, networks, and individuals that attack U.S. private sector systems, especially financial systems.

Deploing 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 U.S. financial and commercial system.

And encouraging 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 a precursor to sanctions.

Innovative attacks require innovative responses, and Congress could enlist the private sector to participate in cyber-driven targeted active defensive measures that reward, enable, and empower the private sector to help defend itself in concert with the government. Yes, 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 issuances of letters of marque and reprisal, as provided for explicitly in Article 1, Section 8 of the U.S. Constitution. This model could take different forms to include a reward program for those groups able to uncover, identify, and even deliver cyber hackers to U.S. courts or authorities, such as unleashing cyber forensic teams and private litigants and plaintiffs' lawyers against those attacking U.S. systems; empowering victims of attacks to sue the perpetrators and those benefiting directly from any cyber infiltrations, just as victims of terrorism are provided the right to sue terrorists and their supporters today; and encouraging Justice, DHS, and Treasury to consider issuing special cyber warrants to allow private sector actors to track and even disrupt cyber attacks in certain instances to defend their systems.

Committee members, thank you for allowing me to appear before you and discuss 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.

Thank you.

[The prepared statement of Mr. Madon can be found on page 56 of the appendix.]

Chairman DUFFY. Thank you, Mr. Madon.

And Mr. Bejtlich, you are now recognized for 5 minutes for your opening statement.

STATEMENT OF RICHARD BEJTLICH, CHIEF SECURITY STRATEGIST, FIREEYE, INC.

Mr. BEJTLICH. Chairman Duffy, Ranking Member Green, and members of the subcommittee, thank you for the opportunity to testify.

My employer, FireEye, provides software to stop digital intruders; we have 3,400 customers in 67 countries, including half of the Fortune 500. In 2014, our Mandiant consulting service conducted hundreds of investigations in 13 countries. So my testimony today is based on not only my experience doing our own work, but also on the experience of our company doing these investigations.

The title of this hearing includes the phrase "cyber threat," and it is important to understand the threat, but we also need to expand that to include the concept of risk. We need to think in terms of threats, vulnerabilities, and consequences. Risk is a function of these three factors, and if we influence any one, our overall level of security will change, as well.

Furthermore, while risk is a forward-looking concept, where we worry about what could happen, some scenarios have already occurred, making that theoretical risk an actualized event.

I separate damaging scenarios into two buckets, chronic and acute. Chronic scenarios occur over an extended period, with impacts spread across time in ways that can be difficult to measure. Acute scenarios, on the other hand, involve immediate and distinct impact, usually with obvious physical or virtual damage. Thankfully, we have not yet seen a combination of those two, meaning long-term, highly-visible costly damage. And 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 United States is also susceptible to two acute damage scenarios. First, many of us worry about attacks against critical infrastructure. The electrical grid, financial sector, water supply, and telecommunications systems are the big four targets. To date, according to public testimony and public news reporting, some foreign actors have already infiltrated elements of critical infrastructure, while others have attempted to disrupt critical infrastructure.

The second acute damage scenario involves disruption or destruction of virtual infrastructure. And we have two public examples where foreign actors have infiltrated American companies and destroyed data on thousands of computers.

I would like to talk briefly about the four big threat actors, and without probably any surprise, they will be the same ones mentioned by my colleagues. We worry about nation-states, organized criminals, terrorists, and activists.

There is some overlap and mixing of these groups, but if we are able to handle the top end, the nation-states, our abilities will sort of flow down and cover the others, so I would like to talk briefly about the four big nation-state actors: Russia; China; North Korea; and Iran. And I will mention that just in the last year-and-a-half

alone, Mandiant has responded to intrusions by all four countries, including the big public ones I am sure you are aware of.

Russia poses acute and chronic challenges. Russian government forces can conduct full-spectrum information operations, and they possess top tier cyber capabilities, including the ability to preserve their operational security and frustrate forensic analysis.

China also poses chronic and acute challenges. They can conduct full-spectrum information operations, although not at the Russian level. Unfortunately, what they lack in their top-tier capability, they make up for in volume and persistence. For example, the Chinese theft of commercial and sensitive data from American companies is unequaled. In my 18 years of doing this work, I have never seen anything like it.

Turning to the other two big threat actors, North Korea and Iran, both of them primarily pose acute challenges—in other words, the ability to conduct a short, sharp attack. We have seen this now with the North Koreans, or at least forces that were under their control, with the attack against Sony Pictures Entertainment in November of 2014.

Iran has a similar capability. In fact, they conducted a virtual destruction action against the Sands Casino in February of 2014. Both of these countries have geopolitical risks associated with them, which makes it perhaps more likely that they would use a cyber attack to compensate for their military deficiencies.

I would like to conclude by mentioning that I hope during the hearing, we can talk about some alternative strategies to deal with these threats, primarily shifting from a strategy, at least in the government, of closing the barn door after the horses have left, to one of actively looking for intruders that are already in the network; and also, hopefully, moving from a situation where if you lose your Social Security number, there is really no way to recover from that, to one where there are business processes that can accommodate the loss of personal data.

Thank you, and I look forward to your questions.

[The prepared statement of Mr. Bejtlich can be found on page 36 of the appendix.]

Chairman DUFFY. Thank you.

The Chair now recognizes himself for 5 minutes of questions. The testimony we heard today is quite sobering. I imagine everyone on the panel and everyone here today has received a letter that has said, "Your personal information has been compromised." I think I have received 4 letters in the last 8 months. The first one I received was quite disturbing. Sadly, we are just getting used to the fact that our information continues to be compromised.

Is anyone's information—is any information safe, whether we are talking about personal information, we are talking about programs in the Federal Government? To the panel—

Mr. CILLUFFO. Richard, do you want to—

Mr. BEJTLICH. Sure, I will take a quick shot at it. Sir, I would argue that history has shown that no data is potentially safe. We are talking—if you are talking at the very end of our capabilities in the government, you have the risk of insiders, like Mr. Snowden or Chelsea Manning. In the private sector, you have nation-state actors going after private companies.

And from my own personal experience, it takes a sustained effort by a private company to simply hold off a nation-state, or at least to detect when they have gotten into your company so you can kick them out quickly.

So it is very difficult to protect information at all.

Mr. CILLUFFO. Mr. Chairman, to build on that, I think we will never be in a position to say we can prevent all attacks. But there are steps we can take to mitigate the consequences and the potential damage by segmenting and segregating certain information in different sorts of networks. And that starts looking inside, understanding your family jewels, understanding what matters most to either, A, a company, or B, a government, or whatever it may be.

But to Richard's point, how many companies, even the biggest in the world, went into business thinking they had to defend themselves against foreign intelligence services? That is precisely what is happening. The current approach is by definition reactive. Every time we get hit, instead of calling the police, we call the locksmith. We are building higher walls, getting bigger locks. At the end of the day that, by definition, is doomed for failure. It is reacting, reacting, reacting. We have to push the equation in a different kind of way. I am happy to touch on some thoughts during Q&A.

Chairman DUFFY. I think that goes to Mr. Madon's point, where he was talking about not just being on defense. He was talking about being on offense. And one that we had looked to the Federal Government not just for defense. I don't know if we are doing any offensive measures or not, but is there a role for the private sector, do you think, Mr. Madon, in the offensive play, not just defense?

Mr. MADON. I do, and I think it is very varied. I don't think there is just one approach. I think first it starts, as was mentioned earlier, with information sharing. That is a critical component but that is not the only component. It is how you share information. And part of that information-sharing relationship between the government and the private sector has to start with safe harbor.

I can't tell you how many times I hear folks from the financial sector want to share information with the government but they are concerned about liability. And that liability—I think before true information sharing occurs, that liability needs to be addressed.

Mr. CILLUFFO. Could I build on that? Because, think about it, cyber crime is the only crime I know of where we blame the victim. Every other crime, you blame the perpetrator. In this case, we are blaming the victim.

And I am not disagreeing that companies can and must do more, but at the end of the day they are up against an adversary that is very sophisticated and will require at least the rules of the road. I am not ready for sanctioning companies to necessarily hack back, but there is a whole bit of policy space between hacking back and doing nothing but being reactive and building higher walls.

Proactive forensics collection. This is key. Think about it as a football analogy. You have linebackers. Yes, they are defending against other people trying to score on your system, but they are blitzing the quarterback. There is more we can do in that environment as well, whether it is through technologies.

But most importantly we need to define the rules of the road because right now if companies were to engage in this, they would

be breaking laws, the Computer Fraud and Abuse Act in particular. I think that does require some updating and close examination.

Mr. MADON. And my main point is, let's get the conversation started. Let's really have a robust conversation with our Nation, with ourselves, about what it looks like for the private sector to really track and even disrupt cyber attacks in certain instances to defend their systems.

Yes, sir?

Chairman DUFFY. Go ahead. You can finish this thought.

Mr. MADON. And of course, it would not happen overnight. I think there is no expectation of that. And it would require a defendable attribution regime because as our technology gets increasingly more precise, the ability to attribute the location of these attacks becomes more enhanced.

Chairman DUFFY. Thank you. I have several more questions but my time has expired. The Chair now recognizes Mr. Cleaver for 5 minutes.

Mr. CLEAVER. Thank you, Mr. Chairman. All three of you made profound statements with which I agree, and I thank you for being here. Does the United States engage in hacking into systems around the world?

Mr. BEJTLICH. Well, sir, it depends on what you mean by hacking. It has been reported in the press, I think as you would expect, that there are traditional intelligence operations the U.S. Government conducts, as every other country does. The significant difference, though, for the United States is that we don't steal commercial secrets and then give them to our domestic companies for the purposes of commercial advantage.

Mr. CLEAVER. The reason I asked the question, is I am following up on something that was said earlier, and that is, when we discover that a nation is in fact hacking into commercial operations or into the Pentagon, which I think has been done a couple of times, I am just wondering about the response, in a way that is more than saying, "We know you did it," which is what I think we have said recently.

That wouldn't stop me from robbing a 7-Eleven, if I were a 7-Eleven robber, for somebody to say, "Well, Cleaver, I know you did it."

Mr. MADON. Sir, I think that is precisely the point. You highlighted the essential problem, which is that it is incredibly ambiguous what exactly we are doing as a nation when our most valuable—our treasures are being stolen from us, left, right, and center. And I think having a transparent, concrete plan to address those issues is sorely needed.

Mr. CILLUFFO. Congressman, if I can build on that just a teeny bit, clearly, we need to penalize the perpetrators and the adversaries from this behavior and change their behaviors. To me, that does require articulating a clear cyber deterrence strategy, to deter, compel, and dissuade. Obviously, that is going to take on different instruments and instrumentalities based on both the perpetrator and the incident itself.

But I feel we do have to be more transparent and be willing to speak about leaning forward. What good is having the doomsday

machine if no one knows you have it? At the end of the day, of course the United States has the capability, but we use it in a very sophisticated and measured, commensurate kind of way.

To Richard's point, a number of these countries are doing it to benefit their companies. That is an unfair playing field and U.S. companies are penalized greatly by the perceived and/or real sins of others and we are getting our shirts cleaned in this case.

So I do feel there is a way, and there are other instruments that can be brought to bear, both proactive, but also sanctions. The Administration recently promulgated an Executive Order that allows for using economic sanctions against cyber perpetrators.

I think it is going to be put to the test really soon. We will see how it plays out in reality, if we can translate those nouns into verbs.

Mr. CLEAVER. Someone hit on this earlier, but is it possible—do we in fact have the technology now, or are we capable of producing the technology that would create a zero-fail system?

Mr. BEJTLICH. Sir, in my experience there is no such thing as a non-hackable system, and I think that is what you mean by zero-fail.

Mr. CLEAVER. Yes. So, go ahead, Mr. Madon?

Mr. MADON. And likewise, there will never be a system or a condition where attribution will be 100 percent. That is also an ideal. But I think it is a matter of weighing risks. And this revolution in attribution where technologies are advancing to the extent where we are very confident that certain attacks originated from a certain state actor, for example, I think that we are getting to a place where we can be comfortable with the amount of risk that we are taking on.

Mr. CLEAVER. After North Korea hacked into our system, Kim publicly said that didn't happen, we didn't do it. And so I was hoping on the next day we could produce something, some indisputable evidence that yes, you did it, and here is how we know you did it. Does that exist?

Mr. MADON. That is the Treasury model, sir. That is precisely what we did with illicit finance. We confronted those nation-state actors with declassified intelligence and said, yes, you did.

Mr. CILLUFFO. Can I build on that, because I am going to throw a compliment in Richard's direction. Mandiant, in their report on China and their activity, that was the smoking keyboard. Very difficult to discern, but they did demonstrate smoking keyboards. You are starting to see attribution improve dramatically. Never to 100 percent. The smart actors are using proxies. They want the veneer of plausible deniability if they get their hands caught in the cookie jar.

But there are other means than simply cyber forensics to get information on who is doing what, so we have other intelligence capabilities that can be brought to bear.

Mr. CLEAVER. Thank you.

Chairman DUFFY. The gentleman's time has expired. A smoking keyboard, that is quite an analogy.

The Chair now recognizes the gentleman from Pennsylvania, Mr. Fitzpatrick, the vice chairman of this subcommittee, and the chair-

man of the Task Force to Investigate Terrorism Financing, for 5 minutes.

Mr. FITZPATRICK. I thank the chairman. Mr. Cilluffo, the four nation-states that you mentioned in your opening statement—Russia, China, Iran, and North Korea—it seems like every time you talk about nation-states and cyber terrorism, those are the four nations that sort of roll off your tongue.

I was wondering if you can discuss how each of those nations decide or select the subject of the attack and how it may differentiate between the four of them?

Mr. CILLUFFO. Excellent question, and not an easy answer because it is going to come in various sizes and forms. In China, we heard, and I think Richard said, it is a numbers game. They have so many bodies they can throw at the problem that they are quite sophisticated, deeply involved in not only military application and cyber capability but obviously in economic and industrial espionage.

Russia, I think, is the more sophisticated actor of those two. They are integrating cyber into not only their war fighting but into their intelligence apparatus, which often includes human intelligence, according to the U.S. National Counterintelligence directorate of a couple of years ago. They lean so heavily on—and it is worth touching on proxies.

So in China, we know military officers are moonlighting. After work hours, they are doing business for others. In Russia, what you have is more a criminal underground, that they turn a blind eye, but when the government wants them, they do their bidding. Which is maybe very different than Iran, for example, which is turning to its hacking underground, the Ashiyane network, the Basij. They are actually co-opting them into the fold, their activity, which is very different.

So when the stakes are really high, the country that—and it is worth noting—so computer network exploiter, espionage, computer network attack is using attack mode. If you can exploit, you can attack. And there has been article after article after article on countries that have done the cyber equivalent intelligence preparation of the battlefield of, say, our electric grid. That has no economic value but it has significant value in a national security kind of setting. So I am concerned that if the intent shifts, the capability goes up exponentially.

Now Iran, North Korea, they are less constrained perhaps by some of this activity, so they are going to be going to the cyber drive-by shooting equivalent, which is easily built because the bar is low, and also a more sophisticated capability.

And it is worth noting, these are the countries we talk about. Every country that has a modern military has a cyber capability as well, so it is worth noting that.

Mr. FITZPATRICK. Is it possible to know really whether the attack is coming from the state sponsor or from just a group of private hackers, say within Russia?

Mr. CILLUFFO. That is the $64,000 question. So the 2007 attacks on Estonia, was that driven by the Kremlin? I think the messaging was driven by the Kremlin but I think in this case you actually had

criminal actors engage in that activity. So that is where some of this forensics collection becomes so important.

Mr. FITZPATRICK. Did you have an opinion as to the number of prosecutions or actions brought by the Administration in response to cyber attacks?

Mr. CILLUFFO. Not nearly enough. Right now, we are penalizing the victim. So I actually think that in Russia's case, you have a small number of actors who are responsible for developing most of the tools that are being used in the underground, or the malware, or the botnets that are being rented.

If we could go after—I recently had the head of EUROPOL in and he said 80 percent of their attacks were coming from Russian-speaking countries. He had claimed there are about 150 super-hackers. Maybe instead of spending billions of dollars on our cyber security, we should aggressively pursue those 150 hackers.

Mr. FITZPATRICK. Mr. Madon, on the subject of financial institutions, clearly, there is a public role in coordinating response and defenses, and a purely private role as well. But within the financial institutions, we have to encourage the institutions to be communicating with each other, to support each other.

But also within individual institutions, is there a challenge of divisions of certain, say, banks or related banks in different countries, even within those institutions talking to each other?

Mr. MADON. Of course that is the case, sir. But I think that the decision by many global financial institutions to create these financial intelligence units that cross the different verticals within the bank is a terrific effort. And I am seeing more and more of those units being created and being empowered and properly funded.

Mr. FITZPATRICK. My time has expired.

Chairman DUFFY. The gentleman yields back. The Chair now recognizes the gentlelady from Ohio, Mrs. Beatty, for 5 minutes.

Mrs. BEATTY. Thank you, Mr. Chairman, and Ranking Member Green. And thank you to our expert witnesses here today. I am not sure how I feel. I guess I wanted you to be able to answer Congressman Duffy's question by saying, yes, that some of our information is protected and safe and we could work through this and come up with a fail-safe system. But that does not appear to be the case.

As I recall, in February James Clapper, the Director of National Intelligence, testified before the Senate Armed Services Committee, and in that testimony, he stated that in the future we might see more cyber operations that will change or manipulate electronic information in order to compromise its integrity—that is, its accuracy and reliability—instead of deleting or disrupting access to it.

And obviously as members of the subcommittee who oversee the financial regulators, part of our role is to ensure the integrity of financial information.

So I would like to know whether the panel agrees with Director Clapper's assessment of future cyber operations to manipulate data, and if you do, what can our financial institutions and regulators do to combat such attacks to ensure the prevention of manipulation of financial data?

Mr. BEJTLICH. Yes, ma'am, I agree with that assessment. The manipulation of data such that there is an effect, but no one really understands what happened. That is the top end of the problem.

The way to counter that, and honestly, the way to counter all of these problems, in my opinion, is to have a strategy that relies on detecting the infiltration before the adversary completes the mission.

In other words, we currently have delays of upwards of 200 days or so between when an intruder gets into a network and someone notices. And the someone noticing, two-thirds of the time, is the FBI. That needs to change. We need to have a much tighter window so that when an intruder gets into the network, someone notices quickly and cuts them off before their accomplish their mission.

So although we can't stop everyone from getting to the data, if we can stop them before they change it, steal it, or destroy it, then we win.

Mr. MADON. I also agree with General Clapper on that. I would say there is another half of that equation, which is actually more disturbing. I mentioned this briefly, and that is the insider threat. So an insider threat can be a malicious employee who started in an organization feeling great about the financial institution, and then somewhere along the line became disgruntled. It could be a compromised system, or it could be a very sloppy employee.

I think focusing these efforts also on the insider threat, and understanding your employee—financial institutions are becoming and have—are experts at knowing their customer. They are required to do that. I think it is time to also expand that to include knowing your employees.

Mrs. BEATTY. Okay.

Mr. CILLUFFO. Sadly, I too agree. We have actually seen it based in recent public cases as well that the data has been manipulated. But I think in terms of your oversight responsibilities, if I may be so presumptuous, what makes this committee so significant is a sustained campaign against our banks, markets, clearinghouses or other areas is the potential to erode trust and confidence in our very systems themselves.

It is all about perception, and that is with markets, and that can include data manipulation. But there are backups. There are ways where you can stave off the bleeding, and I think both of the other witnesses said there is a lot more we can do in terms of detection.

And I might note, of all the sectors of our critical infrastructures, yours is so much further along than others. I am actually worried about regional banks more than I am Wall Street. It is Main Street. It is all the regional banks and financial institutions outside of Wall Street that are going to be the primary targets.

Mrs. BEATTY. Okay, thank you. In my few seconds left, two of you testified that with corporations being at the tip of the spear in the question which related to public and private partnerships.

What are the tools needed in the private sector, and if we start with regional banks, what are the tools they need to be in the game, to help themselves and us with them?

Mr. CILLUFFO. The financial services sector has what is called the Financial Services Information Sharing and Analysis Center, the FSISAC. It is the gold standard of information sharing and analysis centers. They have even gone so far as having automated

information sharing in terms of known signatures and I.P. addresses through an entity called Soltra.

So I think that we need to expand that beyond some of the bigger financial institutions to others, but there is a model to turn to and it is one that is actually working.

Chairman DUFFY. The gentlelady yields back. The Chair now recognizes the gentlelady from Missouri, Mrs. Wagner, for 5 minutes.

Mrs. WAGNER. Thank you, Mr. Chairman, and I thank our panelists for being with us here today. As we have all discussed, cyber security is quickly becoming one of the largest threats to our country and carries severe national and economic security concerns. The studies have shown the number of security incidents in the United States every day range in the hundreds of thousands, and we seem to learn of a new major cyber breach almost every week.

Earlier this year, millions of customers with health insurer Anthem had their personal information compromised, and just recently, as we have discussed over and over again and we will be in briefings later on today, the Office of Personnel Management announced that millions of confidential records on current and former Federal Government employees have been compromised.

Not only does this represent a major threat and breach of privacy for the individuals whose information is compromised, but it hampers our ability to gather intelligence abroad, and empowers and emboldens foreign governments, many of whom are behind these attacks.

In both of these instances that I mentioned before, we know the attacks are attributed to China, to their cyber unit that engineered the attack. However, what we don't know is, how is our government responding and helping to prevent attacks like this in the future?

You all have talked about a number of risk factors out there and things that are being done, but clearly current actions by the United States to address specifically Chinese and Russian cyber space capabilities is not sufficient. And I never, ever like it when the U.S. Government is in a reactive mode. Nor do I like to hear that it takes upward of 200 days to notice an intruder.

As some of you talked about building, we just seem to be reacting, building that firewall higher and higher, yet wow. Why is it taking upwards of 200 days for us to notice, recognize an intruder? Would anyone like to respond to that?

Mr. MADON. Sure, I couldn't agree with you more, ma'am. There are certain things we can do. One is, as I mentioned, enhancing Section 314(b) of the USA Patriot Act, which will allow financial institutions to share information about cyber-related financial activity within their sector without liability. So enhancing those safe harbor provisions is absolutely critical to that.

Mrs. WAGNER. Mr. Madon, let me interrupt. I believe the House has moved on that through CISPA, and on a voluntary basis, as agreed for that kind of sharing, both within industry and in the government, if they voluntarily choose to. Is that correct?

Mr. MADON. Yes. So I think the safe harbor, not just trends of cyber information but specific, pointed information that banks can share with each other.

Mrs. WAGNER. Right.

Mr. MADON. So expanding it not just between the private institutions and the government, but also within and among financial institutions.

Mrs. WAGNER. Without liability.

Mr. MADON. So what I am saying is, start the conversation, figure out a way to enable that, because if there isn't a conversation and sort of a template that banks and financial sector institutions can use, then the information simply isn't going to flow.

So I am not saying it is easy, ma'am, and it would take quite a bit of thought, but I think that if the conversation begins in bringing in the private sector to come up with creative solutions, there is a possibility.

Mrs. WAGNER. I think you are right. Let me ask you also, Mr. Madon, while I am at it, are there currently adequate international frameworks in place governing nation-states' use of cyber attack?

Mr. MADON. In short, no. I don't think there are. But I think what we can do is again look at the Treasury model and look at the financial action task force as a model, which is an international body which sets international standards and norms on anti-money-laundering, accounting, the financing of terrorism and proliferation financing.

We can use that FADV model in a cyber context as a way of bringing the nation-states to work in a FADV-type body and assess implementation and effectiveness of international norms and standards.

Mr. CILLUFFO. Can I add just very briefly?

Mrs. WAGNER. Yes.

Mr. CILLUFFO. There are some initiatives out there. The Council of Europe, for example has a cyber crime convention which I think is at least a starting point in terms of inducing changes in behavior.

But I think the bigger issue here is we do need to articulate a clear deterrence strategy, and we don't deter cyber. We deter actors, so it will have to have a deterrence strategy that is focused on all the different perpetrators and actors and what the commensurate penalties and response will be.

So I think there is an awful lot that needs to be done, and I think we actually need new cyber alliances. Let's start with our five-eyes community—the U.S., the U.K., Canada, New Zealand, and Australia—and build that out to our transatlantic partners in Europe, then start building out, building that out to allies in Asia, Japan, Korea, in the Middle East, Israel, and on it goes. We haven't really had those conversations in a significant kind of way.

Mrs. WAGNER. Thank you very, very much.

I apologize for going over, Mr. Chairman. I yield back.

Chairman DUFFY. The gentlelady yields back. The Chair now recognizes the gentleman from California, Mr. Vargas, for 5 minutes.

Mr. VARGAS. Thank you very much, Mr. Chairman. Again, thank you for this discussion. It is interesting today to hear some of the words that came out: smoking keyboards; stop the bleeding; doomsday machine. It almost seems like a 1960s movie in some ways. Hopefully, it has a happy ending.

One of the things that did strike me was that you said we need to have a robust discussion in our country, and I think we are

starting to have that, to be frank. Everyone is afraid of losing their personal information, especially their Social Security number.

And we need to penalize the cyber criminals. That gets tough if they are the top-ranked nations, foreign nations. That is a difficult situation. We need to lean forward. We have the capabilities, the doomsday machine. What doomsday machine? I am not familiar with any doomsday machine.

Mr. Cilluffo, I think you are the one who mentioned we have—what doomsday? What are you talking about?

Mr. CILLUFFO. It was meant to demonstrate that we have offensive capabilities that can be brought to bear as well. And if you don't articulate, and to some extent be transparent about that, perpetrators—

Mr. VARGAS. Let's talk about that, because I think what you meant is maybe disrupt them. In other words, if they are disrupting us, we disrupt them more. Is that what you mean? What do you mean by these capabilities?

One thing is trying to find out who they are, and it sounds like we have the capabilities to do that, to figure out now who are the perpetrators. It seems like we are getting better and better at that. So we find out it is Russia. What do we do?

Mr. CILLUFFO. That is way after-the-fact, though. So to Richard's point, there are steps that can be taken left of boom, or in this case before an actual breach and/or incident occurs. And in terms of some of our capabilities, sometimes all you need to do is demonstrate that and that has a net deterrent effect, or it can dissuade. It can raise the stakes, make the penalties so high that they may decide not to engage in this activity.

So what we are really talking about is inducing changes in behavior. If people feel that they can get away with this and get away with this in a wanton kind of way, you are going to see more and more and more activity. So the point is, how do we shift that equation where you raise the costs.

Mr. BEJTLICH. Sir, if I could just quickly say, this is sort of like an American football game where you have the Patriots versus the Broncos. Tom Brady plays against the Broncos' defense and Peyton Manning plays against the Patriots' defense. We need our Tom Brady going against their Peyton Manning. In other words, our offense disrupting their offense.

Mr. VARGAS. I like the football analogy. I was a linebacker. I like the blitzing linebacker. It is fun to tackle the quarterback. But I guess my question really is, it seems like you could figure out who these guys are, but then how do you punish them? Really honestly, at the end of the day, how do you go and punish them? You have all these companies in China that are stealing our information. How do you at the end of the day punish them other than strict sanctions? How do you do that?

Mr. BEJTLICH. Sir, at the operational level I have seen these guys attacking targets and slowing down and not being able to accomplish their mission because of friction introduced by the defender. If you are an attacker and someone is suddenly attacking your system, kicking you off the target, kicking you off your own system, maybe deleting your system, that raises the cost quite a bit.

And many times we think that these guys are 10 feet tall and bullet-proof. There are guys who are sitting in uniform, 18 years old, following a script, essentially.

Mr. VARGAS. Let me get to one thing I did want to get to before my time runs out, and that is, you did talk about Social Security, that if someone's Social Security number is hacked, there should be some protocols in place or something to be able to put that person back to where he or she was.

Why don't you talk a little bit about that, because I think people are very interested in that.

Mr. BEJTLICH. Yes, sir. So when you steal a credit card and you lose a credit card, there is basically no cost to recover from that. When you lose your Social Security number, when you lose your healthcare records, I don't know how you recover from that. You are looking at unbounded cost.

We need to replace the Social Security number with something that if it is public, it doesn't matter. We need to move to a system where we acknowledge that if the data gets out, there is a way for the customer to recover from that. And right now, when a Social Security number is used as a method of identification and authentication—if you know my Social, you can log into Web sites essentially, and that has to be changed.

Mr. VARGAS. Anyone else want to comment on that? Because I think that is important, something that a little thinking outside the box. Would you like to comment on that, sir?

Mr. MADON. Sir, sorry, on your former point I would say you mentioned sanctions. And I just point to the incredible work that the Executive Branch and Congress did—

Mr. VARGAS. If I could interrupt you for just one second. One of the things that was interesting—I am from California and of course we have great capabilities there. The FBI and the Treasury have been named over and over again as models of doing a good job. Private companies are also, and I think that is important to know because it seems today that we are talking mostly about the good work that the Federal Government has done, but California also—

Mr. CILLUFFO. Mr. Vargas, could I just pick up on that, because I actually think the future is within the private sector, and not only domestically but also in cooperation, concerted efforts with others.

Mr. VARGAS. Thank you. My time has expired. Thank you, Mr. Chairman.

Chairman DUFFY. The gentleman yields back. The Chair now recognizes Mr. Tipton from Colorado for 5 minutes.

Mr. TIPTON. Thank you, Mr. Chairman.

I appreciate you bringing up the Broncos and the Patriots. I am out of Colorado, so, this is very disturbing, obviously, in terms of the real threats that we are going to be facing as a country.

Mr. Cilluffo, you were talking about penalizing the risk victims, and I happen to agree with that. We are going after the banks who didn't—or, even Home Depot, I think that was cited earlier, in terms of testimony, as opposed to the culprits who are perpetrating the crime.

A lot of my concern that I see is when we are looking at the Chinese as an example, we have heard the reports that they have our

plans for the F-35. They were able—not only coming at it from an economic standpoint, but also from a military standpoint as well. And, we are talking about the doomsday machine when we are—staying with the football end of this, its said that the best offense is a good defense.

I understand being proactive, so how do we find that proper balance? As a Nation, shouldn't we be incredibly concerned if they are able to get into our military industrial complex to be able to steal some of our best technology? And, then we move into the financial end of the world, and our bank accounts are going to be exploited, and then we can shut down the electrical grid as well.

How do we get those components together to be able to be on the offense?

Mr. MADON. Sir, that is a great concern, and I actually share the view that the private sector is very much a part of the solution to that.

Some of the reforms that I mentioned earlier are a rewards program for groups to uncover and identify cyber hackers to U.S. courts and authorities; empowering the victims of attacks to sue the perpetrators, and those benefiting directly from cyber infiltrations, just as victims of terrorist attacks can do so today.

And, also, unleashing cyber forensic teams, and private litigants, and plaintiffs' lawyers against those attacking U.S. systems.

Mr. TIPTON. Now, what are we going to do? There is something called sleep malware that can be put into a system to be activated at a later time. When we are identifying some of the threats that are going to be in place against us—if it is just sitting there, and it is late, and it is not doing anything, can we identity that now?

Mr. CILLUFFO. Actually, that is an excellent point, because most breaches today occur vis-a-vis or through vulnerabilities in your supply chain, or third-party vendors. And until you start looking at this issue holistically, that is a legitimate vulnerability we need to be thinking about.

I might also note, though, the defense industrial base, they do have unique pilots, vis-a-vis, information sharing with the public and the private sector with government—along with the financial services sector. I think they are up there, but even they, as we saw, have been successfully hacked—whether it is RSA, you name the entity. They have been hacked to one extent or another.

I am going to take a different approach—I think the economic instruments here could be very valuable and useful. I actually think China, long term, will have enough to lose that they will recognize that there is some change in behavior that they need to consider and think about, unfortunately it is not there now. They are seeing immediately in front of them, why spend billions on R&D if we can just steal it, and spend it on gaining market share.

But, at some point they will have market share that they are really concerned about, but I do think that could level it out a little bit, which is different than actors that want to cause harm. So,—that are driven—and I am not suggesting China doesn't, because they are investing in a military technologies as well, but that is something we need to be thinking about.

Mr. TIPTON. Do we have an issue, as a country, when we are having software, as an example, maybe being written in China?

Coming into our country, and then we start bringing into the component of it, trust your employees—we have technology that we are using in our systems right now that is being written overseas. Is that something that we need to examine?

Mr. BEJTLICH. Yes, sir, it is absolutely a concern, and, in fact, the top end attackers, when they realize they can't get into a target technically using the cyber component, they try to get their nationals hired as programmers in sensitive companies.

Mr. TIPTON. And secure coding, that is something the United States ought to be investing in. If we built planes the way we code for software, none of us would ever fly. So, at the end of the day there are initiatives from a STEM education standpoint that we can be looking at in terms of secure coding and the like.

Mr. MADON. There are companies out there, like my own, which is looking very much at the inside threat which a compromised system would be, so that when that malicious software fires up it is identified within the system. So, there are tools, and techniques out there to identify those problems. It is not foolproof, but they exist, and getting better.

Mr. TIPTON. Thank you, Mr. Chairman. My time has expired, and I yield back.

Chairman DUFFY. The gentleman yields back. The Chair now recognizes the ranking member of the subcommittee, the gentleman from Texas, Mr. Green, for 5 minutes.

Mr. GREEN. Thank you, Mr. Chairman. I thank the witnesses as well, and I greatly appreciate your testimony.

You have spoken of an offensive tactic, or strategy, if you will. And, what you seem to be saying is rather than have a firewall, create a backfire; fire back. Be offensive. Let people know that there are penalties, that there is a price to pay for encroaching upon our technology and our systems, our software.

Now, is there technology currently available such that we can now, without attribution, without the certainty of attribution, attack the source without having actual attribution?

Mr. BEJTLICH. Sir, the U.S. Government has unique attribution capabilities to trace all the way back to the true source of an activity. This is one of the few areas I disagree with my co-panelists in that I don't feel that it is the role of the private sector to be doing hack-back. We can enable attribution, we can help through our own forensic investigations, figure out what is happening.

I would much rather see the private sector engage in finding intruders and removing them quickly, and leave the power of striking back at the adversary as part of the state's monopoly of force.

Mr. GREEN. Yes, if we had this unique ability to strike back at the point of origin, what is it that causes us to hesitate, if indeed we are hesitating?

Mr. CILLUFFO. Congressman, first, for the record, I don't advocate hacking back. I think there is a lot that can be done in terms of proactive forensics collection, but, one thing—and you used fireback, I look at it more as suppressive fire so you are protecting your systems. The challenge with some of the technology—

Mr. GREEN. Excuse me, if I may, I really am not talking about suppressive fire. I appreciate your—

Mr. CILLUFFO. No, I was saying—

Mr. GREEN. —I understand, but what I would like to know is what can we do to the hacker that is actually attacking our system. Why can we not? If we know that the point of origin is a certain place, why can't we go to that place and take offensive action as opposed to continuing to be on the defense?

Mr. MADON. Sir, at a minimum, we can remove them from the formal financial sector. We can—

Mr. GREEN. —No, no, no, I am not—I am talking about attacking that system. What is it that prevents us as a part of our counter measures, our defense becomes an offense of attacking that system that is attacking us?

Mr. CILLUFFO. Friendly fire?

Mr. GREEN. I don't—

Mr. CILLUFFO. —because there could be innocents along—in other words, exploiting other systems that you would be taking down, and god forbid, one manages a hospital in Pyongyang—

Mr. GREEN. —I see, but—

Mr. CILLUFFO. —or whatever it may be.

Mr. GREEN. Well, I needed to hear that.

Mr. BEJTLICH. Sir, I think there is also a gain-loss in the intel community which says they would much rather watch the fireworks then let the adversary know that they see the fireworks by interfering with their system. So, there might be some resistance that has to be overcome.

Mr. GREEN. All right, let's talk about credit cards for just a moment. It is my understanding that you can go online and buy credit card information. I am interested in seeing this actually happen—seeing a demonstration of this kind of activity. I understand that if you are sophisticated enough, you are supposed to be able to do this, and people are actually buying credit card numbers, and they are buying social security cards.

Is there any place available to members, or more specifically to me so that I can get a demonstration of how this actually works?

Mr. BEJTLICH. Sir, there are companies out there that investigate this sort of behavior. It is not something we do at FireEye. You may actually be able to find some banks who will show this because one of the ways they validate they have been hacked is to go out and buy a sample of these credit cards to determine if it came from their system. And by doing so, they initiate a response.

Mr. GREEN. Are these available—is the credit card information available to just anybody? Can anybody go online and find this information and buy the—so that I can steal another person's identity? Actually buy this information? Is it available?

Mr. BEJTLICH. It is available, but you tend to have to be a vetted person who is brought in by another criminal.

Mr. CILLUFFO. It is referred to as the Dark Web, so there is the cyber equivalent of black markets, and it is worth noting that credit card data is now going for cents on the dollar whereas health care records are going for much more because the potential to commit fraud and the likelihood of getting caught is less.

And, also worth noting in particular, they are going after children's health records because they are not checking their credit until they are 18, so you could have 10 years of fraud committed against you.

Mr. GREEN. Are you of the opinion that the penalties for identity theft are sufficient? Do we have sufficient mandatory penalties, do we need stiffer penalties for identity theft?

Mr. BEJTLICH. Sir, I think the penalties probably are harsh enough. We just had a prosecution of someone who ran something called the "Silk Road," and he essentially got life in prison for running an underground site.

Chairman DUFFY. The gentleman yields back. The Chair now recognizes the gentleman from Maine, Mr. Poliquin, for 5 minutes.

Mr. POLIQUIN. Thank you very much, Mr. Chairman. I appreciate it, and I thank all of you gentleman for being here today.

This is a very sobering exercise for a lot of us who are not experts in the area that you folks are in. We have to—as a country, I believe, stay on offense when it comes to a lot of these issues, and Congresswoman Wagner commented on that a little bit. And, what I have heard today where you have not only terrorist organizations, and you have organized crime, but you also have sovereign states.

You have countries that are supporting cyber attacks against our infrastructure, our health insurance companies, our cell phone companies, military installations, and this is, as we all know, very serious stuff. It threatens our way of life, our economy, jobs, and when our economy can't function because of these sort of threats then we can't generate the tax revenues that we need to defend ourselves.

This is really serious stuff, and there is a big cost to this, and I understand that. I don't understand all the specifics, but I understand there is a huge cost to our country in doing this. So, in anything in life, any organization you need to have leadership. If you have leadership and you marshal the resources of a country like ours to address a problem, I am certain we can do that, and it sounds like we are not doing that, and we are not staying on offense in a coordinated way as much as we can be.

So, my question to you, and I will start with each of you, whomever would like to go first, Mr. Cilluffo—am I pronouncing it right?

If you were the President of the United States, and you controlled one third of our government, and you were the Commander in Chief, what would be the one thing that you would do to fix this problem?

Mr. CILLUFFO. A great question. I wish there was one silver bullet I could turn to address this, but, by and large, I would look at owning the interagency piece. Do all that we can to enhance not only our own cybersecurity, but also demonstrate our capability. Articulate a deterrent strategy, articulate the penalties, follow through. There are a lot of nouns, not a whole lot of verbs. We have to follow through. These bright lines are being transgressed regularly.

And, more importantly, I would find ways to build on the private sector's capability—

Mr. POLIQUIN. Okay. Let's drill down a little bit more, if I may, Mr. Cilluffo. We are not the only country that has this problem. We know who the bad actors are, right? Russia, China, North Korea, and Iran when it comes to state sponsoring of these cyber attacks. So, other developed nations across the world have these same problems. A lot of our friends in Europe, for example, and the Pacific Rim.

So, my question is, wouldn't part of this activity to stay on offense as a country, to protect our homeland, protect our economy and way of life, and our freedom include coordination with other—

Mr. CILLUFFO. Unequivocally.

Mr. POLIQUIN. With other people around the world?

Mr. CILLUFFO. Unequivocally.

Mr. POLIQUIN. And that can be done, correct?

Mr. CILLUFFO. It can, and it has not—

Mr. POLIQUIN. —and it has not been done, correct?

Mr. CILLUFFO. Not to the extent it needs to be done.

Mr. POLIQUIN. Mr. Madon, what do you think? If you were the President of the United States and you had all these resources at your disposal, what would you do?

Mr. MADON. I would call a meeting together with my staff and say, "What authorities do I have to hit them back, hit them back hard, and do it publicly? Very publicly?"

Mr. POLIQUIN. And, that would include, clearly—because you mentioned this before, dealing with international law, or the development thereof, to make sure that those that are responsible for this are held accountable because in many cases, it seems to me, that we probably have the resources to find out who these people are.

We certainly know who the countries are, correct?

Mr. MADON. Absolutely, sir.

Mr. POLIQUIN. Mr. Bejtlich?

Mr. BEJTLICH. Sir, I would first accept that the government is compromised. We need to go out there and find these guys now. We have to do that.

Mr. POLIQUIN. When you say the government is compromised, do you mean in a case like China, or Russia? Is that what you mean?

Mr. BEJTLICH. There are intruders in the network. We need to go out there, find them, and kick them out. That will be the first message we send, is that we see you, and we are doing something about it.

Mr. POLIQUIN. And we have the resources to do that, in your opinion?

Mr. BEJTLICH. I don't know, sir, if we have the resources necessary.

Mr. POLIQUIN. Do we need to do anything here, anything in Congress? Do you have the legislative support that you need, or anything else that we can do in Congress to make sure that we have an opportunity to stay on offense with respect to this?

Mr. BEJTLICH. I think a reinterpretation of the FISMA law that focuses more attention on detecting and responding to intruders, and less on building up the walls might be necessary.

Mr. POLIQUIN. Okay. Great. Anything else from any of you?

I appreciate very much you being here to help educate us. Keep this country on offense to stop this. Mr. Chairman, I yield back.

Thank you very much.

Chairman DUFFY. The gentleman yields back. Without objection, members of the full Financial Services Committee, who are not members of the subcommittee, may participate in today's hearing for the purposes of making an opening statement, and asking ques-

tions. We do have Mr. Royce from the full committee. Mr. Royce is also chairman of the House Foreign Affairs Committee.

Mr. Royce, you are recognized for 5 minutes.

Mr. ROYCE. First, let me thank Chairman Duffy, because we are looking at the same issue in the Foreign Affairs Committee. I thought I would pursue a line of questioning here. There are some questions that—they are brief questions, but they are a little complicated. I will start with Mr. Cilluffo and ask him what constitutes an act of war in cyberspace?

Mr. CILLUFFO. I am not sure we have enough time for me to try to explain—

Mr. ROYCE. Oh, try to be succinct.

Mr. CILLUFFO. If it does affect our national and economic security, and it is driven by a nation-state actor, Article 5 could be triggered. For example, in the NATO context, if Russia engaged in a computer network attack against Lithuania, that doesn't have to be a military attack, it can also be on civilian infrastructures.

Mr. ROYCE. So, in terms of our obligations with NATO, you see the possibility here that cyberwar and cyber terrorism, or the actions taken, depending upon the extent of it, could be so interpreted?

Mr. CILLUFFO. Absolutely. I mentioned earlier Five-Eyes, NATO, Transatlantic, and then bilats with Korea, Japan—

Mr. ROYCE. You are listing a lot of treaties here that we are in—it is an interesting question because obviously, in the case of North Korea hacking into the banking system of South Korea, you had that special bureau in North Korea. It gets even more complicated because I think those individuals were doing some training up in Moscow.

I think they were training them, but, as we dig deeper and deeper into this, this is, sort of, the trip-wire that we are discussing here because they were intending to bring down the banking system in South Korea, and, in fact, did quite a job of making it possible for a few days for that to work. I always wondered where they got the expertise in North Korea to do that, but, who in the Administration decides what is an act of cyberwar, or cyber terrorism, or cyber vandalism as the President called that Sony hack—cyber vandalism.

Who makes that decision in terms of differentiating how we designate one of these assaults?

Mr. BEJTLICH. Sir, from what I have seen, it is the President's call.

Mr. ROYCE. And how, if at all, is the Administration responding differently between cyber attacks from inside the United States to those that are generated from outside the border of the United States?

Mr. BEJTLICH. Sir, from the perspective of attacks that are conducted by people in the United States, we generally have the law enforcement capability to find them, apprehend them, and prosecute them—which is a capability that does have some effect here.

Mr. ROYCE. Does this call into question whether the Pentagon should have the capability if this is, as you have indicated, an act of war to a certain point? That we should—once upon a time, Billy Mitchell sort of drove our policy by dropping that test bomb on that

battleship closer than he was supposed to, to make a point that we needed an air force. We needed a new branch of the service, basically, because this was going to be a new form of warfare, and along came Pearl Harbor and proved Billy Mitchell—he may have been court martialed for it, but he was absolutely right.

We needed a separate branch. We needed an air force. Are we in a situation now where because—and let's face it—we have advanced warning on this in terms of what Iran intends and some of the other actors intend, to say nothing of some of the other terrorist organizations that now call themselves a state. They have announced that this is a cheap way for them to carry out war against the infidel, or war against the United States—

Mr. BEJTLICH. Yes sir—

Mr. ROYCE. Are we at that point where we need to consider this in terms of our national security in the same way during World War Two that it dawned on us that we needed a separate branch of the service, the Air Force, in order to handle a new mode of warfare?

Mr. BEJTLICH. Yes, sir, I tend to lean tend towards the creation of a cyber force, and I have some pending research on that topic.

Mr. CILLUFFO. Congressman Royce, if I can build on that, it really is about delineating Title 10 activity within our armed services community.

Right now, I think some of the intelligence activity trumps some of the Title 10 activity. I do think we have to get to the point where we can stand up combatant commands and, at some point, I, at the very least, see cybercom being, firstly, a full combatant command, not part of strategic command. And, also, more in a Title 10 hat than its Title 50 hat coupled with NSA.

Mr. ROYCE. And that leads me to the next question, which is, how far along is Moscow on this? If they are at the point now where they are taking from the North Korean bureau responsible for cyber attacks, taking students into Moscow and teaching them these capabilities—I read this in the paper, I don't have the details on it, but it is pretty obvious that they got the training somewhere.

If they are setting up and using proxies, and have become that aggressive, how far along are they, apparently, in setting up a separate department and giving them this charge—this responsibility, in terms of their offensive capability.

Mr. MADON. Sir, I think it is quite evident from the attacks that we have seen that they, the Chinese, and our adversaries, are quite far along. And, I think that our response needs to be vigorous, and needs to be extremely public—

Mr. ROYCE. We are behind them, in other words. We are not as far along as they are in terms of defense. Thank you very much.

Chairman DUFFY. The gentleman's time has expired. The Chair now recognizes the gentleman from Arkansas, Mr. Hill, for 5 minutes.

Mr. HILL. Thank you, Mr. Chairman. I appreciate the opportunity. Excellent topic. It deals on our committee hearing that we had the other day on cyber security issues. We have—I am working 60 cases in Little Rock of doctors who have had their identity stolen for filing their tax returns this year. So, it is a real-life issue, and certainly in Little Rock, Arkansas.

And, one thing that struck me—we talk a lot around here, and we have our budget priorities, and the Administration has their budget priorities of the flavor of the month, whether it is environment, or something else, and yet, I think one of the biggest risks that we have are the IT systems of our Federal Government.

And we haven't talked much about that today. The IRS, of course, their disclosure—I thought West Virginia was impenetrable, but perhaps not. And, we had the HUD Secretary in last week, and his IT system was probably put in when President Johnson was in office.

So my question is, can you asses for me the risk we have with the data maintenance systems of our domestic agencies? Obviously, OPM will have a classified briefing today on it at 1:00.

Mr. MADON. Sir, I think it is unfortunately very apparent that it is underfunded, it is underresourced, and that there are true institutional challenges with those systems. It is a reminder that our information doesn't necessarily have to be highly classified to be critically important. And, I think it calls for funded, comprehensive review of the risk exposure across the Federal Government.

And, I think what they will find is that they vulnerabilities—there are standard vulnerabilities across the enterprise, but also specific vulnerabilities for each institution. And, I think that the solutions have to be a funded mandate to take care of those risks and vulnerabilities.

There are too often unfunded mandates that give confusing guidance to some of these institutions and departments, and I think a very crystal clear funded mandate to get these IT systems up to par is critical.

Mr. HILL. I agree with that, and I am concerned on both sides of the aisle that there is a lot of—Congress likes to dole out punishment to Executive Branch agencies that are bad actors, of which there are many, and the list is long and painful, but in the IT and data security area, I think that is the wrong place for Congress to withhold critically needed funding, which affects all of our data. So, I think we should be concerned about it.

Mr. Cilluffo, you made a comment about regional and smaller banks. I am a former CEO of a—and active in the regional banking arena. And next to consumer laws and credit quality, I would say IT security is the number one thing banks spend money and time on, both in their capital expenditures budgets, and in their operating budget.

I think if more businesses operated in that manner, we would be a lot better off. So, a second question on the Federal systems, are they spending adequate time in penetration testing of our Federal IT systems? Something we have spent 24 hours a day, and hundreds of thousands of dollars a year on in my business.

Mr. CILLUFFO. First, and I also do think that the financial services sector serves as a model for other sectors of our critical infrastructure, but if you take JPMorgan, spending $250 million, had 1,000 people devoted, they did everything just right, and they still got hit. So, at the end of the day, it is more than just resources.

On the pen-testing side, and I think my colleague said it just right, policy without resources is rhetoric. Most of the systems that we have today are built on weak foundations. In other words, you

can have all the complex security, but if it is built on quicksand, or if a home is built in a flood area, it is still going to get flooded no matter how advanced the system is. So, I do think pen-testing is critical.

But, I also think it has to be more than a check-the-box kind of mentality. So, it shouldn't just be advanced warning. We all know there is going to be a pen-test, there should be no warning pen-tests that can be done in a simulated kind of way that doesn't affect the day to day operations of the organization. So, exercise, exercise, exercise, and exercise yet again is the answer.

Mr. BEJTLICH. And, sir, just quickly, before you do the pen-test, in other words, checking to see if you can get into the front door, you should go in the house and see who is already there.

Mr. HILL. Yes. I yield back.

Chairman DUFFY. The gentleman yields back. If the panel would agree, the ranking member and I would like to do a second round. We have a few more minutes. Thank you. The Chair then yields himself 5 more minutes.

We have a lot of government agencies that collect information. Sometimes these agencies hold on to this information. Is the risk to Americans greater if not just their financial institution or their hospital has information, but the government also collects this information and houses it as well? Is it a double risk to the American citizen?

Is that a yes?

Mr. MADON. Yes. That is as close to a factual statement, absolutely, and I think part of the challenge is it is currently not a thoughtful approach. Right? There is obviously information that should be kept and held, and I think—but it should not be rote. It should be something that is considered, and thoughtful and there should be a true look at what information we are holding, and whether it is important or not.

Mr. BEJTLICH. And, also, sir, a presumption; what happens if this data is stolen.

Chairman DUFFY. I want to hear that—I only have 5 minutes. I want to hit a couple of different issues.

So, I would imagine that terrorist organizations maximize their capabilities against America, and our allies. Whatever capability they have, they will use against us. So, if they have the capability of taking down an electric grid, they probably would. Fair enough.

Since they haven't done that, they probably don't have that kind of capability yet. Is that a fair assumption on my part?

Mr. CILLUFFO. That is fair. The one flipside is they are so dependent for their own tradecraft on some of this that they may at least think about it in a calculated way. But, yes, if they have the capability, they will use it.

Chairman DUFFY. But is it fair to say too that the Chinas and the Russias of the world probably have the capabilities of doing some catastrophic damage to critical infrastructure, if they so choose?

Mr. CILLUFFO. You bet.

Chairman DUFFY. I want to give you all a chance, but I only have 3 minutes left. If we could quickly hear about the dangers of hacking back. I know Mr. Cilluffo, you don't agree with that. I don't

know if Mr. Madon, or Mr. Bejtlich, quickly, do you guys think that is a good idea or a bad idea?

Mr. BEJTLICH. Governments can—government-conducted operations, I am okay with. Private sector, I would not be okay that.

Chairman DUFFY. Mr. Madon, you can be a contrarian if you want.

Mr. MADON. And I am going to be somewhat okay.

Chairman DUFFY. I thought you would be.

Mr. MADON. And that is that I think it is important to start the conversation, and I understand that attribution is an incredibly important part of that conversation, but I think to just discredit the value that the private sector could bring to this fight, without really deep consideration, we do so at our own peril.

Chairman DUFFY. Okay.

Mr. CILLUFFO. And, rules of the road are important here, Mr. Chairman. You need clarity. So, before you do anything, you need to know what is—

Chairman DUFFY. Strict guidelines.

Mr. CILLUFFO. —and what is acceptable behavior.

Chairman DUFFY. So, you get a chance to talk to Congress. I will ask each of you to give me the top two priorities that we should have in this institution to help protect, and to fight back in this game of cyber war. What are two takeaways from each of as a top priority?

Mr. BEJTLICH. Sir, my first priority would be find the guys who are already in the network, and kick them out. And, then secondly, based on what you learn during that exercise, figure out what you have to do in order to find them the next time they get in, and kick them out faster. And then eventually, get your defenses in order so that it is much, much less likely that they can get in the first place.

Chairman DUFFY. And, did you say that we don't have that capability? Or, you are not, because, obviously we would have kicked them out of OPM if we had the technology.

Mr. BEJTLICH. You are right.

Chairman DUFFY. So, you are saying that has to be developed, that has to be a focus?

Mr. BEJTLICH. Right. We need to fund that, sort of, strategy, and also the technology, and bring it in to do that.

Chairman DUFFY. Mr. Madon?

Mr. MADON. One, explore offensive strategies that have worked in the past as a holistic government solution, and take those strategies and use them as a template for the next aggressive cyber campaign. That is one.

Two, truly consider the insider threat, as my colleague was mentioning. That often gets short shrift in the cyber debate. So, that would be highlighted.

Chairman DUFFY. So you are telling us to think outside the box, use all the reasonable tools at our disposal?

Mr. MADON. Yes, sir.

Chairman DUFFY. Mr. Cilluffo?

Mr. CILLUFFO. Firstly, to support the—as my colleague just mentioned, some of our computer network attack capabilities to ensure that we continue to be the most sophisticated actor in this domain.

Provide the ability to articulate what a deterrent strategy is, and then should a perpetrator transgress, be willing to stand up in a unified kind of way to respond commensurately.

And ultimately, ensure that you have some of the members and staff who are technologically savvy and can serve as advisers at all times because policy technology people—and you have great people here, so lean on them.

Chairman DUFFY. I will. Listen, I think this has been fascinating testimony. Talking about our security, I think we might get to this hearing without you having to answer questions about servers in other locations, and that is—anyway.

Ranking Member Green, I yield to you for 5 minutes.

Mr. GREEN. Thank you, Mr. Chairman. If you need additional time.

Mr. Hill, permit me to thank you for indicating that technology is important, and that we should be careful about how we raid some of these funds because I, too, am concerned about that approach. So, I thank you for bringing it up and mentioning the later part which has to do with some of the actions that we take without going through regular order.

Let me ask this of you. I understand the profile of the hacker. I understand that profile, and I am talking now more specifically about identity theft. What I am not sure of is the profile of the person who actually acquires the information in this dark world that we have been talking about, and actually uses it. Is this a person who purchases 1,000 identities and proceeds with that 1,000 trying to do as much mischief as possible, or does the person acquire one identity and work that? What is the profile of the criminal mind in the criminal who does this?

Mr. MADON. Sir, I think using one slice is there is no one profile, and if you take the OPM case, I am pretty confident wearing my former counterintelligence hat that there are some very happy Chinese counterintelligence officers right now who are combing through our information to identify vulnerabilities in U.S. employees and trying to exploit those vulnerabilities for recruitment.

Mr. GREEN. Is it your general consensus that this is a profile that would not simply be a person who would live in the United States? Do we have people who live in our country who acquire this information and use it?

Mr. MADON. There is certainly a criminal element, as well. So, I think each attack is very varied, I don't think there is one flavor. And I think it could either be used for—to sell on, as my colleagues were mentioning, the Dark Web. It could be used by a nation-state to conduct counterintelligence activities, so I think there is a broad range of ways to use this critical information.

Mr. GREEN. I am concerned right now with people in the United States, because you have talked about some of the sanctions that can be imposed, and while litigation is a possibility, when you are talking about litigation in a national or international setting, it can be quite difficult because of treaties and other things that would be necessary.

But, let's talk about people within the United States. Do we find that we have people who are going into this dark place and acquir-

ing this information, and they are using it, and they are right here in the United States? They are among us.

Mr. BEJTLICH. Yes. Yes, sir, that happens, and many times they are prosecuted.

Mr. GREEN. And, what I am trying to—my next question is, do they purchase one identity, or do they purchase a thousand? I am trying to get some sense of where—how this information is actually used. Is it used by a single perpetrator with one identity, or does this perpetrator decide that, "I will just sit here, and I will create 20 different identities, and I will find a way to make money doing it?"

Mr. BEJTLICH. Sir, the cases I have seen typically involve either the bulk collection, the bulk sale, or bulk fraud associated with that date. You tend not to see single actors with a few identities.

Mr. GREEN. Let's go back to—you spoke of rewards, almost as though this would be a bounty. Would you explain how you think that might work—the reward system?

Mr. MADON. It could model something like the qui tam system where you have individuals who notice that there are nefarious activities, for example, the whistleblower program where they bring these activities to law enforcement and they get rewarded for that. And, I think it could be a system that is very similar to that system, where there are rewards provided by Federal, State, and local government for individuals who report cyber crime.

Mr. GREEN. Now, what is the fallacy in this, if you think that there is a fallacy? Someone else. What is the fallacy in providing a reward for a whistleblower, as it where, different type, who brings evidence to the government for prosecution purposes? What is the fallacy in that?

Okay, thanks. I take it that is something that you would all agree is feasible and doable, and something that we should consider.

Mr. BEJTLICH. I will just say that it is the first time I have heard of such a thing, so I don't really have an opinion at this point.

Mr. CILLUFFO. And you would probably want to put bounds around, just like in the conventional world, bounty hunting in general. So, I haven't really thought about this in such a way, but if you go back in our history with piracy, yes, we did have the Letters of Mark, and the U.S. Government enabled and empowered entities to not only get a bounty, but keep the booty, literally, in terms of some of the activity there. They were sanctioned by the government.

Mr. GREEN. If I may quickly, Mr. Chairman, I think that this has been indicated to be a system of providing information, intelligence to the government, not acquiring assets, public or individual—not acquiring assets, but providing information. Is that what you are talking about, sir?

Mr. MADON. That is right, but I don't—I think in the current construct, I think the switch from providing information on cyber attack to information on—putting on the time machine hat, an attack on the open seas—I see very little daylight actually between the two. I think they both cause incredible damage to our country.

Mr. GREEN. Thank you, Mr. Chairman. I owe you 1 minute and 6 seconds.

Chairman DUFFY. The ranking member yields back. The Chair now recognizes the gentleman from Arkansas, Mr. Hill, if you have more questions.

Mr. HILL. Just a theme I would like to wrap up on—I was having dinner the other night, or trying to, and the power went out in the restaurant. And I was drinking my beer—which is off the record, I didn't have a beer; I had a coke.

And they literally asked us to leave the restaurant because the power went out. I said, "Why don't you just take my order, cook the food, and I will pay you cash?"

"Oh, well, we can't do that. We have no way to account for—we have no way to write it down." How pitiful is that? But when you get that societally, and when you think about that in a banking context, we are now so dependent on this interconnected Web, that I do view cybercrime as—for the next generation, the same as a nuclear threat. And, that is not too dramatic, I think, even though we think about the massive loss of life in a nuclear environment. But, the ability to shut down the power grid in a capital market system, or the electrical grid—and the data communication system in a modern economy now is—could be just as horrific.

So, how do we broadcast a system of mutual assured destruction in cyber? How do we begin through treaty work, bilateral work, communication? Instead of keeping it so sub-rosa that we actually say, "Hey, look pal, you try to take down our commercial or national security interest, you are toast."

What is the process there? How do we get there on that?

Mr. CILLUFFO. That is precisely, Congressman, the approach, I think, we do need to take because we can't treat this as a quiet issue alone. We have to—it has to not only have sunlight, but for it to have any semblance of impact and consequence to change behavior, it needs to be publicly articulated. I think that is a deterrent strategy, I think we need to look at all the instrumentalities—military, political, economic, and others that can be brought to bear.

Recognize that cyber related issues are on par with traditional forms of diplomatic issues, and it really is going to come down to signaling and having the wherewithal to follow through on our words, which we haven't had great success in recent on always following through on redlines that we have devised. But, we do need to put mark—we do need to put lines in the silicon and demonstrate when they are crossed, expect a response.

The one issue, I would say, that is a little different, vis-a-vis, nuclear, is that the bar is so low to have a cyber capability, whereas you needed a huge infrastructure both scientifically and economically to have a nuclear capability. In this case—

Mr. HILL. That would make it more disturbing.

Mr. CILLUFFO. I hear you, and the club is so much bigger, but there are, again, as I started out—not all hacks are the same, not all hackers are the same, and there are certain things we can do to delineate those actors that are most brazen in their activity.

Mr. HILL. Any other comments?

Mr. MADON. Sir, I vehemently agree. And, I think, sitting back and saying, over, and over, again, ouch that hurts, and basically

signaling to our adversaries that they can continue to attack us with impunity is unacceptable for our Nation.

And, I think we need to explore all options and come up with a campaign, and a thoughtful approach about how to respond to these attacks.

Mr. HILL. Thank you, panel, and thank you for your service for our country, and I yield back, Mr. Chairman.

Chairman DUFFY. The gentleman yields back. I want to thank the witnesses for their testimony today. I feel just a tad bit safer knowing that you three are on Team USA. Thank you for being here. Thank you for all of your work. And thank you for your testimony.

The Chair notes that some Members may have additional questions for this panel, which they may wish to submit in writing. Without objection, the hearing record will remain open for 5 legislative days for Members to submit written questions to these witnesses and to place their responses in the record. Also, without objection, Members will have 5 legislative days to submit extraneous materials to the Chair for inclusion in the record.

This hearing is adjourned.

[Whereupon, at 11:48 a.m., the hearing was adjourned.]

A P P E N D I X

June 16, 2015

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/

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

Center for Cyber
& Homeland Security
THE GEORGE WASHINGTON UNIVERSITY

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

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

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

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/

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/

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

(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

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

"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

Michael Madon June 16, 2015

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.

SEAN DUFFY
UNITED STATES REPRESENTATIVE
PROUDLY REPRESENTING WISCONSIN'S 7TH DISTRICT

1208 Longworth HOB
Washington, DC 20515
Office: 202-225-3365
http://duffy.house.gov

"A Global Perspective on Cyber Threats"
Mr. Frank J. Cilluffo, Associate Vice President, The George Washington University; Director, Center for Cyber and Homeland Security; co-Director, Cyber Center for National and Economic Security
Mr. Michael Madon, Board of Advisors Member, Center on Sanctions and Illicit Finance, Foundation for Defense of Democracies; Vice-President, Business Development, RedOwl Analytics
Mr. Richard Bejtlich, Chief Security Strategist, FireEye, Inc.
June 16, 2015
Questions for the Record

Questions of Congressman Sean Duffy (WI-07):
(To all witnesses)

1. You list a number of cyber threats to the United States, but wouldn't you agree that cyber crime (stealing personal and financial information) is the most significant?

The greatest specific and immediate risk to the individual citizen is the theft and abuse of his or her personally identifiable information (PII) by criminal organizations.

In terms of acute challenges to the American public, the greatest risk is damage to critical infrastructure such that a loss of power or disruption to the financial system causes significant impact to a substantial segment of the population for a time in excess of one to two weeks.

In terms of chronic challenges to the American public, the greatest risk is the erosion of the competitiveness of American private industry and national defense capabilities, arising from the ongoing theft of American trade secrets and sensitive defense and intelligence data.

2. Are you concerned that if the industry, in conjunction with government leaders, does not take strong action soon against cyber crime that the reputation of the safety of the Internet could be compromised, leading users to fear using it?

I do not expect users will fear using the Internet as a whole. I suspect individual organizations

could lose the trust of their users, however.

3. Do you believe the financial services industry is working together sufficiently to protect every customers' information that is online, not just their own?

I believe the leaders and largest elements of the financial services industry are investing sufficiently in cyber security, but significant risks remain at the level of small and medium sized businesses.

Unfortunately, all financial service industry participants, as well as government offices, insurers, and other organizations, still process sensitive data that lacks "recoverability."

For example, a credit card contains data with a high level of recoverability. If a customer's credit card data is stolen, it is easy and cheap for a consumer to recover.

In contrast, Social Security numbers contain data with a low level of recoverability. If a customer's Social Security number is stolen, it is generally not possible for a consumer to recover.

All organizations processing "low recoverability" data, such as Social Security numbers, should evaluate how they use such data, and whether it could be removed altogether.

At the very least, organizations should not authenticate (i.e., prove the identity of) users by virtue of their knowledge of their Social Security number.

4. Is the industry capable of setting a strong enough standard for protecting security system, or should Congress seek to establish one?

FireEye supports the efforts of the National Institute of Standards and Technology to create and constantly update its Cybersecurity Framework, and we encourage all industries processing sensitive data to integrate the Framework into their security practices.

PayPal

Subcommittee on Oversight and Investigations Committee Hearing:

"A Global Perspective on Cyber Threats"
June 16, 2015

Statement for the Record

PayPal would like to thank Chairman Sean Duffy and Ranking Member Al Green for convening the Subcommittee hearing, "A Global Perspective on Cyber Threats". We also thank the distinguished witnesses for providing their expertise on this important topic.

Last year, PayPal had 162 million active digital wallets and was available in 203 markets around the world. PayPal helps people and businesses accept and make payments in more than 100 different currencies and withdraw money from their PayPal accounts to their bank accounts in 57 different countries. In the last quarter of 2014, PayPal's revenues were $2.16 billion, growing 18% year over year, and PayPal's international business generated $1.1 billion, growing a little less at 17%. As a world leader in the payments industry, we appreciate the opportunity to provide our comments on one of the biggest challenges we face daily: cybersecurity.

Introduction

The world has seen a remarkable transformation in commerce with the advent of Internet based companies. Goods and services are routinely purchased and delivered electronically. This has lead to significant changes in industries like journalism, travel, and banking. Online payments (eBilling and ePayments) cut across all industries and are being used by a significant portion of U.S. households. In fact, the livelihood providing for millions of families oftentimes derives solely on marketplaces like eBay's platform.

Further, a majority of the world's population relies on the Internet, either directly or indirectly, for an ever-increasing set of services. Barring an unforeseen catastrophic failure, it is expected that this trend will continue to gain momentum. What more likely is the perception by Internet users that the Internet is unsafe and therefore unsuitable for everyday use. Should this perception become widespread, crowd psychology could take hold and as with the 2008 world financial crisis, result in a loss of faith in "the system". This is what PayPal is working every day to ensure does not happen.

PayPal believes that cybercrime and other cyber issues are the most significant area that could cause this type of loss of faith in the safety of the Internet. We believe action is needed immediately to counteract this negative trend.

Cybercrime is distinct from other attacks

One of the many challenges to discussing issues in cyberspace is that a number of issues are conflated under the 'cyber' banner. The problems grouped into the term 'cyber' are in fact quite different, and the solutions are likely to be different. Without precision about which issue is being discussed, it is very easy to talk at cross-purposes. PayPal chooses to utilize a particular categorization scheme (largely suggested by Scott Charney[1]), which we believe clearly delineates between distinct issues.

Cybercrime

The most important threat facing PayPal – and we believe the entire payments industry – is cybercrime. Cybercrime is criminal activity, using computers and the Internet to directly or indirectly steal from consumers or businesses. The global scale of the cybercrime problem is not known, although by most estimates it costs businesses and consumers several billion dollars (USD) per year. Even within cybercrime, there are different subcategories, such as theft of intellectual property where the financial costs are indirect (potential loss of sales revenue). However, PayPal believes direct forms of cybercrime, such as taking money directly from bank or credit card accounts and identity theft, are the most pressing problem.

Cybercrime is distinct and different from other malicious activities online such as :

- Cyber-Espionage by individuals, groups, or state actors
- Cyber-Terrorism
- Cyberwarfare

The Scope of Cybercrime

Cybercrime, like other forms of crime, is a multi-faceted and ever-changing problem. and the most prominent/frequent attacks against PayPal and other payment providers are detailed below.

Malware and Phishing Attacks

Today much of the harm that occurs on the Internet is a direct result of malware-compromised end-user computers or phishing. Criminals use both of these techniques either to compromise user accounts, or organize compromised machines into botnets which are responsible for the growth in spam, phishing, and distributed denial of services (DDoS) attacks.

At PayPal, attacks and financial losses can be mainly attributed to either accounts compromised because of phishing and malware or the use of stolen financial instrument such as credit cards.

[1] http://go.microsoft.com/?linkid=9746317

Attack Actors

Though attacks on PayPal by activists have occurred and attacks against other companies have involved presumed state-sponsored attackers, PayPal believes that the majority of the attacks on our customers and systems are attributable to either individual criminals or organized crime groups.

PayPal's Approach to Combating Cybercrime

PayPal has focused its efforts on combating cybercrime in several distinct areas:

- Internal security controls on PayPal's systems to make them resistant to attacks
- Ecosystem Partnerships to improve user and Internet-wide security
- Global Partnership with Law Enforcement

Internal Security Controls

PayPal follows industry standard practices for securing its internal systems against attacks that would compromise the confidentiality, integrity, or availability of its systems. Having a robust set of internal controls is an important line of defense in protecting PayPal and its customers from attacks, breaches of personal information, and loss of customer funds.

Ecosystem Partnerships

Many Internet-scale security challenges such as phishing, authentication, and malware are too large for any company to solve on their own. PayPal has been a leader for many years in developing new collaborative approaches to improving Internet safety and security for our customers and the ecosystem as a whole.

PayPal was one of the founding members of DMARC.org, an organization created to develop new anti-phishing technologies and get them widely deployed by industry. As more than 60% of PayPal's global customers are now protected by DMARC technology which has been widely deployed by a large number of the world's top ISPs and mailbox-providers.

PayPal was also a founding member of the FIDO Alliance, an organization created to develop new technologies that move the world to safer and more secure ways of authentication by eliminating passwords and replacing them with better technologies.

PayPal has also partnered with groups such as the National CyberSecurity Alliance (NCSA) on their Stop-Think-Connect campaign to educate consumers in the US and globally about staying safe online.

Global Partnership with Law Enforcement

PayPal partners with Law Enforcement globally to respond to law enforcement requests for assistance, and to bring cases against criminals who attempt or succeed in stealing from PayPal or our customers.

Congress can help our efforts by fostering an open and fluid system of information sharing, among both industry participants and government officials. PayPal and other members of the financial community should be working together on a daily basis to protect all customers, not just our own, from the cybercriminals that lurk behind computers across the globe. As the online payments industry continues to grow, PayPal will continue to be a leader and staunch ally in the fight against cybercrime.

Thank you again for holding this hearing today, and we look forward to a continued partnership with Committee Members.