S. Hrg. 115–298

CYBER THREATS FACING AMERICA: AN OVERVIEW OF THE CYBERSECURITY THREAT LANDSCAPE

HEARING

BEFORE THE

COMMITTEE ON HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS UNITED STATES SENATE

ONE HUNDRED FIFTEENTH CONGRESS

FIRST SESSION

MAY 10, 2017

Available via the World Wide Web: http://www.fdsys.gov/

Printed for the use of the
Committee on Homeland Security and Governmental Affairs

U.S. GOVERNMENT PUBLISHING OFFICE
27–390 PDF WASHINGTON : 2018

COMMITTEE ON HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS

RON JOHNSON, Wisconsin, *Chairman*

JOHN MCCAIN, Arizona
ROB PORTMAN, Ohio
RAND PAUL, Kentucky
JAMES LANKFORD, Oklahoma
MICHAEL B. ENZI, Wyoming
JOHN HOEVEN, North Dakota
STEVE DAINES, Montana

CLAIRE MCCASKILL, Missouri
THOMAS R. CARPER, Delaware
JON TESTER, Montana
HEIDI HEITKAMP, North Dakota
GARY C. PETERS, Michigan
MAGGIE HASSAN, New Hampshire
KAMALA D. HARRIS, California

CHRISTOPHER R. HIXON, *Staff Director*
GABRIELLE D'ADAMO SINGER, *Chief Counsel*
COLLEEN BERNY, *Professional Staff Member*
MARGARET E. DAUM, *Minority Staff Director*
JULIE KLEIN, *Minority Professional Staff Member*
LAURA W. KILBRIDE, *Chief Clerk*
BONNI DINERSTEIN, *Hearing Clerk*

CONTENTS

WITNESSES

WEDNESDAY, MAY 10, 2017

ALPHABETICAL LIST OF WITNESSES

APPENDIX

CYBER THREATS FACING AMERICA: AN OVERVIEW OF THE CYBERSECURITY THREAT LANDSCAPE

WEDNESDAY, MAY 10, 2017

U.S. SENATE,
COMMITTEE ON HOMELAND SECURITY
AND GOVERNMENTAL AFFAIRS,
Washington, DC.

The Committee met, pursuant to notice, at 10:06 a.m., in room SD–342, Dirksen Senate Office Building, Hon. Ron Johnson, Chairman of the Committee, presiding.

Present: Senators Johnson, Lankford, Daines, McCaskill, Carper, Tester, Heitkamp, Peters, and Hassan.

OPENING STATEMENT OF CHAIRMAN JOHNSON

Chairman JOHNSON. Good morning. This hearing will come to order. I apologize for my tardiness. I thought the vote was actually scheduled for 10.

I want to welcome the witnesses. I want to thank you for your thoughtful testimony. I think this will be an excellent hearing based on reading the testimony.

This Committee has four primary goals: border security, we have held, I think, 23 or 24 hearings on it now; cybersecurity, the subject of this Committee hearing; protecting our critical infrastructure, which has a lot of cybersecurity components to that as well, and combating Islamist terror, any type of extreme violent behavior, also definitely has a cyber component to it as well.

So, this is going to continue to be a focus. I really do appreciate the way we are going to discuss this today. Again, based on the testimony, it is going to be a very good presentation of a variety of views in terms of what we need to do.

What I am hoping to certainly get out of this is what we have gotten out of some earlier hearings. We held a hearing on agents on the front line trying to secure our border and enforce our immigration laws, and out of that hearing, I think, we developed a consensus and a process for trying to give those agencies the authority to fix their personnel issues so they can actually hire the people and treat them with parity.

Last week we had a hearing on the Government Accountability Office (GAO) duplication, and I think we also developed a consensus that we need to take GAO's recommendation to actually produce legislation to force the agencies to actually implement their recommendations.

What I am hoping we get out of this hearing, because I think this is really the crux of what we need to do in government, is we have to figure out how we can employ, engage, utilize the absolute best and brightest minds when it comes to dealing with this enormously difficult, enormously complex issue of how do we protect the Internet, the Internet of Things (IOT), our cyber assets from the relentless and incredibly destructive attacks that are just ongoing virtually every second of the day.

It was General Keith Alexander, the former National Security Agency (NSA) Director, who said that cyber attacks represent the greatest transfer of wealth in history. I have a report here, I guess by the Center for Strategic and International Studies.[1] They did an estimate. Somewhere between $375 and $575 billion per year is what they are estimating is the global economic cost of all these cyber attacks.

Again, this is an important hearing. It is just going to be one in a series as we try and grapple with this. But, again, what I am hoping is we all recognize we have to figure out how to break through the bureaucratic rules, our pay scales, or how do we engage the private sector so we literally do have the best and brightest.

And, by the way, we have some really fabulous patriots who are working at way below what they can make in the marketplace already working in different agencies here addressing this. We just need to make sure we get as many bright minds as possible working on such a difficult issue.

I do ask unanimous consent that my written statement be entered in the record.[2] Without objection, so ordered.

Chairman JOHNSON. And, with that, I will turn it over to Senator McCaskill.

OPENING STATEMENT OF SENATOR MCCASKILL[3]

Senator MCCASKILL. Thank you, Chairman Johnson.

This hearing is an important opportunity for us to focus on the threats we face and to begin talking about how to address our Nation's cybersecurity needs.

We have critical vulnerabilities in cybersecurity, and they impact our Nation and countries around the globe. The Federal Government, States, and the private sector have all experienced cyber breaches with devastating outcomes.

Just last week, a candidate in the French Presidential race had electronic messages and documents from his campaign hacked and posted online in an attack that looks remarkably similar to the attack on the Democratic National Committee (DNC) just prior to the party's summer convention, nominating convention, and prior to the Presidential elections.

The perpetrators of these types of attacks are trying to undermine our democracy by tarnishing particular candidates. In this instance, those attacks were, in fact, carried out by Russia to influence voters and portray our electoral system as flawed.

---

[1] The report referenced by Senator Johnson appears in the Appendix on page 73.
[2] The prepared statement of Senator Johnson appears in the Appendix on page 31.
[3] The prepared statement of Senator McCaskill appears in the Appendix on page 32.

Make no mistake about it: Russia is trying to break the backbone of democracies across the world. We need to figure out how to protect our governments and our institutions and our elections from further cyber attacks, and we need to do it now.

One of the problems we face as a Nation is we do not have all the trained, qualified professionals we need to adequately address these threats. Right now, the demand for cyber professionals is far greater than the supply, both in government and in the private sector.

We are also missing leadership on cybersecurity. Today scores of senior cyber-related positions in agencies throughout the government remain unfilled. We are waiting for nominees to be announced for two of the top cyber-related jobs at the Department of Homeland Security (DHS): Under Secretary at the National Protection and Programs Directorate (NPPD) and Deputy Under Secretary for Cybersecurity and Communications. There are essential cyber-related positions at the Department of Defense (DOD), Judiciary, State, and Commerce that are still awaiting nominations from the White House as well.

Right now, we are needlessly fighting with one hand tied behind our back. I implore the President to fill these positions with qualified nominees as quickly as possible.

Cybersecurity is an area that demands bipartisan solutions. To begin with, we need to ensure our government is properly organized to protect the country against cyber threats. Mr. Chairman, I am pleased that our staffs have begun discussions with our House colleagues on elevating cybersecurity within the Department of Homeland Security. Despite the significant role the Department plays in the Nation's cybersecurity efforts, cyber appears to be a secondary function within DHS. That needs to change, which is why I am excited that our bipartisan and bicameral staffs are discussing legislation that aims to appropriately elevate and operationalize DHS' cyber mission.

Federal efforts alone cannot guarantee cybersecurity. States and the private sector are presenting pioneering solutions to confront serious threats. The private sector owns and operates the majority of the critical infrastructure in this country and serves as our engine of innovation.

I look forward to hearing the testimony from our witnesses from the private sector who spend every day working hard to understand the nature of the threat. I take great pride that the citizens of Missouri have vital roles in defending our country from cyber attacks. Mr. Kevin Keeney is here today, and he is an excellent example of a State tapping into existing resources to amplify its talent pool and protect its infrastructure. He has been integral in developing the Missouri National Guard's cyber architecture, which is playing a key role in training units throughout the country to safeguard their systems. It is probably not a surprise that in his civilian life he is the director of cyber incident response at a Fortune 200 company. He is well aware of the threats we face and has firsthand experience defending against them. The citizen warriors in the National Guard are one important step toward solving the Nation's growing cyber workforce problems, and I am pleased to welcome him.

Mr. Chairman, I also want to bring your attention to an emergency meeting on a troubling development in the investigation of an act of cyber warfare by Russia against our country that will occur at 10:30. I will certainly remain here at the hearing for the testimony, remain to question the witnesses, but I wanted to explain to you why many of my colleagues will be leaving the hearing in order to attend this emergency meeting.

Chairman JOHNSON. I understand. I appreciate it.

It is the tradition of this Committee to swear in witnesses, so if you will all rise and raise your right hand. Do you swear that the testimony you will give before this Committee will be the truth, the whole truth, and nothing but the truth, so help you God?

Mr. GREENE. I do.

Mr. CHABINSKY. I do.

Mr. VALERIANO. I do.

Captain KEENEY. I do.

Chairman JOHNSON. Please be seated.

Our first witness is Jeffrey Greene. Mr. Greene currently serves as senior director of Global Government Affairs and Policy at Symantec Corporation. He is a member of the National Institute of Standards and Technology's (NIST) Internet Security and Privacy Advisory Board (ISPAB), and served as a guest researcher on President Obama's Commission on Enhancing National Cybersecurity. Mr. Greene.

TESTIMONY OF JEFFREY E. GREENE,[1] SENIOR DIRECTOR, GLOBAL GOVERNMENT AFFAIRS AND POLICY, SYMANTEC CORPORATION

Mr. GREENE. Thank you, Chairman. Thank you, Ranking Member McCaskill. I appreciate the opportunity to be here today.

Understanding the current threat environment is essential if we are going to craft good policy and develop good defenses, and I am pleased to see that the Committee is continuing its focus on this issue.

2016 was a year that we saw new levels of cyber attacks. It was a year marked by multi-million dollar virtual bank heists, explosive growth of ransomware, attacks on the power grid in the Ukraine, exposure of over 1.1 billion identities through data breach, and massive denial-of-service attacks launched from compromised Internet of Things devices. And, of course, there was the operation to influence our Presidential election.

But, perhaps the most striking feature of 2016 is that instead of using valuable zero-day and sophisticated malware, attackers increasingly attempted to hide in plain sight. We call this "living off the land," illicitly using legitimate network administration tools and software features.

In 2016, the world of cyber espionage shifted dramatically toward overt activity. In addition to the attacks in the Ukraine and our election, we saw an attack on the World Anti-Doping Agency and destructive, widespread attacks on computers in Saudi Arabia.

Interestingly, this shift coincided with a decline in economic espionage. After the 2015 agreement between the United States and

[1] The prepared statement of Mr. Greene appears in the Appendix on page 34.

China not to conduct economic espionage, detections of malware linked to suspected Chinese groups dropped considerably. Notably, though, we did see some of these groups appear to shift their focus to what were more political targets.

In the financial realm, at least two outfits targeted the Society for Worldwide Interbank Financial Telecommunications (SWIFT) network. In one instance, North Korea-based attack groups stole $81 million from Bangladesh's central bank after stealing their SWIFT credentials. And, they would have made off with more but for a typographical error. It is important to note that SWIFT itself was not compromised. It was the theft of credentials that allowed this theft.

Business email compromise (BEC), scams also skyrocketed. These are also known as "Chief Executive Officer (CEO) fraud" or "whaling," and these scams are a low-tech form of fraud where criminals will send spoofed emails to an organization's financial staff, directing them to make large wire transfers or other fund transfers.

During the first half of 2016, we saw more than 400 businesses targeted every day in these type of scams, and just last week, the Federal Bureau of Investigation (FBI) put out an alert that said that over $5 billion has been lost to this type of scam over the past 4 years.

Ransomware also continued its explosive growth. In 2016, we saw three times as many new malware families as we had in the previous 2 years. And, the average ransom tripled from $294 to $1,077.

2016 was also the first major incident originating from IOT devices. The Mirai botnet was made up of compromised routers, digital video recorders, and security cameras, and it was used to carry out the largest denial-of-service attacks we have ever seen. In October, it took down some of the world's most popular websites and applications. Weak security, particularly in the form of hard-coded and default passwords, made these devices easy pickings for attackers.

There was some good news, though. In December of last year, three Romanian nationals who ran the Bayrob gang were arrested and extradited to the United States and are currently waiting trial. This was the culmination of an 8-year investigation, and we are proud to have assisted throughout that.

Security starts with basic measures such as strong passwords and up-to-date patch management. But, while these steps may stop some older, simpler exploits, they will be little more than a speed bump for even a moderately sophisticated attack and will do little to slow a determined, targeted attacker.

Effective protection requires a modern security suite that is being fully utilized. This includes multifactor authentication, advanced exploit detection and prevention technologies, encryption, and data loss prevention tools. IOT presents its own challenges, and while the tools to secure these devices are available, too often manufacturers are not building them in. The Chairman mentioned earlier that attacks are happening every second. By our statistics, we are seeing our IOT honeypots attacked on average every 2 minutes, and based on what I have seen from some of our competitors

and friends in the security community, that may actually be longer than the average.

For these types of devices, we developed Norton Core, which is a home router specifically designed to secure these devices from attacks.

Good security is not going to happen by accident. It requires planning and continued attention. But, criminals are always evolving. The shifting tactics demonstrate the resourcefulness of the criminals, but they also show that improved defenses and a concerted effort to address vulnerabilities can make a difference. The attacks are evolving and developing new ways to go after us, but that evolution does come at a financial cost to the attacker. So, we need to keep in mind that we need to go after the business model of the attackers, not just the technological.

Thank you again for the opportunity to testify, and I am happy to answer any questions.

Chairman JOHNSON. Thank you, Mr. Greene.

Our next witness is Steven Chabinsky. Mr. Chabinsky currently serves as Global Chair of Data, Privacy, and Cyber Security at White & Case LLP. He formerly served as Deputy Assistant Director of the FBI's Cyber Division and as a senior cyber adviser to the Director of National Intelligence. He was also a member of President Obama's Commission on Enhancing National Cybersecurity. Mr. Chabinsky.

TESTIMONY OF STEVEN R. CHABINSKY,[1] GLOBAL CHAIR OF DATA, PRIVACY, AND CYBER SECURITY, WHITE & CASE LLP

Mr. CHABINSKY. Good morning, Chairman Johnson, Ranking Member McCaskill, and distinguished Members of the Committee. My name is Steven Chabinsky, and it is my privilege to appear before you today to discuss cyber threats facing America.

Let me begin by stating what by now seems clear. The cyber threat is real and growing, as is the risk to our national security, our finances, our energy sector, our automobiles, our biomedical implants, and our health records. These and more all appear to be at growing risk. In short, the problem is getting worse, and we are losing. I believe we are following a failed strategy that can and must be changed. But, before I describe what it would take to solve this problem, let me describe what we are up against.

First, when it comes to organized cyber crime, some groups exhibit a level of skill and logistics that appear to be taken straight from a Hollywood script. Consider the international crime group from a few years ago that hacked into a credit card processor's network. They found the databases containing prepaid debit cards, changed security protocols, increased account balances, eliminated account withdrawal limits, and distributed card numbers to members in 24 countries throughout the world. Within 10 hours, they conducted 36,000 automated teller machine (ATM) transactions and stole $40 million.

Second, Internet attacks are becoming more destructive. In addition to ransomware, one of the more troubling episodes we witnessed recently was the rise of botnets formed out of compromised

[1] The prepared statement of Mr. Chabinsky appears in the Appendix on page 42.

IOT devices. Just last October, we witnessed a distributed denial-of-service attack against a single company that had the domino effect of taking dozens of popular websites offline, all based on hacked IOT devices. A friend of mine told me her grandfather apologizes if he helped bring down the Internet.

Third, we continue to expect the private sector to defend itself against foreign military and intelligence services that want to steal their intellectual property (IP). Just 2 weeks ago, the Department of Homeland Security warned of an emerging, sophisticated campaign, almost certainly foreign State-sponsored, that is targeting a wide range of sectors, including information technology (IT), energy, health care, communications, and manufacturing.

Last, our military dominance is at risk. Countries that could not overpower us with traditional weapons now can reach us through the Internet. During times of conflict or simply as a matter of sabotage, enemies can target our critical infrastructure which is compromised in no small part of antiquated, hard-to-defend control systems.

All of this leads us to observe that things are bad and getting worse. Still, our downward spiral is not inevitable. We can improve our security considerably. But, there is a catch. Doing so will require that we reconsider and change the fundamental nature of our efforts.

Most important, we have to stop thinking that cybersecurity is a problem that users can fix. We are not going to get ourselves out of this mess by having every consumer, every business owner, and every operator of critical infrastructure practice good cyber hygiene, or even by having them adopt the NIST Cybersecurity Framework.

Instead, the burden for cybersecurity must be moved as far away as possible from the end user. That will require a 180-degree shift from what we are doing now.

We must adopt higher-level international solutions that include greater threat deterrence, the design of more secure products and protocols, and a safer Internet ecosystem. Put differently, we must resolve cybersecurity problems primarily at their source rather than at their destination.

By way of analogy, when faced with the Flint, Michigan, water crisis, a Federal State of emergency was declared, and solutions are being put in place to repair and upgrade the city's water system and to replace the pipes. Nobody could imagine opting instead for establishing NIST guidelines that would require every home and every business operating in Flint to purchase their own state-of-the-art water filtration system and to hire the experts needed to continuously monitor and upgrade those systems.

Financially incentivizing the companies that can add security higher up in the Internet stack should be considered a budget priority with perhaps as much as 10 percent of our roughly $600 billion defense budget being set aside for the advancement of higher-level cybersecurity solutions.

We should explore other financial models as well. Is it not odd that we have a Connect America Fund that brings broadband to rural markets, but we do not have a Protect America Fund to bring cybersecurity to the entire Nation.

I have elaborated upon each of these ideas, as well as a number of others, in my written testimony. I would like to thank you again for this opportunity, and I look forward to answering any questions you may have.

Chairman JOHNSON. Thank you, Mr. Chabinsky.

Our next witness is Dr. Brandon Valeriano. Dr. Valeriano is the Donald Bren Chair of Armed Politics at the Marine Corps University and an adjunct fellow at the Niskanen Center. Dr. Valeriano has published numerous books and journals on cybersecurity. He also serves as the area editor for international relations and strategy for the Journal of Cybersecurity. Dr. Valeriano.

TESTIMONY OF BRANDON VALERIANO, PH.D.,[1] DONALD BREN CHAIR OF ARMED POLITICS, MARINE CORPS UNIVERSITY, AND ADJUNCT FELLOW, NISKANEN CENTER

Mr. VALERIANO. Yes, thank you to the Chairman and the Members of the Committee for allowing me to offer this testimony today. I offer an empirical perspective of the macro dynamics of the cybersecurity field. The cyber challenge is neither new nor is it revolutionary. Instead, it is a continuation of international rivalries and grievances, but now also fought in cyberspace at a low level of intensity.

But, understanding active cyber operations in their proper context, which is as methods of coercion, we can seek to understand how the international cyber threat landscape works, what challenges will continue to proliferate, and how to fight back by establishing resiliency in cyberspace. Yet only by understanding the macro picture of the cybersecurity landscape can we articulate policy goals to move forward to meet the challenge. While dangerous, the cyber threat landscape exhibits genuine stability, aided by complexity and restraint which leads to careful action in cyberspace. This relative stability and restraint, however, is often in danger of being upset without maintenance and attention.

The universe of cyber threats is pretty clear. Of course, there are States; then there are non-state actors and proxies; and then there are cyber criminals. Each of these actors has distinct motivations, abilities, and limitations. It makes little analytical sense to lump them together as one unified cyber threat actor.

For States, the cyber strategies are a new way of communicating threats and undertaking aggressive operations. Yet there are no new digital avenues of conflict. We have yet to witness a cyber conflict where the genesis all occurred solely in cyberspace.

Cyber methods are typically used as methods of coercion. States use cyber tools to create leverage against the opposition and change strategic calculations, therefore influencing behavior.

Within coercion, there are three types of cyber operations:

There are cyber disruption operations, which are short-term harassment operations meant to influence the opposition, but at the same time expend minimal effort and require few resources beyond coordination.

Espionage operations are long-term activities meant to manipulate information. The goal is either take, steal, or alter information

[1] The prepared statement of Dr. Valeriano appears in the Appendix on page 58.

the target has in order to alter the bargaining situation between two parties.

Last, we have degrade operations which seek to damage the opposition's ability to maintain control of operations, destroy opposition targets, and sabotage procedures. Degrade operations seek to punch at the heart of the target and escalate costs in order to provoke a change in behavior. But, they also the costliest, most time intensive, and riskiest operations we have seen.

In terms of cyber threat actors, of course, the most prominent is Russia. Yet Russia has demonstrated no great sophistication in cyber operations. As opposed to the media coverage, it is often shocking how low tech their techniques are. However, their evident willingness to conduct political espionage and utilize information warfare tactics is a troubling aspect of Russian behavior.

In many ways, it seems that Russia is trying to remain relevant on the international scene by sending cheap signals when they have few capabilities to challenge the dominant powers conventionally.

It must be remembered that the Russian influence operations have been attempted in Ukraine in 2014, the United States in 2016, and France in 2017, with no discernible effect on actual election outcomes. Each time they have failed and provoked a reaction that both hardens the target but also alerts the next target of the likely incoming attacks.

China, on the other hand, focuses mainly on cyber espionage. China has entered into a cycle of probe, penetration, and retrenchment with the United States. Every few years the United States launches a successful counterespionage operation that either halts China or forces them to reset their efforts. Yet China does maintain the ability to contest international decisions and actions that they feel go against their interests. They have launched cyber actions directed against missiles in South Korea and other actors in the South China Sea.

Finally, we have Iran. Iran is thought to be a serious and sophisticated cyber actor, but evidence suggests the opposite of this conclusion. Past attacks did not meet objectives. They have failed to ever target the United States directly except for financial institutions. And, their attacks are built on past malware. The main danger from Iran though is the high probability that it will use proxy actors to attack Western targets.

Now, thinking about moving forward and restoring resilience. That digital violence is rare between States might suggest that we have gotten this era of cyber conflict wrong.

Moving forward, we need a holistic view of the cyber challenge. It cannot be studied purely as a technical domain, but also we need to include international conflict, the motivations of criminals, which would be sociology, the psychological impact of threats, the ethics of cyber action, legality, the dynamics of coercion in security frameworks, and also now the biological implications of digital connectivity.

The manipulation of information is the most dangerous aspect of cyber conflict, and it introduces a new style of political warfare. But, we should be not be shocked or unprepared to meet this challenge.

The problem is active measures to defend the Nation and go on aggressive attacks are often ineffective and counterproductive. There is very little utility in using cyber operations to compel the opposition to behave as expected or desired because these strategies fail more often than not.

Yet we also must strive not to normalize malicious cyber actions. Being hacked is not the price of running a government in the modern international system. It is a perverse outcome of building a structure and system that has little concern for security.

Now, I know I am running out of time, so let me conclude. In short, the geopolitics matter. Intention and willingness matter in addition to capabilities. What we observe in cyberspace should not be shocking or confusing because cyber conflict is generally an extension of typical international interests.

Thank you.

Chairman JOHNSON. Thank you, Doctor.

Our final witness is Captain Kevin Keeney. He serves as Captain in the Missouri National Guard—thank you for your service—where he leads—is it just "M–O–CYBER?"

Captain KEENEY. MOCYBER, Sir.

Senator MCCASKILL. We call it "ROCK." [Laughter.]

Chairman JOHNSON. An umbrella entity for multiple cyber teams. He is also director of the Cyber Incident Response Team (CIRT) at Monsanto, a sustainable agricultural company. Captain Keeney.

TESTIMONY OF KEVIN KEENEY,[1] CAPTAIN, MISSOURI NATIONAL GUARD, AND DIRECTOR, CYBER INCIDENT RESPONSE TEAM, MONSANTO COMPANY (TESTIFYING IN HIS PERSONAL CAPACITY)

Captain KEENEY. Chairman Johnson, Ranking Member McCaskill, and distinguished Members of the Committee, thank you for inviting me here today. To respect everyone's time, I will keep my opening comments brief. My hope is to leave as much time as possible to answer the Committee's questions in a meaningful way.

The cyber threat landscape is not defined by segmented military, government, and commercial networks. It is all one Internet. As Americans, we are extremely connected and impacted by the Internet and its security every day of our lives. Whether you know it or not, I would like to share two examples that the Committee may or may not be aware of that I hope to demonstrate how our current approach to deal with the cyber threat landscape is not broad enough.

U.S. Transcom provides logistics and projects the U.S. military's power around the world to conduct full-spectrum military operations, to include things like humanitarian relief. These fine men and women must leverage private companies to achieve the mission and, thus, must leave the protective enclaves of the military network to do so. This leaves the military reliant on others for its security.

[1] The prepared statement of Mr. Keeney appears in the Appendix on page 69.

Is it right for these companies to need to defend themselves against nation-state actors and larger entities that have much broader capabilities themselves because they are providing a service to the U.S. Government? This needs to change. The U.S. Government has a role here as well.

Homeland Security might be the answer, but they lack the authorities or capabilities to address a nation-state that might try to conduct espionage on the movement of military personnel and supplies. The active military might be the answer, but they lack authorities on their standing how to fully interact with commercial companies providing logistics to the U.S. military that they are reliant upon to conduct military missions around the world.

My second example is in corporate America. They create amazing intellectual property that solves the problems and fulfills the needs and wants of the global market. In doing so, they operate on the Internet and are exposed to predatory nation-states who wish to steal this intellectual property and profit from it without having to make the large investments in research that are needed to create it.

Senator Johnson, you kind of stole one of my lines here because as General Alexander said in 2012, it is the greatest transfer of wealth in history; the U.S. Government has a role here, too.

The point I am trying to make here to the Committee is that we need a whole-of-nation response to properly deal with this threat landscape that we have been living with for quite some time, much to the delight of our adversaries.

While trying to be brief, which is not easy in these complex topics, I hope these examples serve to demonstrate the seams that exist in our current approach. We have organized ourselves in a way that provides opportunities to criminals, hactivists, nation-states, and generally malicious actors.

In closing, cyber threats facing America are many and cannot effectively be dealt with Committee by Committee. It is my hope that the Senate will work to address the cybersecurity threat landscape as a whole body, combining for the defense of the military, government, and commercial networks, like the Internet works, not how we have organized ourselves.

Thank you for the time today, and I look forward to your questions.

Chairman JOHNSON. Thank you, Captain Keeney.

We are going to turn it over to Senator McCaskill for her questioning first.

Senator MCCASKILL. Thank you so much, Mr. Chairman. I appreciate your consideration.

Let us start, Captain, with telling the Committee about the cyber kits that you have made, and I think that the part that the Chairman and Senator Lankford will be most interested in is that you have done this with zero—count it, zero—additional public money, zero additional Federal dollars. It is very impressive. And, would you explain what these kits are and how you are sharing this across the country with other units?

Captain KEENEY. Absolutely. I would be glad to. It is an honor to serve with the men and women that have created this capability on their own time.

I will tell you it was born out of an exercise in which I first met General Alexander, actually, in 2012. Cyber Guard was the exercise, and we were National Guardsmen responding to critical infrastructure key resources, and we brought our little cyber kit in there, and we jumped in the mud with the adversary. And guess what? We got bruised up, because getting in the network which the adversary has already compromised creates some real problems.

So, we went home, put our thinking caps on, like Guardsmen do, and we tried to figure out a way that we could interact with the adversary in a safe manner or passively, yet identify their attacks. That was born out of an open-source project known as "ROCK," for network security monitoring (NSM). This project has taken off like a rocketship. It is now by my estimation, through talking with various team members, used by 40 different government entities—military, Federal agencies, research entities—and it is also being used in the commercial market.

I think it is pretty successful. As a matter of fact, I am collaborating with some folks from the Wisconsin Guard that I met last week at Cyber Shield for them to start leveraging the capability in their National Guard.

I hope I have answered your question.

Senator MCCASKILL. Well, you have, and I think it is really important that, I think this is one example of where the National Guard does not get all of the love it deserves because you have a very big and important job in an environment at a company that is constantly under attack by not just hactivists but also nation-states. And, we know that if we just look at the F–35 and what China is fielding right now, those similarities are not accidental. They are, in fact, a product of cyber warfare. So, I am really proud of what you all have done.

I think your recommendation is very interesting, and I would like to spend the rest of our time today talking about your recommendation. What you are saying is we should have a new uniform service that is U.S. Cyber that brings everything under, one roof. Why don't you talk about that a moment and talk about why you think it is important to separate U.S. Cyber from the rest of the military and the rest of the civilian workforce.

Captain KEENEY. OK. Pretty complex topic. Obviously, creation of an entire new uniform service is nothing that we are going to solve here today in this room exactly, but I would like to share some thoughts on the problems I have seen.

I do not mean to speak disparagingly, but there is a little bit of rice bowl fighting amongst the services for cyber——

Senator MCCASKILL. Horrible turf wars everywhere, especially on cyber.

Captain KEENEY. Absolutely, because it is the cool new thing and everybody wants a piece of the action.

Senator MCCASKILL. Right.

Captain KEENEY. In particular, I see pretty hard lines drawn between the active duty and the National Guard and Reserve component. I find that very interesting because many of the folks on the active duty that I have the opportunity to train, they are wonderful. But, they are also a lot younger and a lot less experienced than the folks that I have worked with in the National Guard due to

their experience in industry for 10, 15, or 20 years, and they are still wearing the uniform. The things they bring to that cyber fight are rather unique. But, I digress. I am bragging on my boys in the National Guard, obviously.

But, U.S. Cyber I think would enable us to consolidate training, the training that is being repeated across the different services. How about studying how to fight this threat and adversary through university programs that are not looking at it through the lens of the Navy, the Army, or the Air Force, but holistically, how do we fight this as a Nation?

And, I think there are opportunities. If we made a force that was made of active component and Reserve component and leveraged the titles available to each of those components, what I mean by that is, for example, Title 32 and Title 18 authorities that people in uniform, in the National Guard, can partner with law enforcement and with the Governors of their States and interact with that critical infrastructure or just businesses in corporate life.

We are not structured that way today. We look at that as that is a Homeland Security issue, but I would question how much that is actually happening in corporate America and what does that collaboration look like between companies and Homeland Security, even though that is their role, as I understand it.

Senator MCCASKILL. Do you interact with Homeland Security in your role at Monsanto?

Captain KEENEY. I do not. Now, we do interact with the FBI when we have an investigation.

Senator MCCASKILL. Right.

But, there is not an ongoing communication or integration in terms of critical infrastructure?

Captain KEENEY. We do subscribe to some of the government's threat feeds through Homeland Security, but, honestly, I think that the corporate solutions have far surpassed that with companies like Symantec, CrowdStrike, many others. This sharing that we are all talking about, they have an entire ecosystem and a business model built around it that is lightning fast, that shares information across all sectors.

Senator MCCASKILL. So, you are envisioning 50 percent active, 50 percent Reserve, and what about qualifications? I mean, one of the things I learned when I visited your unit—by the way, if you go visit their unit, you do not get a coin. You get a rock, which I thought was very cool. What I learned was that there was somebody who was very talented in the unit that almost was not allowed to continue because of a pull-up requirement.

Captain KEENEY. Yes, he had to meet physical fitness requirements of the Army, yet this soldier in my unit is a multi-millionaire, owns multiple businesses, is extremely successful, and as I joke around with him, he can bend, time and space on a keyboard. And, he is an E5 sergeant, makes—by the way, he travels from another State and probably at the cost to himself. Like many of the members of my unit travel from all over the country to come to Missouri and work on ROCK and innovative projects like that. To think that we would kick him out of the military and not have him as—when we are all talking about the critical shortage of resources and human capital, it just does not make sense. We need to change

how we are approaching the skills gap and how we are recruiting and retaining talent. And, I do not know if we can do that inside the existing military construct.

Senator MCCASKILL. The mental stamina is important, but there is no reason—as you said in your written testimony for this Committee, there is no reason a double amputee could not perform at the highest standard in a unit that was, in fact, dedicated to U.S. Cyber.

Captain KEENEY. Absolutely. And, what purpose it would give that individual to continue to their country in that way.

Senator MCCASKILL. One of the problems we have with this area is that we are trying to approach this like we have approached every other problem. We had a cyber hearing in Armed Services yesterday, and my staff did a chart of the Cyber Command within the military, and then did a chart with NPPD at Homeland, and I got to tell you, it is worse than spaghetti. It is so confusing and so disparate, and there is no wonder that we are having all these turf wars.

So, I think, even though this is a bold idea—and a lot of people around here would just go, "Well, we cannot do that," and there is probably going to be significant pushback from the military—I think this is a really good idea, and I think it is time we think outside the box. And, I appreciate you bringing it to us today.

Captain KEENEY. I think the U.S. Army pushed back pretty hard. They did not want to lose a thing called the U.S. Army Air Corps, and the creation of the U.S. Air Force, thanks to Billy Mitchell, it worked out pretty nicely for us.

Senator MCCASKILL. It sure did, so that is a great example that we need to think boldly and be aggressive here. I do think in the long run it is going to save us resources, too, and up our capability, especially in terms of interaction with the private sector. So, I really thank you, Captain, for being here today.

Captain KEENEY. Thank you, ma'am.

Chairman JOHNSON. Thank you, Senator McCaskill.

We will turn it over to Senator Lankford, but I just want to quick follow up because the question I have in terms of what you do, what threats are you addressing in your exercises? Is it strictly threats against the military? Is it against the homeland? What are you exercising?

Captain KEENEY. So, I would say it depends on which exercise you go to, the focus of that exercise. Cyber Shield is the exercise the National Guard Bureau hosted last week in Utah. It was definitely focused and had a leaning toward protecting critical infrastructure and key resources inside a State and leveraging Title 32 ability for a Governor to say, hey, in a State of emergency, go help these guys, they have not delivered water in a week, or something, and they need help.

Senator MCCASKILL. Or there is no light.

Captain KEENEY. Right, or there is no lights or whatever. So, those scenarios are being built for sure, but there is not a whole lot of personnel, manning, training, funding, all of that, because—and the buildup of the cyber mission force that General Alexander kind of kicked off—I think it is 5,000 to 6,000 personnel—it does not include those elements at all.

Chairman JOHNSON. But, again, your exercise is primarily about critical infrastructure in your States as opposed to exercises in terms of military assets.

Captain Keeney. Absolutely, which is a great step in the right direction.

Chairman JOHNSON. Again, that is really what we are concerned about here in the Committee.

Captain KEENEY. Sure.

Chairman JOHNSON. I will turn it over to Senator Lankford.

OPENING STATEMENT OF SENATOR LANKFORD

Senator LANKFORD. Thank you, Mr. Chairman.

Mr. Greene, let me ask you about the threats and the quantity of threats worldwide at this point. Give me a best guess here, cyber criminals versus State actors versus folks that are just hactivists that are trying to just cause mayhem in a certain area. Give me a percentage of the threat.

Mr. GREENE. Well, it depends upon the sector being attacked. I do not mean to lawyer the answer. One of the other issues you run into is there are not clear lines. A lot of times you will have a nation-state either acting as a so-called hactivist or using hactivists without knowledge. I would say that on the financial fraud, until this year, it was 99 percent criminals. This year was the first year we saw a major nation-state engage in major bank fraud, the North Korea attacks on Bangladesh and elsewhere. So, the pure dollars is probably still low. As I said, the FBI put the BEC scam at $5 billion over 4 years. The Lazarus Group took, I believe, $81 million from Bangladesh.

In cyber espionage, I am purely guessing. A guesstimate, I would say you are looking at the majority of it, if not more, being nation-state, or certainly appearing to come from nation-state regions. The issue there you have sometimes, though, is something could look like a nation-state, but you do not know whether someone is doing it as part of their day job or is taking the skills they learned in their day job and are using it at night and selling it on the black market.

Is there a third component I missed?

Senator LANKFORD. No. That is fine. That gives me a good balance there. How many of those are outside of the United States when we deal with cyber criminals? Obviously, all nation-states are outside the United States. But, the actual individual on the keyboard is outside the United States?

Mr. GREENE. The percentage of—the large criminal groups are typically based outside of the United States. Their infrastructure, though, is global, so you will see a lot of attacks. The actual launch point will come from inside the United States. I believe that still the majority of the launch points come from an actual computer in the United States. But, the major gangs that we see, Bayrob that I mentioned, which was taken down in Romania, there was an Estonian group a few years ago, you see a lot—the overall majority of that activity is not U.S.-based in terms of the top leadership at this point.

Senator LANKFORD. OK. So, let me broaden this out to a broader conversation as well. We have talked for years about having a

cyber doctrine, a clear set of lines and boundaries where the United States would be able to announce worldwide here are the boundaries for what we would accept or what we would not accept, and here are the responses that we would have. That has been discussed but has not been implemented.

So, my question of any of you is: What are the major features of that cyber doctrine that we need to make sure that they are there from your perspective so we can actually work toward getting this implemented? And, as we deal with nation-states and we deal with international actors, what are the pressure points to be able to apply to people, to be able to make sure there is actual enforcement? Anybody can jump in.

Mr. CHABINSKY. I will take a shot at this, Senator Lankford. In my time with the intelligence community (IC), I found that the aspect that was lacking most was what I would refer to as "options analysis," meaning that the intelligence community did then and does now quite well a review of the threat itself and, in fact, even within incidents, the ever-increasing ability to find attribution. And, then, we would write it all up as an incident report and hand it to the President of the United States, essentially saying this is what happened. And, what was clearly missing was, well, what can we do about it? What are the options?

No one in the private sector ever would provide their boss with a copy of a problem without some reasonable basis of what the options are, but the intelligence community to this day is not set up with a group of career intelligence analysts across what I would call the Diplomatic, Information, Military, Economic, and Law Enforcement (DIME/LE) options—all elements of national power as can be provided by the government or the private sector or the government and the private sector working in concert.

So, we do not know what works, and we do not know how that applies to specific criminal groups or specific nation-states. As a result, to answer the question becomes hard because we have not created the intelligence that would allow us to understand what our options are.

Senator LANKFORD. Great, but when I move back to this intelligence, it really provides us information for policymakers to be able to make the decisions. I think my question for you is: Who is helping develop that list of options that you are articulating to say this is the boundary? It is one thing to be able to know where it is coming from. It is another thing to be able to know what is a reasonable, effective deterrent.

Mr. CHABINSKY. So, clearly, when it comes to critical infrastructure, there has been a large series of normative discussions internationally about taking down destructive attacks on the energy grid, on the financial services grid, as these types of boundaries, but less understood on what the boundaries are or what we would do about it. And, I am not aware of groups that are exploring those types of options.

Senator LANKFORD. OK.

Mr. VALERIANO. I think this is the next step. We need to have a comprehensive list of all cyber incidents, and that could be something the DHS or another organization could start. There has been talk, but we have not actually done that, and that is the problem.

We do not have a basis of evidence. We do a lot of speculation, and we cannot make policy based on speculation.

There is only one real line that we need to institute, and that line is violence; that line is destruction. Anything more than that will limit our own ability to respond and act. So, that is a problem with setting up lines in cyberspace. The clear thing is to stop any attack on critical infrastructure—anything that can cause death and destruction, if we have not seen it yet, and hopefully we never will see.

Mr. GREENE. If I could answer, I think one important point, there has been a lot of literature written about could we have cyber norms, and the argument against it frequently is, well, we will not have compliance, how will we know? I think we need to have the conversation going in, understanding that there will not be perfect compliance. It is impossible. President Reagan said, "Trust, but verify," in a different context. We need to understand that we need to do it as best we can. An 80-percent solution would be better than where we are today. So, I think one of the things that has stopped a lot of the conversations is this debate over can we come up with perfect norms, and the answer is no. But, that does not mean we do not try.

Senator LANKFORD. Right. Well, this continues to accelerate, and I know I am running out of time. I will honor that as well. But, this continues to accelerate. I was with one of our universities doing research on cyber activity where they have developed the capability, which many others have—and they are studying the opportunities there—of pulling up next to a vehicle, hacking into their Bluetooth from the vehicle, and taking control of the vehicle. That is something that most Americans do not consider, that there is the possibility that someone could get close to them and be able to do that. But, they are trying to evaluate not only how easily can it be done, how many things can you operate once you are in the system, whether it is a heart monitor that is connected, whether it is the Internet of Things, whether it is operating systems, whether it is a small manufacturer that bought a piece of equipment but then has not upgraded the software in years, and the vulnerabilities are there. We are exceptionally vulnerable in our system. And, I do agree that one of the prime things we have to move is in actual deterrence, that if someone reaches it and uses that, what is the consequence of it? And, that helps provide us the next step of what needs to be done, and I would hope we could work with this Administration to help actually get that close and so that worldwide there is a relationship internationally, if you hack into our systems and if you steal our information or if you destroy systems, here are the boundaries and here is what our response is.

I yield back.

Chairman JOHNSON. Senator Lankford, I will turn it over to Senator Daines. And, I will turn it back to you if you want to stick around. I am here for the duration, anyway. Senator Daines.

OPENING STATEMENT OF SENATOR DAINES

Senator DAINES. Thank you, Mr. Chairman. And, thank you for your testimony today on this critical area of national security.

My observation has been that over several years policymakers have lamented this growing problem, yet there have been few meaningful solutions beyond saddling businesses with more regulations.

Mr. Chabinsky, I appreciate your comment around it is kind of, I think, embedded in the culture of this town, and that is, we will answer the question, "So what?" but not the question, "Now what?" in terms of optionality and action plans.

I spent 12 years in the cloud computing industry before coming to Congress. I do understand how important it is for businesses to guard sensitive data. Our hosting operations were targeted. Our business model was selling to Fortune 500's and large public institutions. I do understand how important it is to guard that data and the responsibility you have to your customers to protect it. Securing sensitive information is an important part of the conversation, but there is more to be done. I do believe that as lawmakers we need to widen our aperture a bit, and I do appreciate being here today and you all being here.

I venture a guess that many here would not dispute that the private sector rapidly outpaces the Federal Government in its ability to adapt and respond to rising trends in cyber crime. In fact, that is why just back in February I introduced the Support for Rapid Innovation Act of 2017, which allows DHS to foster and enable progress rather than impeding it by setting static requirements. This bill would promote deployment of more secure information systems, better detection and discovery of malicious code, faster recovery.

Mr. Keeney, you are the director of a Cyber Incident Response Team for a publicly traded company. Where could you use more help from the Federal Government? And, conversely, where does government interference simply get in the way?

Captain KEENEY. So, speaking from my opinion, I would say that the way the government could help most corporate America is to do the things that corporate America cannot do for itself. So, U.S. law does not allow for corporate America to strike back against an adversary that continues to bloody their nose and do damage to their shareholders, which are likely American citizens.

The U.S. Government, when they do targeted offensive cyber operations, they are generally in response to traditional military operations. But, I do not hear much or see much about offensive operations being done as a counterpoint, as somebody crossed a red line, you are not going to steal intellectual property of a company valued at $1 billion or some number, some threshold; every situation is different. But, the U.S. Government can do those things because U.S. law does not allow those corporations to do it for themselves.

If a tanker ship full of goods sailed out of the port in Delaware and in the middle of the Atlantic got sunk by a nation-state adversary, what would be the response of the U.S. Government? I think it would be pretty clear. We would go after quite quickly whatever nation-state did that. Why is it any different in cyber?

I hope, Senator, I have answered your question on the front half of what I think the government can do. It is mainly the things that we cannot do for ourselves.

Senator DAINES. Yes, I think that is kind of along the line where Senator Lankford was headed here in terms of kind of rules of engagement in defining a doctrine as it relates to cyber. I was an advocate and supported, as we debated last year, elevating cyber to its own combatant command, Cyber Command, to try to focus efforts here and get ahead of this.

I joined our cloud computing company in 2000, a few years after it started up. We grew the company, took it public. It was acquired by a large corporation. But, back then, it was trying to let bankers understand the fact that basically our asset here was IP. You cannot come and count and measure the asset. We always said if our cloud computing company ever went out of business, all that was left was cubicles and some computers. So, it is all in the power of the electrons. That is the power, the IP. And, when you have whether it is a nation-state, some bad actor out there destroy electrons in this case, or code, from a cyber attack, that really is not any different. You used a good analogy there of destroying a physical asset. When you start thinking that way, that is helpful feedback for us here, how we can help the private sector.

Let me shift gears here and talk about another subject: attribution. It concerns me that policy discussions on cyber too often default to mitigation and recovery. If we compare cyber crime with a physical robbery, we are focused entirely on building a bigger, better fence. Physical security around a house or a building works not because the barrier is impenetrable, but because there are consequences for getting caught. We use floodlights for deterrence, cameras to identify criminals. We provide information to the police, and that leads to an arrest. Right now, there are few, I would argue no, consequences for cyber criminals.

Mr. Chabinsky, I refuse to accept that attribution is an unsolvable problem or something that can only exist in the shadows of the intelligence community. Given your experience with the FBI's Cyber Division, how can we hold these hackers accountable?

Mr. CHABINSKY. Senator Daines, let me start by saying when I was growing up, I used to be impressed when I saw that there were Members who were medical doctors, and I am still impressed by that, but I do not know how useful that is for representation. I am far more impressed now when there are Members who have a technical background, and so it is really quite important for our Nation that you are representing us, and I appreciate your service.

If I could agree more than 100 percent, we have completely looked at this topic in a way that would never be acceptable in any other context by going and blaming the victims. Time and again, we see after an intrusion that the CEO is called to testify, even before committees in this institution, of how this could happen and what they are going to do about it. But, what we do not see is the FBI call to ask what are we doing to catch the bad guys and when is this ever going to end.

Attribution is not as large a problem as one might expect when you have attackers who are working over time, whether they are

criminal actors or nation-states, it is actually quite difficult to keep anonymity for any meaningful length of time.

There is this phrase in the security community that the defender has to get it right all the time, but the attacker only has to get it right.

Well, with respect to attribution, as far as the bad guy is concerned, it is just the opposite. You have to have your tradecraft right 100 percent of the time, and losing it just once leads to attribution. And, the headlines will show that we are much more confident with attribution. What we are not confident yet with—and this is what Senator Lankford was saying—is what are we going to do about it. And, that is where the government—again, with Captain Keeney to my left leading the charge, that is where the government needs to come in. We have spent even on the government side tens of billions of dollars on information security to patch systems, billions of dollars, but our funding for law enforcement is perhaps in the millions. The FBI, with over 14,000 special agents, has a few hundred special agents that are involved in this type of investigation and attribution and then penalty.

There is just no doubt that businesses cannot defend against the types of organized criminals and intelligence services we have. Until we realize that it is not the government's role to help the private sector better protect itself by giving them guidelines and giving them information about patches, but to get out there and get rid of the threat, we really are going to see this rise to unsustainable levels.

Senator DAINES. Well, Mr. Chabinsky, you asked if you could agree with me more than 100 percent. I would ask the same of you, actually. [Laughter.]

It is interesting, you have lawmakers who want to run to say how can we better protect the private sector as it relates to technically. There would be a few things there, but generally it is tap it light. Every private sector organization, one of the greatest fears you have is making the front page of the Wall Street Journal because you just compromised the information of your customers. That is built in—that is why in the C-suite now, of course, the Chief Information Officers (CIOs) and Chief Technology Officers (CTOs) are certainly sitting right by the CEO because of the risk and the downside consequences of that kind of a compromise.

But, I think you have provided some guidance and some clarity here around what real help might look like and what the Federal Government's role ought to be focused on, and I thank you for those comments.

Mr. CHABINSKY. Thank you, Senator Daines.

Chairman JOHNSON. Thank you, Senator Daines.

Let me follow up on that thread of questioning, because we are still asking the question: What can you do about it? And, that is fine to set up a cyber force, fund more law enforcement. Once they have the resources, what will they do about it? It is nice to hear that we are better at attributing these things, which is part of the problem, but you have that same problem in kinetic warfare as well, potentially. Who perpetrated this attack?

Once we have attributed it, and let us say there is a state actor, I want to know your suggestion. Here is your chance. What will we do about it? I will start with you, Mr. Chabinsky.

Mr. CHABINSKY. Thank you, Senator Johnson. I think as earlier testimony from Mr. Greene supports, when we decided to make a full effort to address Chinese cyber espionage, economic espionage, it, in fact, was quite successful. But, it took everybody realizing that they had to stop telling people to patch their systems and live with Chinese economic espionage. It became a central focus of Congress as well as the last Administration. At every single high-level meeting with Chinese officials, this topic was addressed, and it ended up resulting in an agreement that, by and large, has been effective for what it was hoping to achieve.

Chairman JOHNSON. You are saying publicly exposing, public pressure, sanctions potentially on the actors, those types of things, is what would be your first line of response?

Mr. CHABINSKY. Every nation-state responds differently to there are different carrots and sticks for different nations. Sometimes you can do things positively. We have also seen on the criminal front enormously successful international takedowns of organized crime groups, but they are too few and far between because they are underfunded.

Chairman JOHNSON. Well, but also protected by rogue regimes as well, right? They are outside the long arm of the law if they are potentially in Russia, potentially in China. What about North Korea? What do you do about North Korea?

Mr. CHABINSKY. To some extent, but I do not need to remind the Senator that we are the United States of America.

Chairman JOHNSON. I understand.

Mr. CHABINSKY. And, if we are going to be here hand-wringing that we have no influence internationally against rogue nation regimes, then we might as well hang it up and call it a day as a country. OK? We have enormous elements of national power. It is time to get serious and create a strategy——

Chairman JOHNSON. I was not hand-wringing——

Mr. CHABINSKY. I know the good Senator was not. And so, I believe that we have the capabilities. We just have not been funding any thought leadership in those areas to figure out what to do about it.

Chairman JOHNSON. Dr. Valeriano, what are your thoughts on this?

Mr. VALERIANO. There is a reason we have not seen much escalation in the cyber domain, and that is because everyone is vulnerable. Asking for more escalation, asking for responses, looking for conventional or even cyber responses to cyber violations is a dangerous step that we have not taken yet, other nations have not taken yet, and there is a reason why, because we are all vulnerable.

So, what we are asking for here is dangerous, and that is why we have instituted a system of norms that seems to have worked so far. And, what we have done to reply in terms of sanctions or diplomacy has generally kept a lid on the cyber escalation so far. And, the worry is if we go further, what will happen next?

Chairman JOHNSON. So, you are agreeing with Mr. Chabinsky on this one? Because I think in testimony you were pushing deterrence, and you were saying it is impossible.

Mr. VALERIANO. It is more that I just do not believe in the word "deterrence" in cyberspace because of the way that term, what it really means, it does not fit. But, we do need responses. It is just these responses need to be managed, and they need to fit into the international context as they operate now.

Chairman JOHNSON. Mr. Greene, do you want to chime in on this one?

Mr. GREENE. On the criminal front?

Chairman JOHNSON. I mean, the response. So, again, just to summarize what I am hearing, on the one hand, to respond offensively with other cyber attacks we are saying is pretty dangerous. We are all vulnerable. We are going to ramp it up. So, what has been effective is raising the issue, having reports, saying that we have this little directorate in a particular nation-state exposing that, putting diplomatic pressure on it, seems to have provided some measure of success. What else can we do? Or what is your reaction to—I think I summarized that properly.

Mr. GREENE. We are not going to arrest our way out of this problem, but we can help it, and I go back to when I talked about how we address security generally, there is no 100-percent solution. There might be 5, 6, 7, or 10-percent solutions. The arrest of the three Romanians who were extradited had a deterrent impact on other criminals. Indictment alone, even if we cannot reach out and touch them, if you have an international indictment, international scope, you limit the ability of a criminal to travel, to use their funds. It has an impact.

Chairman JOHNSON. To travel, to use their funds, transfer those around the world.

Put them in a safer place.

Mr. GREENE. I suspect that the Chinese military folks who were indicted 2 or 3 years ago probably did not like seeing their faces on FBI wanted posters, the same with the seven Iranians who were indicted. But, it does, as Mr. Chabinsky said, come back to resources. The FBI is doing what it can. They have some really great people, and they partner really well with the private sector. But, we can amp up that deterrence if we have more folks working it.

Chairman JOHNSON. Let us make the analogy to criminal statutes. You have a very well defined crime. We all know exactly what it is. I am not going to use an analogy, but you can think of your own. And, then, you have very well defined penalties in law.

We do not have that for cyber criminals—I mean, we do but we do not. Correct? For example, cyber warfare, what is the definition really of cyber warfare? And, I think, Doctor, you were talking about if it crossed the threshold of violence, I think that is what you said.

Mr. VALERIANO. Yes, war denotes violence.

Chairman JOHNSON. And, that could be violence against things as well as people, correct?

Mr. VALERIANO. Not necessarily.

Chairman JOHNSON. You would confine it to people?

Mr. VALERIANO. Yes.

Chairman JOHNSON. So, you would not consider it warfare then when, for example, we believe North Korea destroyed how many computers at Sony? If a bomb were dropped and thousands of computers were destroyed at a company, would we not consider that warfare?

Mr. VALERIANO. Conventionally, in academic discourse, it is a thousand battle deaths. That is what warfare——

Chairman JOHNSON. Pardon?

Mr. VALERIANO. A thousand battle deaths is what warfare is in terms of figuring out what it is and what it is not.

Chairman JOHNSON. OK.

Mr. VALERIANO. And, that is how we have always defined it, and that is how we continue to define it. And, I do not see any need to change it with cyber warfare.

Chairman JOHNSON. So, would you say that we have defined cyber crime, cyber warfare, well enough?

Mr. VALERIANO. I think so. I think we use the term "war" too much. You could maybe call this "political warfare," "gamesmanship," things like that. But, it is not war.

Chairman JOHNSON. But, it would if they started attacking critical infrastructure——

Mr. VALERIANO. Yes.

Chairman JOHNSON [continuing]. And lives were——

Mr. VALERIANO. And, the reason you do not want to call it "war" is because that demands a response. And, it is not clear we can respond at this point, so we want to save it for those real instances where we have to respond.

Chairman JOHNSON. Can you guys comment on what the doctor just said there? We will start with you, Captain.

Captain KEENEY. I would like to tie together a few of these things that we have been talking about over the last couple minutes.

So, from an attribution perspective, I think pretty recently CrowdStrike did some attribution of—it is a public company, not a U.S. intelligence agency, so, therefore, anyone who pays for their subscription gets this information, right?

On Ukraine in specific, there was an application that the Russians were using that soldiers in the Ukrainian military had on their smartphones, which then led the Russian military to be able to target those soldiers in the Ukrainian military who were using artillery pieces. How interesting.

Well, guess what? In the battle, warfare, they were able to target the high-end artillery pieces with 80 percent success in destruction and like 50 percent in the lower-end pieces of artillery. So, that is great. That is what I would call hybrid warfare. So, it is the mixing of both of these domains.

So, then how do we respond to that? I believe that is the question we are kind of talking about. I think we have to define, Did they cross a red line? If they did, is their intel gain lost? Do we need to attack back or not? Do we lose something if we do? The whole impacts of DIME obviously have to be assessed.

Then we target it, and that targeting could then pick an effect. It could be cyber in nature; it could be physical destruction in nature; it could be political in nature. And, then, we deliver the effect,

especially if they cross a red line. And, we should not reveal what those are to our adversary either, which we have done in the past.

Chairman JOHNSON. I would argue in that case you are already in a kinetic war. I think we already define that as war, and we just assume that the armies are going to be using whatever cyber assets they have to conduct that war. I think really what is more troubling is outside of kinetic war, you are just sitting here minding your own business, and all of a sudden there is an attack, whether it is a denial-of-service attack or——

Captain KEENEY. I could give you a very relevant example from corporate America. So, if China has been stealing our intellectual property and doing things like that pretty in the open and hacking, and we had a pretty good response through political means to change that, what I think would happen—what I think has happened is our adversaries changed their tactics. The war is still ongoing. They are just not using overt hacking techniques. Instead, they have moved to human intelligence collection operations inside of corporate America. I know this to be true.

Chairman JOHNSON. Well, there is a reason their fighter jet looks a lot like ours.

Captain KEENEY. Exactly.

Chairman JOHNSON. Doctor, you were going to say something?

Mr. VALERIANO. I would just add that changing the tactics means that what we are doing actually is working, and if they are reverting to conventional intelligence means, that actually is a very useful result.

The other thing about the CrowdStrike issue and Ukraine is that was retracted by CrowdStrike, and they said that they overestimated the impact of these attacks on the artillery pieces. So, we are not even sure we have very good examples of active cyber warfare.

Chairman JOHNSON. Well, let us put the kinetic part of that Ukrainian conflict aside and just open source, the attack on the electrical grid twice now. Pretty sophisticated cyber attack. That is what I am talking about. That type of thing is really coming close to maybe what you want to define as cyber warfare, but I think most people would probably consider it to be so.

Mr. VALERIANO. It does seem to be, though, basically probes and testing how far they can go. And, the solution was very conventional in that they just flipped the switch and turned things back on.

Chairman JOHNSON. Well, they had breakers. They could do that. I am not sure—as I understand the American—and I am no electrical engineer here, sorry. I am an accountant. But, at least I am an accountant, OK? I am a business guy. We would have a much more difficult time. We are probably more vulnerable because of the advancement of our technology. That is part of the problem. With the Internet of Things, all the explosive devices, we have become more and more dependent on our electrical grid, more and more dependent on the Internet, and as a result, we are far more vulnerable, which I guess would indicate to me we better start defining these things. We probably ought to start laying out some pretty strong lines and be very predictable. You cross this and, this is something that we would define as war, and, then, of course, pol-

icymakers, Presidents, Congress, would have to decide what the response would be.

Does anybody want to argue against that point?

Mr. VALERIANO. No, and I would just add that we should not blame the victim, but we also have to look to the victim and see what they are doing, and that is clear from your example.

Chairman JOHNSON. Sure. But, again, I think Mr. Chabinsky's point is very appropriate, that analogy, in terms of blaming the end user and Flint. Would we really expect every household to put in a filtration system? Does it not make a lot more sense at the source? And, that would really get me into my next line of questioning, the personnel issue.

I want to visit your—whatever you call it, the ROCK or MOCYBER. I think it is a really intriguing process because I think that is what we need to do, is we need to figure out how do we tap into the brilliant minds in the private sector across the board, not just as it relates to this. I mean, you take a look at our IT resources here in the Federal Government. They are just antiquated. We are still using floppy disks apparently. Some of these are just legacy systems that are ridiculous, but we have layer upon layer of procurement policies that make it almost impossible to update and modernize. We cannot afford to let the bureaucratic, sclerosis prevent us from really addressing these cyber threats.

So, how do we do that? I mean, we have one example of how we did it with the Missouri National Guard. Can you just kind of speak to that? Mr. Chabinsky, you are at the ready there.

Mr. CHABINSKY. Thank you, Chairman Johnson. First, I would say we have to really figure out what we want our people to do. I think that the workforce development issue runs the risk of training a lot of science, technology, engineering and mathematics (STEM) minds and taking them away from innovation and curing the problems, the bigger problems of——

Chairman JOHNSON. Well, I would rather have them in the private sector, but we have to figure out how to tap into——

Mr. CHABINSKY. But, what I am suggesting is that I do not want to have to have them at all. In other words, if we solve this problem correctly, we do not need more and more people to solve the problem. So, if we can get this up to a higher level, the first question is: What is our strategy, and what people we need—the fewer amount of people that are needed to execute on a strategy that will reach the greatest goal?

Chairman JOHNSON. Just to clarify, what you are saying is what you would like to see is in the private sector, every time you design a new device, that source is where you build the protection, the defense so it cannot be——

Mr. CHABINSKY. So a four-part plan. One is threat deterrence. The other is at the Internet ecosystem itself where there is much greater visibility on where botnets are, where the command and control is and the ability to take those down. And, then, at the device level, making sure that the market works better through more transparency and what the security is. And, finally, better metrics that are designed to show is what we are doing actually working against the threat.

In each of those instances, what is clearly not needed are more people on the ground in every agency and every business that are running cybersecurity. You might only need 1,000 people at the Internet ecosystem level. You might end up needing 40,000 people for workforce development at the business level.

Chairman JOHNSON. Again, I get your point, but how do you organize and how do you direct those 1,000 people?

Mr. CHABINSKY. So, one area that we had recommended on the Commission for Enhancing National Cybersecurity is that we should consider apprenticeships, because the pace of this problem is moving so quickly, and going through school and building up debt and then getting out only to find out that what you learned 4 years ago has no practical application to the current threat just is not working for us. In some parts of Europe, including the United Kingdom (U.K.), there are apprenticeships where the Federal Government actually helps sponsor what the credentialing would be, where a company brings people in, it is on-the-job training, they are getting paid for doing it, and we could have a better workforce immediately. So, that would be one example of a way to get more people into this battle.

Chairman JOHNSON. So, where would those apprenticeships—in which companies?

Mr. CHABINSKY. Well, currently——

Chairman JOHNSON. Service providers or——

Mr. CHABINSKY. Everywhere, unfortunately, now, because it is needed everywhere. One day I would like to have a strategy that would focus them up to higher levels.

Chairman JOHNSON. Does anybody else want to speak to what Mr. Chabinsky is saying? We will start with you Mr. Greene.

Mr. GREENE. Two points. On the apprenticeship point, we have a program similar to that in our company, Symantec Career Connection, where we work with high school and college-level students to get them on-the-job training, help place them when they get out, tend to serve military and underserved communities.

The second point, though, is identifying what resources you have is really important. We just finished internal cyber war games that we do every year, and part of that is to motivate the workforce, to have something everyone enjoys working on, but also we identify skills in people that we may not know they have, they may not know they have. We come out of that with a better knowledge of what our workforce can do and how best to use the skills that they have.

So, there are ways that you can do it. I think that there are probably folks within agencies, companies, whatever, who can do a lot more than they are. It is easier to take someone who knows a network, teach them how to secure it, than to bring in someone who does not know that network, has a school book knowledge of security, and have them learn both things at once. So, we need to make better use of the resources that companies and government already have.

Chairman JOHNSON. By the way, I am all for efficiency and doing things smart. So, in addition to the apprenticeship, are you pretty well buying into what Mr. Chabinsky is saying here in terms of the approach, invest it at the source as opposed to the end user?

Mr. GREENE. Yes, I think——

Chairman JOHNSON. That is the right direction?

Mr. GREENE. Yes.

Chairman JOHNSON. Doctor, do you have an opinion on that?

Mr. VALERIANO. Well, I think what we have here is education in universities, and we are not leveraging the power of our universities so far. We have NSA accreditation on different levels, but that is about it, and it is not really used to great effectiveness. We have not seen great programs built. We have seen a lot of money go to private universities, but it has not been used very well. We need to expand diversity. We need to expand access. We need to do this throughout the United States, and we have not done that so far.

Chairman JOHNSON. By the way, last week we had the Chancellor of UW-Madison talking about 42 percent of researcher time on Federal grants in research universities is spent complying with Federal regulations, pushing paperwork. So, no kidding we are not very effective at this.

Captain, do you want to comment on this part of the discussion?

Captain KEENEY. Yes, it reminds me of a book I read recently about the history of the American Telephone and Telegraph Company (AT&T) and Bell Labs and how Bell Labs grew into AT&T and created satellite and fiber optics and all the things that we take advantage of today. They got so big and so dominant that we had to break them up into smaller pieces, right?

Chairman JOHNSON. And, they got more competitive.

Captain KEENEY. All that kind of stuff, right?

Chairman JOHNSON. By the way, I like small business myself. That is where I come from. I like competition.

Captain KEENEY. Sure. Me, too.

I have owned a couple along the way. But, my point there is in reading that book, one of the things that stuck out to me and I think is relevant to this conversation is the people that made the biggest leaps were not the engineers; they were not the guys that studied and got a degree in physics. They were important to solve technical problems, but it was the innovators in the early days of Bell Labs, the guys and gals who thought outside the box, who just wanted to tactically solve problems, who then went to an engineer who was certified and trained in all those things, and said, "I need to solve this piece of the puzzle," but they were able to innovate. And, I think in the cyberspace, by apprenticeship programs and getting younger minds engaged and not having to go get $100,000 in debt and take 6 years to get through a program before we get them applied to the problem, I am always impressed by young people when you just give them a problem to solve.

Chairman JOHNSON. By the way, it is interesting you just mentioned this. I just pulled up a quote I sent myself, George Bernard Shaw: "The reasonable man adapts himself to the world; the unreasonable one persists in trying to adapt the world to himself. Therefore, all progress depends on the unreasonable man."

Kind of adapting to what you are talking about is you do need people thinking outside the box, looking at this, and it is not necessarily coming from computer scientists, though. It might come from somebody—and that is why the more people you have look-

ing—I would say it is smaller innovative companies is I think where the solution lies, as opposed to some massive Federal bureaucracy trying to really dictate this, which is one of the parts you pointed out, too, is let us address this from the standpoint as it is as opposed to the way we have constructed our bureaucracy. Is that a valid point?

Mr. CHABINSKY. And, Chairman Johnson, if I could just pull a thread on what Captain Keeney said, he said that the young minds were brought problems to solve. We have an enormous capacity in the cybersecurity world never to define what the actual problem is that we are looking to solve. And so, we have a lot of information sharing where people are just throwing things at each other, but there is really no goal at the end of it all. And, we somehow think that it will all magically come together to solve the cybersecurity problem. Why do we not define first what are the five largest cybersecurity problems our Nation is facing, then figure out who are the—but, let us figure out who the fewest number of companies, who the fewest people are to create the solutions for the top problems to inure to the benefit of the most.

Chairman JOHNSON. So let me just, a little off topic, but my perspective, coming from the private sector, in Washington, D.C., is everything is tactical. My problem-solving process in the private sector starts with laying out reality, strengths, weaknesses, opportunities and threats (SWOT) analysis, root cause analysis based on that reality. And, by the way, we are trying to lay out that reality here. That is what these hearings are about. You establish goals. Once you agree on what the goals are, then you start developing the strategies, and the tactics are there to support the strategies. But, if you are at the tactical level, they are not tied to a strategy. They are divorced—if they are not directed toward a goal—they are divorced from reality. I think I just described the Federal Government versus the private sector.

So, we need to lay out the reality, and the problem we have in cyber is it is very complex, and we do not have very many members with Senator Daines' experience on this. I was at an American Enterprise Institute (AEI) conference, and we were talking about the whole encryption issues. And, one of the points I made is on this island we are primarily Gilligans; not too many professors here.

So, it is a real challenge, the complexity of this, and you just have people that do not—there are very few professors. So, it starts with that knowledge.

But, let me close this out because I have to close this hearing in 6 minutes. What would you say are the top priorities, what are the things that, this dysfunctional place needs to do to start addressing this more effectively? And, I will start with you, Mr. Greene. Then we will just go right down the aisle. Give us the number one thing we have to do, or number two. And, I will just tell you, in the first 4 years where everybody was saying, "Hey, you got to do cybersecurity." It was always, "You have to start sharing information more effectively." And, we kind of did that a little bit, but we have just barely scratched the surface on what we need to do. Mr. Greene.

Mr. GREENE. The thing that worries me the most long term on a national scale is the explosive growth—and we are still at the lip

of the curve—of connected devices. And, the point you made about Ukraine getting the power grid back online because they could go flip a breaker, we need to start building systems that—assessing how critical they are, if they are truly critical, either not connecting them—that has to be an option; it is not considered today—or making sure we have some manual way to fix it if we are talking truly critical. So, securing those critical devices that are going to be connected.

The other half of that piece is shifting the market incentives. Right now, there is all the incentive to be first to market. There is no incentive to be secure to market. Most of the incentives should be functionality, speed getting to market, but we need to build in in the design phase at least the thought to the security piece. So, if we can introduce the concept of secure to market, either through empowering consumers, understanding what they are doing, how the government purchases, but we need to focus on that as we connect everything.

Chairman JOHNSON. In Israel, they have the cyber director now reporting right to the Prime Minister, and they have the three R's: two of them are resiliency, building it so it is resilient, but then be able to recover. That is what you were just talking about. Mr. Chabinsky.

Mr. CHABINSKY. Mr. Chairman, I would recommend that the United States take immediate international leadership to create what I would call a "moon shot," which would be to rid the entire international community of all major botnets within 2 years. If you look at what botnets generate, it includes economic espionage with command and control. It includes financial theft with the command and control of credential-stealing malware. And, it obviously includes attacks through distributed denial of service (DDOSs) of our energy grid and other critical infrastructure.

I believe that that is possible. I believe that it would be an effective way of building international communities as well as determining the vast different roles of governments and the private sector. And, I think that if we were able to achieve that, not only would we resolve an enormous amount of problems before they ever reach our financial sector, our power grid, or, companies; but it also would end up building the type of thought processes that could tackle a lot of the other problems we are seeing. And, I would look forward to working with the Chairman to scope that measure out.

Chairman JOHNSON. OK. I like the idea. Doctor.

Mr. VALERIANO. Of course, the challenge is critical infrastructure, including things like cars, because you should not be able to drive a car and hack into it. That is just absurd. We did the same thing with airplanes. We were connecting entertainment systems to navigation systems.

But, to me the second challenge is about individual reaction, and we have not done a whole-nation kind of plan to figure out what to do next. We did that during nuclear war. We had a bunch of options about what we would do to solve the problem. We have not reassured the civilian population about what will happen if there are cyber attacks. We have not talked about what we have done to protect the civilian population. We are always talking about cyber Pearl Harbor. We are not talking about the daily battles.

And, because of this, people overreact too much to the cyber threat, and they perform badly when challenged with even simple things like emails and clicking on Twitter links.

So, we have not even begun to study the psychology of the user of the Internet. What is this doing to our biology? What is this doing to our stress levels? And, I think that is a clear challenge that we have not even begun to start to talk about right now.

Chairman JOHNSON. OK. Captain?

Captain KEENEY. Senator, I would say my advice would be to expand the role of the military, both active, Reserve. Another idea came to me——

Chairman JOHNSON. You know that will face some resistance.

Captain KEENEY. Yes. Also, another interesting one would be State militias. Not every State has them, but many do, and these State militias could be an ability to bypass the traditional military basic training, all those sorts of requirements that a lot of people in private industry do not want to partake in for some reason. They are scared of push-ups, or pull-ups or whatever it is. But, leverage the State militias may be another way the Federal Government could help fund some State initiatives to get more cyber hands on the rope helping at the State and local idea is an idea.

And, then, I was thinking about certifying in some way, like the Underwriters Laboratories (UL), when you buy some piece of electric, it has UL certification. I am sure this is not my idea and many others have thought of it, but maybe that is a way we could begin to address this. If I buy the Internet-connected light bulb thing I have on my bedroom lamp and I tell Alexa to turn it on and off, if that in some way was able to be updated and was resilient, if there was a new exploit than when I bought it, I would have more confidence in it. That is maybe an approach at the consumer IOT level.

Chairman JOHNSON. We might be able to pass by unanimous consent (UC), if you are good enough with a keyboard, we will waive the push-up requirement. [Laughter.]

Listen, this has been, I think, very informative. I want to continue to work with you gentlemen. We want to work with the private sector to figure out exactly what we need to do here, because this is, I think you all recognize—which is why you are involved in this sector—incredibly important. So, thank you for your testimony. I appreciate your answers to our questions.

The hearing record will remain open for 15 days until May 25th at 5 p.m. for submission of statements and questions for the record. This hearing is adjourned.

[Whereupon, at 11:29 a.m., the Committee was adjourned.]

APPENDIX

Opening Statement of Chairman Ron Johnson
"Cyber Threats Facing America: An Overview of the Cybersecurity Threat Landscape"
Wednesday, May 10, 2017

As prepared for delivery:

Good morning and welcome.

Cybersecurity is one of the most significant issues facing the country, as it affects every sector—from manufacturing to finance to government to energy. In July 2012, General Keith Alexander, then Director of the National Security Agency, stated that the loss of industrial information and intellectual property through cyber espionage constituted the "greatest transfer of wealth in history." Of course, espionage is just one of the many cyber threats we face. Today's hearing looks at the broad cybersecurity threat landscape, which can be broken down into four categories: criminal attacks, malicious attacks, industrial espionage, and cyber warfare.

The mission of this Committee is to enhance the economic and national security of America and promote more efficient, effective, and accountable government. Ensuring an effective cyber deterrence and response strategy is key to achieving this goal. Before we can begin to discuss solutions, we must first understand the threats and trends associated with these threats.

The potential negative consequences of cybersecurity threats have no limit. Recently, a cybercriminal scammed two leading American technology companies out of $100 million. Another spoofed incoming calls to 911 call centers and blocked emergency communications for hours. A popular television show was leaked prior to its release date after a ransom fee was not paid. And, an organized cyberattack on critical infrastructure facilities was linked to power outages in Ukraine.

Emerging trends include the rise of ransomware and botnets as easy-to-use tactics that offer big rewards for cybercriminals. Ransomware, which consists of malware that encrypts data until the user pays a fee, is becoming more profitable and popular, even among less-sophisticated criminals. Internet of Things devices have been used to block access to some of the world's most popular website and can be compromised in a variety of cyber-attacks. Email is routinely used as a way to deceive users into opening the door for criminals to steal data and money.

Regardless of the motivations or identities of the attackers, cyber threats are real and growing. As a country, we must acknowledge and assess these threats and decide how to effectively respond.

I want to thank the witnesses for their thoughtful testimony, and I look forward to this important discussion.

U.S. Senate Homeland Security and Governmental Affairs Committee
"Cyber Threats Facing America: An Overview of the Cybersecurity Threat Landscape"
May 10, 2017
Ranking Member Claire McCaskill
Opening Statement

Thank you, Mr. Chairman. This hearing is an important opportunity for us to focus on the threats we face and to begin talking about how to address our nation's cyber security needs.

Critical vulnerabilities in cybersecurity impact our nation and countries across the globe. The federal government, states, and the private sector have all experienced cyber breaches with devastating outcomes. Just last week, a candidate in the French presidential race had electronic messages and documents from his campaign hacked and posted online in an attack that looks remarkably similar to the attack on the Democratic National Committee prior to the 2016 U.S. presidential election. The perpetrators of these types of attacks are trying to undermine our democracies by tarnishing particular candidates to influence voters and portray our electoral systems as flawed. Make no mistake – we need to figure out how to protect our governments and institutions from further cyberattacks, and we need to do it now.

One of the problems we face as a nation is that we don't have all the trained, qualified cyber security professionals we need to adequately address these threats. Right now, the demand for cyber professionals is far greater than the supply, both in government and the private sector.

We are also missing leadership on cyber security. Today, scores of senior cyber-related positions in agencies throughout the government remain unfilled. We are waiting for nominees to be announced for two of the top cyber-related jobs at DHS, Under Secretary at the National Protection and Programs Directorate and Deputy Under Secretary for Cybersecurity and Communications. There are essential cyber-related positions at the Departments of Defense, Judiciary, State and Commerce that are still awaiting nominations from the White House, as well. Right now, we're needlessly fighting with one hand tied behind our back. I implore President Trump to fill these positions with qualified nominees. Cybersecurity is an area that demands bipartisan solutions. To begin, we need to ensure that our government is properly organized to protect the country against cyber threats. Mr. Chairman, I am pleased that our staffs have begun discussions with our House colleagues on elevating cybersecurity within the Department of Homeland Security. Despite the significant role the Department plays in the nation's cybersecurity efforts, cyber appears to be a secondary function within DHS. That needs to change, which is why I'm excited that our bipartisan and bicameral staffs are discussing legislation that aims to appropriately elevate and operationalize DHS's cyber mission.

Federal efforts alone cannot guarantee cybersecurity. States and the private sector are presenting pioneering solutions to confront serious threats. The private sector owns and operates the majority of the critical infrastructure in this country and serves as the engine of innovation. I look forward to hearing the testimony from our witnesses who spend every day working hard to understand the nature of the threat and how we can better defend our networks. It is essential that we recognize and study the threats so we can develop strategies and policies to protect ourselves.

I take great pride that the citizens of Missouri have vital roles in defending our country from cyberattacks. Mr. Keeney is an excellent example of the state tapping into existing resources to amplify its talent pool and protect its infrastructure. He has been integral in developing the Missouri National Guard's cyber architecture, which is playing a key role in training units throughout the country to safeguard their systems. In his civilian life, Mr. Keeney is the director of cyber incident response at a Fortune 200 company. He is well aware of the threats we face and has firsthand experience defending against them.

The citizen-warriors in the National Guard are one step towards solving to the nation's growing cyber workforce problem and I am pleased to welcome him.

Thank you, Mr. Chairman, and I look forward to hearing from all the witnesses here today.

Prepared Testimony and
Statement for the Record of

Jeff Greene
Senior Director, Global Government Affairs & Policy
Symantec Corporation

Hearing on

"Cyber Threats Facing America: An Overview of the Cybersecurity Threat Landscape"

Before the

United States Senate
Committee on Homeland Security and Governmental Affairs

May 10, 2017

Chairman Johnson, Ranking Member McCaskill, my name is Jeff Greene and I am the Senior Director, Global Government Affairs and Policy at Symantec. I am responsible for Symantec's global public policy agenda and government engagement strategy, and represent the company in key public policy initiatives and partnerships. I also serve as a member of the National Institute of Standards and Technology's (NIST) Information Security and Privacy Advisory Board (ISPAB), and recently supported the President's Commission on Enhancing National Cybersecurity. Prior to joining Symantec, I served as Senior Counsel with the U.S. Senate Homeland Security and Governmental Affairs Committee, where I focused on cybersecurity and Homeland Defense issues.

Symantec Corporation is the world's leading cybersecurity company, and has the largest civilian threat collection network in the world. Our Global Intelligence Network™ tracks over 700,000 global adversaries and is comprised of more than 98 million attack sensors, which record thousands of events every second. This network monitors over 175 million endpoints located in over 157 countries and territories. Additionally, we process more than 2 billion emails and over 2.4 billion web requests each day. We maintain nine Security Response Centers and six Security Operations Centers around the globe, and all of these resources combined give our analysts a unique view of the entire cyber threat landscape.

Understanding the current threat environment is essential if we are going to craft good policy and effective defenses. We are therefore pleased to see the Committee's continued focus on this subject, and appreciate the opportunity to provide our insights.

I. The Current and Emerging Cyber Threat Landscape - Overview

Cyber attacks reached new levels in 2016, a year marked by multi-million dollar virtual bank heists, explosive growth of ransomware, attempts to disrupt the US electoral process by state-sponsored groups, a record number of identities exposed in data breaches, and some of the biggest distributed denial of service (DDoS) attacks on record powered by a botnet of Internet of Things (IoT) devices. Yet while the attacks caused unprecedented levels of disruption and financial loss, perhaps the most striking feature of the 2016 attack landscape is that in many cases the attackers used very simple tools and tactics. During 2016, valuable Zero-day vulnerabilities and sophisticated malware was used more sparingly than in recent years. Instead, attackers increasingly attempted to hide in plain sight. They relied on straightforward approaches, such as spear-phishing emails and "living off the land" by using tools on hand, such as legitimate network administration software and operating system features. Yet despite this trend away from sophisticated attacks, the results were extraordinary, including:

- Over ***1.1 billion*** identities exposed;
- ***Power outages*** in the Ukraine;
- Over ***$800 million*** stolen through Business E-mail Compromise (BEC) scams over just a ***six month period***;
- ***$81 million*** stolen in one bank heist alone;
- A ***tripling*** of the average ransomware demand;
- Average time-to-attack for a newly connected Internet of Thing device down to ***two minutes***.

These shifting tactics demonstrate the resourcefulness of cyber criminals and attackers – but they also show that improved defenses and a concerted effort to address vulnerabilities can make a difference. Attackers are evolving and developing new attacks not because they want to, but because they have to do so. And that evolution comes with a financial cost to the attacker.[1]

---

[1] *Symantec Internet Security Threat Report* XXII, April 2017
http://www.symantec.com/security_response/publications/threatreport.jsp (Pages 8-10)

II. Targeted Attacks: Subversion and Sabotage Come to the Fore

The world of cyber espionage experienced a notable shift towards more overt activity in 2016, designed to destabilize and disrupt targeted organizations and countries. We saw:

- a January attack against the Ukrainian power grid;
- an attack on the World Anti Doping Agency and subsequent release of test results;
- a widespread, destructive attack on computers in Saudi Arabia; and
- a second attack against the Ukrainian power grid in December.

In years past, any one of these events would have been the biggest story of the year. But in 2016, we also saw an attack on the US Presidential election, an operation that the Intelligence Community (IC) attributed to Russia. The IC also concluded that the campaign was likely judged a success by its perpetrators, making it likely that these tactics will be reused to influence politics and sow discord in other countries. Indeed, recent public reporting suggests that similar operations may be underway in France and elsewhere in Europe, and just last week FBI Director James Comey said that he expects to see similar attacks in the US before the 2018 mid-term and 2020 Presidential elections.

Cyber attacks involving sabotage have traditionally been rare, but 2016 saw two separate waves of attacks involving destructive malware. Disk-wiping malware was used against targets in the attacks on the Ukraine in January and again in December, resulting in power outages. Additionally, the disk-wiping Trojan Shamoon reappeared after a four-year absence and was used against multiple organizations in Saudi Arabia. Previously, Shamoon was used in highly destructive attacks against Saudi and other Middle Eastern energy companies, and press reports linked it to Iran.

Interestingly, the upsurge in disruptive attacks coincided with a decline or shift in some covert activity, specifically economic espionage, the theft of intellectual property, and trade secrets. Following a 2015 agreement between the US and China, which saw both countries promise not to conduct economic espionage in cyber space, detections of malware linked to suspected Chinese espionage groups dropped considerably. However, we did see some actors who had previously focused on economic espionage shift their focus to what appeared to be more politically motivated targets. Economic espionage did not disappear entirely, and we are constantly looking for indications of a resurgence in economically motivated theft of data.

III. Financial heists: Cyber Attackers Chase the Big Scores

Until recently, cyber criminals mainly targeted on individual bank customers, raiding accounts or stealing credit cards. That changed dramatically in 2016, and we saw a new breed of attacker with bigger ambitions. These groups targeted the banks themselves, sometimes attempting to steal tens of millions of dollars in a single attack. Gangs such as Carbanak have led the way, demonstrating the potential of this approach by pulling off a string of attacks against US banks. Over the past few years Carbanak appears to have targeted hundreds of banks in multiple countries.

During 2016, two other outfits upped the ante by launching even more ambitious attacks. The Banswift group managed to steal $81 million from Bangladesh's central bank by exploiting weaknesses in the bank's security to infiltrate its network and steal its Society for Worldwide Interbank Financial Telecommunication (SWIFT) credentials. It is important to recognize that SWIFT itself was not compromised; the attackers used stolen credentials to initiate fraudulent transactions. In order to cover their tracks, the attackers doctored the bank's printed confirmation messages to delay discovery of the transfers. They also began their attack at the start of a long weekend to reduce further the likelihood of a quick discovery. And while the attackers did make off with $81 million, it could have been much worse

as they attempted numerous other transfers that were detected because a spelling error in a recipient's name raised suspicions that led to the transactions being suspended.

Another group, known as Odinaff, also targeted users of SWIFT during 2016. Odinaff's efforts were focused on organizations in the banking, securities, trading, and payroll sectors and like Banswift, the attacks appeared to use malware to hide customers' own records of SWIFT messages relating to the fraudulent transactions. These attacks were highly methodical and sophisticated and required a lot of hands-on involvement. We did not find any evidence linking Odinaff and Banswift.[2]

While Banswift and Odinaff demonstrated some technical expertise and employed tactics associated with advanced groups, much less sophisticated groups also stole massive sums of money. Business email compromise (BEC) scams, which rely on little more than carefully composed spear-phishing emails, continue to cause major losses. Also known as CEO fraud or "whaling," BEC scams are a form of low-tech financial fraud where spoofed emails are sent to an organization's financial staff by scammers pretending to be the CEO or senior management. The scammers then request a large money transfer. Our research found that during the first half of 2016, more than 400 businesses were targeted by BEC scams *every day*. More recently, we observed a new technique – the "hijacking" of legitimate invoices sent by companies so that the account number is changed to that of the scammer.

These scams require little technical expertise but can reap huge financial rewards for the criminals – and significant losses for the companies involved. For example, early in 2016, an Austrian aerospace company fired its CEO after it lost almost $50 million to BEC scammers. And just last week the FBI issued an alert noting that "[b]etween January 2015 and December 2016, there was a 2,370% increase in identified exposed losses" from BEC scams. The FBI estimated that over $5 billion was lost to BEC scams between October, 2013 and December, 2016.[3]

IV. Living Off the Land

Attackers ranging from cyber criminals to state-sponsored groups have begun to change their tactics, making more use of operating system features, off-the-shelf tools, and cloud services to compromise their victims. We call this "living off the land" – making use of the resources at hand rather than malware and exploits – and it provides many advantages to attackers. As a start, identifying and exploiting zero days has become harder as improvements in secure development and bounty programs take hold. Similarly, the use of web attack toolkits dropped, likely due to the effort required in maintaining fresh exploits as well as a backend infrastructure. These shifts could also be an effort to preserve resources – zero days are expensive to find (or to purchase on the black market), and developing new exploits requires an investment in research and development that cuts into a criminal's profit. Finally, "living off the land" attacks are at times harder to detect, as recognizing the malicious use of a legitimate tool can be more complex than identifying malware.

The tools used in these attacks are widely used – completely appropriately. Many are default features of Windows and Microsoft Office, and provide functionality to users and system administrators. But under the control of a criminal, they can facilitate remote access and malware downloads without the use of vulnerabilities or malicious tools. That these tools can be misused is not news; Microsoft Office macros have existed for almost 20 years, and were a common attack vector in the past. For that reason, the overwhelming majority of users have macros disabled by default. 2016 saw the emergence of social

---

[2] See *Symantec Internet Security Threat Report*, XXII, April 2017 pp. 48

[3] FBI Public Service Announcement, *Business E-mail Compromise – E-mail Account Compromise the 5 Billion Dollar Scam, May 4, 2017;* https://www.ic3.gov/media/2017/170504.aspx#fn3

engineering techniques aimed at tricking users into enabling those macros – and thus opening the door to macro viruses.

The most high-profile case of a "living off the land" attack took place during the US elections – a simple spear-phishing email led to the theft of Hillary Clinton's campaign chairman's emails. This took place *without the use of any malware or exploitation of hardware or software vulnerabilities*. When executed well, these "living off the land" approaches can result in almost symptomless infections, allowing attackers to hide in plain sight.

V. Resurgence of Email as Favored Attack Channel

Malicious emails were the weapon of choice for a wide range of cyber attacks during 2016, used by everyone from state-sponsored cyber espionage groups to mass-mailing ransomware gangs. One in 131 emails sent were malicious, the highest rate in five years.[4] Email's renewed popularity has been driven by several factors – it is a proven attack channel and is not reliant on technical vulnerabilities, but instead uses deception to trick victims into opening attachments, following links, or disclosing their credentials. Malicious emails disguised as routine correspondence, such as invoices or delivery notifications, were the favored means of spreading ransomware. The availability of botnets-for-hire allows criminals to mount massive campaigns pumping out hundreds of thousands of emails daily.[5]

VI. Ransomware Squeezing Victims with Escalating Demands

Ransomware continues to plague businesses and consumers, and due to its destructiveness is one of the most dangerous cybercrime threats we saw in 2016. Criminal gangs engaged in indiscriminate campaigns involving massive volumes of malicious emails that in some cases overwhelmed organizations by the sheer volume of ransomware-laden emails alone. Attackers are demanding more and more from victims, and the average ransom demand *more than tripled* in 2016, from $294 to $1,077. The number of new ransomware families also more than tripled to 101, from 30 in both 2014 and 2015. The volume of attacks increased as well. Detections were up 36% percent from 2015, and by December we were seeing almost twice the daily volume that we observed in January.

2016 also saw the emergence of Ransomware-as-a-Service (RaaS). This involves malware developers creating ransomware kits which can be used easily to create and customize new variants. Typically the developers provide the kits to attackers for a percentage of the proceeds. One example of RaaS is Shark (Ransom.SharkRaaS), which is distributed through its own website and allows users to customize the ransom amount and which files it encrypts. Payment is automated and sent directly to Shark's creators, who retain 20 percent and send the remainder on to the attackers. Our statistics show that, for the most part, attackers are concentrating their attacks on countries with developed, stable economies – 34% of the detections were in the US, and another 39% spread among the United Kingdom, Australia, Germany, Russia, the Netherlands, Canada, India, Italy, and Japan.

VII. New frontiers: IoT Moves into the Spotlight

While ransomware and financial fraud groups continue to pose the biggest threat to end users, other threats are beginning to emerge. It was only a matter of time before attacks on IoT devices began to

---

[4] See *Symantec Internet Security Threat Report*, XXII, April 2017 pp. 27-28 (https://www.symantec.com/security-center/threat-report)

[5] *See* Attachment for a compilation of recent prices from the black market to rent botnets, purchase ransomware kits, and buy stolen identities and credit card details. *Symantec Internet Security Threat Report, XXII, April 2017, pp. 51.*

gain momentum, and during 2016 Symantec witnessed a twofold increase in attempted attacks against IoT devices. During peak activity the average IoT device was attacked once every two minutes.

2016 saw the first major incident originating from IoT devices, the Mirai botnet, which was composed of routers, digital video cameras, and security cameras. Weak security – in the form of default and hard-coded passwords – made these devices easy pickings for attackers. After compromising millions of devices, the attackers controlled a botnet big enough to carry out the largest DDoS attacks ever seen. In October, the combined power of these compromised devices led to brief outages at some of the most popular websites and online services in the world. Mirai's impact was further magnified when the developer released the source code for the malware, which led to copycat efforts by other groups.[6]

VIII. Successful Disruptions of Cybercriminals

Investigating and prosecuting cybercrime is technically complex, and requires a level of expertise and training that many police agencies and prosecutors are just now beginning to develop. It is also resource intensive – the time and money required to see a case from inception through to a successful conviction is often substantial. The criminals know this, and indeed often count on it. Yet despite these obstacles, law enforcement and the private sector – working together – have made significant progress over the last year and conducted several successful takedowns of prominent cybercrime gangs.

Perhaps the most notable success of 2016 was the arrest and extradition of three Romanian nationals who ran the Bayrob gang. This was the culmination of an eight-year FBI investigation, which we assisted throughout that time. Symantec first exposed Bayrob in 2007, detailing a highly sophisticated eBay scam involving fake auto sales. Despite this public attention the gang continued its criminal activities, carrying out more online auction fraud, as well as diversifying into credit card fraud and recruiting a network of money mules in the US and Europe in order to move nearly $35 million back to Romania. Later, the group turned its attention to building a botnet for cryptocurrency mining, which eventually grew to more than 300,000 computers. On December 16, 2016, the three were indicted in the U.S. District Court in the Northern District of Ohio and are currently in federal custody awaiting trial.[7]

Another major takedown occurred in June 2016 when Russian security forces cracked down on the Lurk group, arresting 50 people in Moscow. The Lurk banking Trojan had targeted Russian financial institutions, stealing more than $25 million. These arrests coincided with a drop in activity from a number of threat groups that focused on financial fraud, including Locky, Dridex, and the Angler exploit kit. Since the Lurk arrests, Angler has disappeared from the threat landscape.

Lastly, the Avalanche botnet takedown dealt a severe blow to cybercriminals across the world. The takedown was a combined effort by multiple international law enforcement agencies and IT organizations, including Symantec. It resulted in the arrest of five individuals and the seizure of 39 servers and several hundred thousand domains, which served as the command and control hub for more than 800,000 compromised computers across the world.

While cybercrime continues to be profitable, the number of significant takedowns and disruptions in 2016 demonstrated that it is no longer a risk-free enterprise. In particular the extradition of the alleged Bayrob masterminds from Eastern Europe to the US sent a strong message that cybercriminals cannot work with impunity from remote locales.

---

[6] See *Symantec Internet Security Threat Report*, XX!!, April 2017 pp. 68

[7] https://www.justice.gov/usao-ndoh/pr/three-romanian-nationals-indicted-cyber-fraud-case-which-they-infected-60000-computers

IX. Protecting Against an Evolving Threat

Attacks are getting more sophisticated, but so too are security tools. Security still starts with basic measures such as strong passwords and up-to-date patch management. But while these steps may stop some older, simpler exploits, they will be little more than a speed bump for even a moderately sophisticated attack – and will do little to slow a determined, targeted attack.

Effective protection requires a modern security suite that is being fully utilized. An attack requires access, and attackers are increasingly relying on stolen credentials to gain their footholds. Deploying effective multi-factor authentication is essential to denying access to the would-be attacker. To block advanced threats and zero day attacks, sophisticated machine learning and advanced exploit detection and prevention technologies are necessary. This includes tools for detecting encrypted malware, as attackers are increasingly using encryption in an effort to bypass common security tools. Automated security tools learn how to identify attacks, even ones that have never been seen before. It is also increasingly critical to use big data analytics to evaluate global software patterns to create real-time intelligence. Today these analytics are able to identify and block entirely new attacks by evaluating how they are distributed and their relationships with other devices and other files.

Data protection is equally important, and a comprehensive security program includes data loss prevention (DLP) tools that index, track, and control the access to and movement of huge volumes of data across an organization. Perhaps most importantly, DLP tools will prevent that data from moving outside an organization. Organizations should also use encryption technology on particularly sensitive data, which renders it unreadable to anyone who does not have the specific cryptologic key.

Device-specific protections are also important. For example, in the retail world, there are tools that can be applied to point of sale systems that will virtually lock down the system and only allow it to perform those limited functions that are absolutely necessary for completing a sales transaction. In the IoT world, there are authentication, encryption, and endpoint protection tools that are designed to run on small and low power devices. These tools can protect everything from a connected vehicle to the small sensors built into a bridge or that monitor critical machinery. Finally, for the IoT devices that simply cannot be secured – either because they lack the power to run security tools or because it is simply unavailable – we developed Norton Core™, the first router designed specifically to secure IoT devices, whether a connected appliance or a digital video recorder.[8]

Good security does not happen by accident – it requires planning and continued attention. But criminals will always be evolving, and security must as well.

Conclusion

With the growth of connected devices – from the health trackers we carry in our pockets to the industrial systems that we unknowingly rely on in our daily lives – computer security is now everything security. In 2016, the attacks on the power grid in the Ukraine, as well as the attacks on the US election, drove home this point. But even as attacks morph and improve, so too do defenses, whether technical or through increased awareness. So while it is true that attackers were able to come up with new attack methods that challenged defenders, it is equally true that developing those attacks cost the criminals time, resources, and money. Cybersecurity is the proverbial journey, not a destination. Understanding the threat, how it is changing, and where it is going, is essential if we are going to stay on track in this journey. This hearing is an important step in advancing that understanding.

---

[8] *See* https://us.norton.com/core

Attachment

Underground marketplace price list

Payment cards	Price
Single credit card	$0.5 - $30
Single credit card with full details (Fullz)	$20 - $60
Dump of magnetic strip track 1&2 & PIN	$60 - $100
Malware	
Basic banking Trojan kit with support	$100
Password stealing Trojan	$25 - $100
Android banking Trojan	$200
Office macro downloader generator	$5
Malware crypter service (make hard to detect)	$20 - $40
Ransomware kit	$10 - $1800
Services	
Media streaming services	$0.10 - $10
Hotel reward program accounts (100K points)	$10 - $20
Airline frequent flyer miles account (10K miles)	$5 - $35
Taxi app accounts with credit	$0.5 - $1
Online retail gift cards	20% - 65% of face value
Restaurant gift cards	20% - 40% of face value
Airline ticket and hotel bookings	10% of face value
DDoS service, < 1hr duration, medium target	$5 - $20
DDoS service, > 24hr duration, medium & strong target	$10 - $1000
Dedicated bulletproof hosting (per month)	$100 - $200
Money transfer services	
Cash-out service	10% - 20%
Accounts	
Online bank accounts	0.5% - 10% of account balance
Retailer accounts	$20 - $50
Cloud service provider accounts	$6 - $10
Identities	
Identity (Name, SSN & DOB)	$0.1 - $1.5
Scanned passports and other documents (e.g. utility bill)	$1 - $3

Testimony of

Steven R. Chabinsky

Before the
United States Senate
Committee on
Homeland Security and Governmental Affairs

"Cyber Threats Facing America: An Overview of the Cybersecurity Threat Landscape"

May 10, 2017

Introduction
Good morning Chairman Johnson, Ranking Member McCaskill, and distinguished Members of the Committee. I am pleased to appear before you today to discuss cyber threats facing America. In particular, the Committee has asked that I provide an overview of the cybersecurity landscape from the threats of "criminal, malicious, industrial espionage, and warfare actors." The Committee also asked that I share my views of how the country should approach cybersecurity threats moving forward.

My Background
For almost twenty years, I have been committed to reducing the security risks associated with the misuse of emerging technologies. After joining the FBI in 1995, I became Principal Legal Advisor to the multiagency National Infrastructure Protection Center in 1998. From there, I continued to serve as the FBI's top cyber lawyer and, in 2006, I joined the ranks of the Senior Executive Service and was charged with the responsibility of building and leading the FBI's cyber intelligence program. I later served as Acting Director of the Joint Interagency Cyber Task Force and as the senior cyber advisor to the Director of National Intelligence, followed shortly thereafter by my selection as Deputy Assistant Director of the FBI Cyber Division. In 2012, I joined the cybersecurity technology firm CrowdStrike, becoming its first General Counsel and Chief Risk Officer. During this period, I also developed and taught a *Cyber Law and Policy* graduate class at George Washington University, and volunteered as a senior advisor to the DoD-led Purposeful Interference Response Team.

Last year, I served as one of twelve members of the non-partisan White House Commission on Enhancing National Cybersecurity. We issued our *Report on Securing and Growing the Digital Economy* ("White House Cybersecurity Commission Report") this past December.

Today, I am the global chair of the Data, Privacy, and Cybersecurity practice at White & Case, an international law firm with 40 offices in 28 countries. I also have been selected to serve on the Department of Homeland Security's Data Privacy and Integrity Advisory Committee. In addition, and since 2013, I have been the cyber tactics columnist for *Security* magazine. I focus my column on cyber risk management techniques, to include most prominently the NIST Cybersecurity Framework.

The observations and conclusions I will share today are in my personal capacity, and are the culmination of a career spent in government, industry, media, and academia.

I. We Are Losing.

We have heard it all before. The cyber threat is real and growing. Our vulnerabilities are real and growing. Our reliance on technology is real and growing. The harm from cyberattacks is real and growing. Consumer cyber risk is real and growing. Corporate cyber risk is real and growing. Government agency cyber risk is real and growing. The risk to our national security is real and growing. The amount of time, money, and talent that our country is diverting from other issues and devoting to cybersecurity is real and growing. All of these problems are real and growing, and they are getting worse.

In short, we are losing. The nation that invented the Internet, and so many of the connected technologies the Internet has made possible, increasingly is falling prey to it.

Why is this happening? With so many companies and agencies doing so much, how can America be losing the cybersecurity battle, and how do we set things right?

There are two primary lines of thought. There are those, the majority in fact, who believe we are pursuing the correct overall strategy, but that we are failing -- for any number of reasons -- in its tactical execution. Those who believe our strategy is sound are likely to focus on measures that network owners and operators can take, but currently are not, to better protect themselves. Examples of this line of thinking include both federal and state demands asking "more" of the millions of businesses and individuals that use the Internet: more cyber risk management plans and programs, more critical infrastructure regulation, more information sharing, more – indeed continuous – network monitoring, more software patches, more workforce development, more data breach lawsuits, more lessons learned, and more money spent.

But there is another line of thought, and it is the one to which I subscribe. There are those, like I, who believe we are pursuing a failed strategy, and that doing more of the tactics that underlie that failed strategy is an exercise in futility with diminishing and even negative returns. For those of us who believe that the strategy itself is to blame, there is a deep frustration at seeing our problems grow worse in the face of our well-intentioned national effort. It is like seeing somebody pushing harder and harder to open a door, when instead they should be pulling.

Those who believe, as I do, that our strategy is to blame, seek a paradigm under which we no longer insist that millions of American businesses and individuals constantly do more to protect themselves from the growing list of organized crime groups and hostile powers. We recognize the inevitability of targeted cyberattack, and are more likely to consider those who suffer computer breaches to be victims, rather than culprits. We believe that the government's primary role is to protect its citizens (and business interests), rather than to better enable citizens and businesses somehow to protect themselves against foreign aggression, and against all odds. In short, we seek strategies that remove the major responsibilities and costs of cybersecurity from the end-users of technology, in favor of higher level, international, public/private solutions that inure to the common good. We want the United States government to lead this security effort with stronger vision, urgency, and unstoppable resolve, and to do so in

coordination with and to the economic benefit of industry. We believe this is possible, but it will require a new way of thinking.

II. Who and What Are We Up Against?

I am convinced that given enough time, motivation, and funding, a determined adversary will always be able to penetrate a targeted system. What follows is a representative sample of the nature of the threat.

A. Criminals Seeking Financial Gain

It is important at the outset to demonstrate that today's cybercrime is organized, evidencing skill and logistics that really can seem like the movies. Take for example the international group that, in 2012 and 2013, hacked into the computer system of a credit card processor, found the database containing prepaid debit cards, changed security protocols, increased balances, eliminated account withdrawal limits, and distributed card numbers to members throughout the world. Essentially, the crew's heist was limited only by the amount of money in the ATMs they robbed, as well as an individual's physical capacity to carry thousands of $20 bills. Which leads to the following question: If an organized cyber group hacked into a credit card processor, created debit cards, distributed them to casher cells in 24 countries, who then conducted 36,000 transactions, how much money would they steal in 10 hours? The answer: approximately $40 million.

Depending on the region of the world, cybercriminals also can find safe harbor in working with government intelligence officers. This past March, the Department of Justice indicted four defendants, two of whom were officers of the Russian Federal Security Service (FSB) and who are charged with protecting, directing, facilitating, and paying the two other criminal hackers. Their alleged crime was breaking into Yahoo's email system and stealing information from approximately 500 million accounts. According to Federal prosecutors, the FSB was interested in gaining access to the accounts of Russian journalists, U.S. and Russian government officials, and a number of private sector employees. Meanwhile, one of the criminals decided to use his access to turn a profit by facilitating a spam campaign.

Not that foreign countries are above engaging in financially motivated hacking. North Korea is the number one suspect behind last year's attempt to rob Bangladesh Central Bank of nearly one billion dollars. Although the intruders were unable to fulfill that tall an order, they did manage a payday that exceeded $80 million.

B. Malicious Actors Not Seeking Financial Gain

One of the more troubling episodes we witnessed recently was the rise of Internet of Things (IoT) botnets, and the potential to use them to conduct disruptive attacks against

Internet infrastructure. One security company recently estimated that hackers hijacked more than 2.5 million IoT devices in 2016, primarily by using source code that was released for a piece of malware known as Mirai. In October of last year, a distributed denial of service attack was launched against a company called Dyn, which is a Domain Name System provider that helps other companies resolve the common domain names of websites to their corresponding IP addresses. Once Dyn was flooded with DDoS traffic (some of it said to have been generated by infected baby monitors of all things), it had a domino effect that impacted the services of over 70 companies, including popular media and ecommerce sites. The clear lessons learned are (1) that we have been quick to deploy billions of IoT devices, with billions more on their way, having little to no security; and (2) that we are only as secure as our third party infrastructure (together with our and their response and continuity plans).

C. State-Sponsored Industrial Espionage.

The private sector continues to find itself having to defend against foreign military and intelligence services seeking to steal their intellectual property. Sometimes these thefts are clearly related to anticompetitive desires, in which competing products are brought to market through state-owned companies or closely affiliated privatized firms. At other times, the theft of trade secrets may be tied to the national security concerns of the sponsoring country, as may be the case when military equipment plans are stolen. Still at other times, the stolen property can have a dual use (such as engines), or be viewed as so economically or societally important to the country that for the nation it is viewed as a matter of national security (such as may be the case with oil refinement techniques, or pandemic-related health research).

Regardless, incidents of foreign-sponsored espionage are never far from the headlines. A recent security report found that, of more than 600 data breach incidents they tracked in the manufacturing sector in 2016, over 90 percent could be defined as state-affiliated espionage. Meanwhile, on April 27, 2017, the Department of Homeland Security released an Incident Report that warned of an "emerging, sophisticated campaign" that has been going on for roughly a year targeting victims in information technology, energy, healthcare and public health, communications, and critical manufacturing. Although attribution has not definitively been made, early indications point to a foreign espionage campaign.

D. Cyber Warfare.

Our critical infrastructure networks are run by computers known as industrial control systems or, simply, control systems. These systems are designed for accuracy, extreme environmental conditions, and real-time response in ways that are often incompatible with the latest cybersecurity technologies, inconsistent with consumer grade hardware and software, and in conflict with common network protocols. As a result of these performance factors and limitations, engineers traditionally have been

responsible for the design, operation and maintenance of control systems, rather than IT managers. Yet, despite their uniqueness, control systems are increasingly reliant upon common network protocols, and connectivity often exists between control systems and enterprise networks, to include the Internet. The result? Critical infrastructure throughout the world is connected to the Internet, creating ready targets for cyber warriors.

Just this past February, Ukraine accused Russian hackers of continuing to target their power grid and financial system. This comes after a December 2016 hack into multiple energy distribution companies in Ukraine, also allegedly by Russia, which left tens of thousands of people without electricity for hours. According to reports of the event, Ukrainian energy company employees arrived at work only to see their computers taken over, with the cursers literally moving around monitors under someone else's remote control. 30 substations are said to have been taken offline in this way.

Closer to home, consider as a possible harbinger of things to come in the United States the rolling blackouts in 2003 that left 55 million people without power. The extent of the failure resulted from a software glitch that, unknown to systems operators, left the control room without any audio or visual alarms for over an hour. The operators thought everything was okay because the computers told them everything was okay.

In another example, known as Operation Aurora, as a proof of concept Idaho National Laboratory physically destroyed a hulking 2.25MW diesel generator in 2007 by way of a cyberattack, causing the machine to shake violently, erupt with smoke, and shoot out shrapnel as far as 80 feet away. And then there was the 2010 Stuxnet worm, in which malware targeted Iran's nuclear centrifuges in order to sabotage the country's ability to enrich uranium gas. Foreign countries and terrorist organizations most certainly have taken note of cyber vulnerabilities within the energy sector.

III. What If Everyone Implemented The NIST Framework?

NIST's Cybersecurity Framework is a thoughtful, elegant, and simply stated document, but don't let that fool you. Attempting to implement it is enormously difficult and costly. This is not because the NIST Framework is poorly crafted, quite the opposite. The majority of security professionals appear to agree that the NIST Framework is about as good as you can get. Its goals are certainly easy to understand, but they are operating in a complex risk environment. As a result, understanding what is expected under the Framework and being able to achieve it are two different things.

By way of analogy, imagine for a moment being provided with the following list of five requirements to implement a space mission:

1. Rocket ship required to reach the moon is established
2. All astronauts are informed, properly suited, and trained
3. Resilience requirements to land on moon without damage are established
4. Adequate capacity to ensure return to Earth is maintained

5. Resilience requirements to land on Earth without damage are established

Clearly, each of these steps is a lot easier said than done, and the list reads like a joke. However, should you think this comparison to cybersecurity is farfetched, pause to consider the details and the enormity of the challenges behind each of the NIST Cybersecurity Framework's 98 specifically recommended outcomes (which, no less, must be achieved while under attack):

1. Physical devices and systems within the organization are inventoried
2. Software platforms and applications within the organization are inventoried
3. Organizational communication and data flows are mapped
4. External information systems are catalogued
5. Resources (e.g., hardware, devices, data, and software) are prioritized based on their classification, criticality, and business value
6. Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) are established
7. The organization's role in the supply chain is identified and communicated
8. The organization's place in critical infrastructure and its industry sector is identified and communicated
9. Priorities for organizational mission, objectives, and activities are established and communicated
10. Dependencies and critical functions for delivery of critical services are established
11. Resilience requirements to support delivery of critical services are established
12. Organizational information security policy is established
13. Information security roles & responsibilities are coordinated and aligned with internal roles and external partners
14. Legal and regulatory requirements regarding cybersecurity, including privacy and civil liberties obligations, are understood and managed
15. Governance and risk management processes address cybersecurity risks
16. Asset vulnerabilities are identified and documented
17. Threat and vulnerability information is received from information sharing forums and sources
18. Threats, both internal and external, are identified and documented
19. Potential business impacts and likelihoods are identified
20. Threats, vulnerabilities, likelihoods, and impacts are used to determine risk
21. Risk responses are identified and prioritized
22. Risk management processes are established, managed, and agreed to by organizational stakeholders
23. Organizational risk tolerance is determined and clearly expressed
24. The organization's determination of risk tolerance is informed by its role in critical infrastructure and sector specific risk analysis
25. Identities and credentials are managed for authorized devices and users
26. Physical access to assets is managed and protected
27. Remote access is managed
28. Access permissions are managed, incorporating the principles of least privilege and separation of duties

29. Network integrity is protected, incorporating network segregation where appropriate
30. All users are informed and trained
31. Privileged users understand roles & responsibilities
32. Third-party stakeholders (e.g., suppliers, customers, partners) understand roles & responsibilities
33. Senior executives understand roles & responsibilities
34. Physical and information security personnel understand roles & responsibilities
35. Data-at-rest is protected
36. Data-in-transit is protected
37. Assets are formally managed throughout removal, transfers, and disposition
38. Adequate capacity to ensure availability is maintained
39. Protections against data leaks are implemented
40. Integrity checking mechanisms are used to verify software, firmware, and information integrity
41. The development and testing environment(s) are separate from the production environment
42. A baseline configuration of information technology/industrial control systems is created and maintained
43. A System Development Life Cycle to manage systems is implemented
44. Configuration change control processes are in place
45. Backups of information are conducted, maintained, and tested periodically
46. Policy and regulations regarding the physical operating environment for organizational assets are met
47. Data is destroyed according to policy
48. Protection processes are continuously improved
49. Effectiveness of protection technologies is shared with appropriate parties
50. Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are in place and managed
51. Response and recovery plans are tested
52. Cybersecurity is included in human resources practices (e.g., deprovisioning, personnel screening)
53. A vulnerability management plan is developed and implemented
54. Maintenance and repair of organizational assets is performed and logged in a timely manner, with approved and controlled tools
55. Remote maintenance of organizational assets is approved, logged, and performed in a manner that prevents unauthorized access
56. Audit/log records are determined, documented, implemented, and reviewed in accordance with policy
57. Removable media is protected and its use restricted according to policy
58. Access to systems and assets is controlled, incorporating the principle of least functionality
59. Communications and control networks are protected
60. A baseline of network operations and expected data flows for users and systems is established and managed.
61. Detected events are analyzed to understand attack targets and methods

62. Event data are aggregated and correlated from multiple sources and sensors
63. Impact of events is determined
64. Incident alert thresholds are established
65. The network is monitored to detect potential cybersecurity events
66. The physical environment is monitored to detect potential cybersecurity events
67. Personnel activity is monitored to detect potential cybersecurity events
68. Malicious code is detected
69. Unauthorized mobile code is detected
70. External service provider activity is monitored to detect potential cybersecurity events
71. Monitoring for unauthorized personnel, connections, devices, and software is performed
72. Vulnerability scans are performed
73. Roles and responsibilities for detection are well defined to ensure accountability
74. Detection activities comply with all applicable requirements
75. Detection processes are tested
76. Event detection information is communicated to appropriate parties
77. Detection processes are continuously improved
78. Response plan is executed during or after an event
79. Personnel know their roles and order of operations when a response is needed
80. Events are reported consistent with established criteria
81. Information is shared consistent with response plans
82. Coordination with stakeholders occurs consistent with response plans
83. Voluntary information sharing occurs with external stakeholders to achieve broader cybersecurity situational awareness
84. Notifications from detection systems are investigated
85. The impact of the incident is understood
86. Forensics are performed
87. Incidents are categorized consistent with response plans
88. Incidents are contained
89. Incidents are mitigated
90. Newly identified vulnerabilities are mitigated or documented as accepted risks
91. Response plans incorporate lessons learned
92. Response strategies are updated
93. Recovery plan is executed during or after an event
94. Recovery plans incorporate lessons learned
95. Recovery strategies are updated
96. Public relations are managed
97. Reputation after an event is repaired
98. Recovery activities are communicated to internal stakeholders and executive and management teams

And to what end? Unfortunately, we lack sufficient metrics to determine whether and to what extent the NIST Cybersecurity Framework and similar international standards are cost-effective. In fact, we lack the metrics to determine whether and to what extent they are effective at all in the face of today's evolving threat. If vulnerability mitigation was

inexpensive and easy to implement, one might be inclined to have everyone do it under the theory that it couldn't hurt; but, that is not the case.

IV. Can Trying to Become Impenetrable Make Things Worse?

As industry and government agencies continue to spend greater resources on vulnerability mitigation, they find themselves facing the problem of diminishing economic returns and perhaps even negative economic returns.

With respect to diminishing returns, information security professionals typically recognize cost effective benefits when applying baseline cybersecurity efforts. However, as companies direct their resources either against low probability events, or on pursuing all available defenses regardless of the ease with which an adversary can counter them, the amount of protection received for each dollar spent becomes progressively smaller and ultimately is worth less than the expenditure.

Imagine for example trying to protect a building by spending two million dollars on a 20-foot brick wall. Meanwhile, an adversary can go to a hardware store and for less than one hundred dollars buy a 30-foot ladder.

Far worse though than the concept of diminishing returns is the concept of negative returns, in which well-intentioned efforts actually make the problem worse. Although it often is difficult to convince good people that they are responsible for escalating a problem, consider our brick wall again. What if the defender spent ten million dollars to build an eighty foot wall? Instead of a buying a ninety foot ladder, the adversary might decide to use an explosive device to get through the wall, perhaps even killing people in the process. Comparing the brick wall to cybersecurity, there is reason to believe that our strategy often has the unintended consequence of threat actors escalating their capabilities and methods, and proliferating advanced malware, to include ransomware, which is increasingly destructive.

V. A Better Approach: Shift the Burden Away from End Users

It is not possible or optimal for every person and every company to be on the frontlines of cybersecurity. Instead, we should focus on fewer, higher level solutions that benefit everybody.

Shifting the burden away from end users will require a sustained international effort to tackle common Internet and communications ecosystem threats, such as eliminating botnets that infect millions of victims and can take down power grids. As stated in the White House Cybersecurity Commission Report, "to the maximum extent possible, the burden for cybersecurity must ultimately be moved away from the end user—consumers, businesses, critical infrastructure, and others—to higher-level solutions that include greater threat deterrence, more secure products and protocols, and a safer Internet ecosystem." It is worth expanding upon these concepts.

A. We should ratchet up threat deterrence.

In order to get security risks under control, whether in the "physical" or cyber worlds, security experts rely upon the levers of vulnerability mitigation, threat reduction and, should the first two fail, consequence management.

In the physical world, threat reduction – achieved primarily through threat deterrence – has been our predominant approach, and it has been largely successful. Throughout the physical security spectrum, whether describing the safety of nations, businesses, or individuals, safety most often is achieved because potential aggressors are deterred out of the fear they will be brought to justice, and actual aggressors ultimately are brought to justice. By way of contrast, our physical safety is not primarily reliant upon missile defense shields, gates, and body armor.

Yet, in the area of cybersecurity, vulnerability mitigation has been our nation's predominant approach, both for securing private sector and government systems. We have retained this focus on vulnerability mitigation despite it being well understood that securing networks is a daunting task even for the most experienced. It also would appear that while relying upon a vulnerability-mitigation-first strategy could work to protect static, isolated environments (such as fortresses and missile silos), there are no obvious examples of it working in dynamic environments when they are expected to interoperate with threat actors (such as the Internet).

It is my conclusion then that the bad guys, whether criminal or military, will not relent unless we improve our abilities to detect, identify and penalize them using all elements of national power. Doing so will require significantly maturing our strategies to focus on how the government and the private sector can coordinate and enhance our Diplomatic, Information, Military, Economic, and Law Enforcement (DIME/LE) options in order to deter or punish significant cyber threat actors. Similarly, the government and the private sector must resolve how to work together to jointly defend the nation in cyberspace.

We also must supplement our law enforcement and intelligence resources to focus on our adversaries. As an international group of scientists led by the University of Cambridge succinctly wrote in 2012, "we should spend less in anticipation of cybercrime (on antivirus, firewalls, etc.) and more in response – that is, on the prosaic business of hunting down cyber-criminals and throwing them in jail." For this to occur, we will need to reconsider how we fund cybersecurity efforts. Currently, the U.S. federal IT security budget is roughly $18 billion. Meanwhile, law enforcement funding is counted in the millions of dollars, with relatively few of the FBI's 35,000 employees trained as cyber intrusion Special Agents.

Our underfunding threat deterrence also hurts the private sector, which largely has been left to fend for itself. One financial institution disclosed that it planned to spend $600 million and dedicate 2,000 employees to cybersecurity last year.

Shifting our primary focus away from vulnerability mitigation in favor of threat deterrence would align our cybersecurity efforts with the security strategies we use in the physical world. In the physical world, vulnerability mitigation efforts certainly have their place. We take reasonable precautions to lock our doors and windows, but we do not spend an endless amount of resources in hopes of becoming impervious to crime. In fact, after taking routine measures, vulnerability mitigation has a relatively low return on investment. As a result, to counter determined thieves, we ultimately concede that an adversary can gain unlawful entry but, through the use of burglar alarms and video cameras, we shift our focus instead towards instant detection, attribution, threat response, and recovery. When the alarm monitoring company calls a business owner at 3 a.m., it does not say, "We just received an alarm that your front door was broken into. But, don't worry, we've called the locksmith." Rather, it is only obvious that the monitoring company calls the police. It is surprising then and suggests a larger problem that, in the world of cyber, when the intrusion detection system goes off the response has been to call the Chief Information Security Officer, and perhaps even the CEO, to explain what went wrong and to have them prevent it from happening again.

B. We should pay for a safer Internet ecosystem

Taking care of problems at the source, before they spread to consumers, businesses, and critical infrastructure, only makes sense. By way of analogy, when faced with the Flint Michigan water crisis, a federal state of emergency was declared, and solutions are being put in place to repair and upgrade the city's water system and to replace the pipes. Nobody would imagine opting instead for a solution to require every home and every business operating in Flint to purchase their own state of the art water filtration system along with the experts needed to continuously monitor and upgrade them.

To move forward with purpose, the Federal government should publish a Request for Proposal seeking innovative solutions. Financially incentivizing the private sector to solve the problem should be considered a budget priority, with perhaps as much as ten percent of our roughly $600 billion defense budget being set aside for the advancement of higher level cybersecurity solutions. In addition, we should consider expanding the telecommunications model we have in place to Connect America, which created a fund to expand rural access to voice and broadband, by implementing a program to Protect America by establishing a fund to extend cybersecurity across all of America. We often hear leaders say the private sector is on the front lines of cybersecurity. I agree, and it is well past time we pay them to defend us.

Similarly, we should promote alternative architectures that focus on threat deterrence. When thinking of cybersecurity, it is worth considering the Nineteenth Century findings of Charles Darwin. Despite the seeming simplicity of the well-known phrase "survival of the fittest," Darwin did not mean to suggest that survival of the fittest should always be considered in terms of health or strength. Rather, the fittest must be considered in terms of being the right fit for a particular purpose. Survival typically requires adaptability in areas other than health or strength, and adaptability can occur by chance

or by design. With due consideration of our economic and national security, as well as the health and welfare of the public, our government should be working with the private sector -- by design -- to adapt our security in a manner that best promotes our survival.

Unfortunately, at best we appear to be leaving decisions about the cybersecurity of our nation's critical infrastructure, and potentially therefore our nation's survival, either to chance, to prevailing market forces, or to the world community.

At worst, our declining security actually has occurred by our own design. Consider for a moment that, to date, the design elements of our policies, technologies, and resource allocations have focused on functionality, interoperability, bandwidth, speed and, more recently, anonymity and privacy. Our design elements have not focused on the security of our critical infrastructure. These choices – notably applied to a manmade, controllable environment – are directly responsible for the depth and breadth of our current unfavorable cybersecurity situation. Yet, despite our design choices, network security professionals routinely are being asked to do the impossible in the form of building trusted, impenetrable, dynamic, interoperable networks out of untrusted components, within untrusted environments, using untrusted supply chains, that rely upon untrusted vendors and untrusted users.

We would do well to take Darwin's findings to heart, and begin to use our public/private partnerships in part to explore alternative models in which hardware, software, protocols, and policies are adapted to better suit the wide range of global use scenarios relating to security and privacy. For example, it is hard to imagine that to this day computers that are used for transmitting classified information (or for enriching uranium for that matter) can accept the same USB thumb drive and fall victim to the same malware as a common computer in a public library. My regular car cannot even accept a diesel pump at the gas station.

We should establish public/private partnerships to determine whether trusted networks require a combination of distinct design elements, to include enhanced identity management, maximized intrusion detection and attribution capabilities, and prioritized actions to locate and penalize bad actors. Similarly, uniquely defined networks operating internationally, with common Terms of Service, might assist nations (and perhaps even non-governmental organizations) agree on principles for transborder access to data in order to prevent imminent danger to life, limb, or property.

Regardless of the solution space, the international and multi-disciplinary aspects of these considerations require substantial government leadership and private sector initiative (similar to the origins of the Internet itself.) To get started, we just might find that the critical infrastructure networks that are in need of the greatest security are, by coincidence, networks that require the least privacy, providing fertile ground for developing systems that not only are hardened, but that better promote authentication, detection, attribution, and global norms that penalize their breach.

C. We should promote market transparency of security.

Products, protocols and systems should be secure by design and by default, their complexity reduced, and their security capabilities disclosed. For starters, and as expressed in the White House Cybersecurity Commission Report, the Internet of Things is of particular concern, and we should pursue strategies "to achieve security by default in all connected devices and to ensure that the consumer and integrator alike know what security capabilities are, or are not, contained in these devices."

One possible approach is for the Federal government to foster the development and adoption of security labels on products, similar to nutrition labels on food, and linked to a clear rating system. We also must focus on reducing system complexity, in order to push back on the trend, which the Commission observed, that "[a]s the size and complexity of software and computing systems continue to grow, more vulnerabilities are exposed and introduced into environments that are increasingly difficult to manage."

D. We should focus on emerging threats to wireless capabilities.

The 9/11 Commission famously reported its belief that the 2001 terrorist attacks revealed four kinds of U.S. Government failures: "imagination, policy, capabilities, and management." Although the government undoubtedly recognizes the need to be predictive and preventative in the area of security there is insufficient collaboration to counter the vast emerging risks presented by purposeful interference.

Many of our nation's essential functions are highly dependent upon wireless communications across the electromagnetic (EM) spectrum. The disruption of GPS location and timing information in and of itself could have cascading effects on the synchronization of computer networks (to include those responsible for financial transactions), vehicle tracking, coordinated movement of people and cargoes, law enforcement offender tracking, surveying, precision agriculture, and a host of other disparate services. Additional disruption capabilities, such as through radio frequency jammers, could create "quiet" zones around wireless networks and end-users, preventing the transmission of vital communications from reaching their intended recipients.

DHS seems particularly well suited to lead an effort that coordinates actions across the government and with the private sector to better detect, collect, centralize, analyze, and respond to purposeful interference events. Strengthening public/private partnerships to address these and other emerging threats would further reduce the cyber risks to our critical infrastructure.

E. We should develop and share better metrics.

As the White House Cybersecurity Commission Report expressed, "Most current efforts to measure cybersecurity effectiveness focus on the actions taken by an organization, rather than on those actions' effectiveness." The Commission therefore recommended the establishment of a Cybersecurity Framework Metrics Working Group to help address that gap, and recommended that "NIST should provide fact-based metrics to establish whether and to what extent use of the Framework is effective." These points cannot be emphasized enough. We currently are spending billions of dollars on projects for which the value proposition is unknown, and we likely are losing fleeting opportunities to better address the risk.

F. We should promote legal certainty and harmonization

Regulators also should get their respective acts together by harmonizing their rules around common metrics-based cybersecurity principles, as well as with one another, and by producing cost-estimates of adequate compliance schemes. Congress should favor national approaches to Internet privacy and cybersecurity over the current patchwork of state-by-state laws, which introduce cost, legal uncertainty, and transactional delay to interstate and international commerce.

The United States as a whole should then promote international standards that foster security, privacy, and interoperability in ways that make it easier for businesses to innovate and operate with certainty across geopolitical boundaries.

VI. Conclusion: There is Room for Optimism, If We Change Course.

I am convinced that the cyber threat is an existential threat that challenges our democracy and significantly alters our nation's potential. I am convinced that how we rise to the cybersecurity challenge will determine whether our nation's best days are ahead of us or behind us. I am convinced that we currently are going in the wrong direction and that, if we keep doing what we are doing, the overall cyber threat against our country will continue to grow to unsustainable levels.

At the same time, I am convinced our downward spiral is not inevitable and that we can improve our security considerably. However, doing so will require that we reconsider, rather than refine and redouble, the nature of our efforts.

It is my hope for our future that the blame for, and the costs of, cybercrime, cyber espionage, and cyber warfare, will fall more squarely on the offenders than on the victims, and that in doing so we will achieve greater threat deterrence; that we will call upon those businesses and standards bodies that drive the Internet and communications ecosystem to bring forward and implement internationally orchestrated measures that provide higher level, innovative security solutions for the shared benefit of all technology users, and that we readily pay the private sector to do so as a key profit center for them; and, that we build more rigor and transparency into hardware and

software security functions, to enable sophisticated purchasers to use market forces to drive more secure product development.

Ultimately, it is my hope that businesses and consumers will benefit from improved, sustained cybersecurity at lower costs and with less user responsibility; and, above all, that our nation will remain secure so that our country's best days still lie ahead.

Thank you for the opportunity to testify today. I would be happy to answer any questions you may have.

Statement of Brandon Valeriano, PhD

Donald Bren Chair of Armed Politics, Marine Corps University
Reader in Digital Politics, Cardiff University
Adjunct Fellow of Cyber Security, Niskanen Center

"The International Cyber Conflict Threat Landscape"

Cyber Threats Facing America,
Testimony before the United States Senate Committee on Homeland Security and Government Affairs

May 10, 2017

Cyber Conflict Dynamics[1]

Cyber conflict represents a long-standing threat to the nation and the international system.[2] First clearly articulated in the 1990s, there is evidence of ongoing cyber conflicts at a proliferating rate since at least 2000 (see Figure 1). The cyber challenge is neither new, nor revolutionary. Instead it is a continuation of international rivalries and grievances now also fought in cyberspace. By understanding active cyber operations in their proper context, which is as methods of coercion, we can seek to understand how the international cyber threat landscape works, what challenges will continue to proliferate, and how to fight back by establishing resiliency in cyberspace.

The cyber security threat arena is undoubtedly a critical vulnerability area for all states, but it also represents an opportunity for the modern nation-state in that cyber capabilities can add to state power and reinforce traditional methods of control. All actors in the international system must confront the challenge of digital connectivity, conflict aided by cyber technologies, and the weaknesses exposed by networked infrastructure.

The problem with the cyber security field is that it often takes a micro view of events, focusing on such famous incidents such as the Russian hack during the 2016 election, the Stuxnet operation against Iran, and the Russian attacks on Estonia in 2007. The cyber security landscape is much more than these high-profile incidents. There is a proliferating universe of cyber security incidents, threat actors, and perspectives that portend escalating danger in the domain. Yet, we also witness few incidents that involve escalation and there is rather limited severity evident in each cyber incident to mark this arena as a critical threat to international stability.

Taking a step back and seeking to understand the landscape as it currently stands can provide critical pathways to meeting the cyber security challenge. Only by understanding the macro picture of cyber security landscape can we articulate policy goals to move forward to meet the challenge. Today, I offer an academic empirical perspective of the macro dynamics of the cyber security field. I will explain the construction of cyber threats as coercive tools, the behavior of major threat actors, and pathways toward ensuring that we have a stable cyber future devoid of escalation and overaction, which are common in technology frameworks. While dangerous, the cyber threat landscape also exhibits genuine stability, aided by complexity and restraint which leads to careful action in cyberspace. This relative stability

---

[1] Much of this testimony draws on two research publications, Valeriano, Brandon and Ryan Maness. 2015. *Cyber War versus Cyber Realities: Cyber Conflict in the International System*. New York: Oxford University Press and Valeriano, Brandon, Benjamin Jensen, and Ryan Maness. Forthcoming. *Cyber Coercion: Compellence in the Digital Domain*. New York: Oxford University Press.

[2] I generally avoid the term Cyber War since it is hyperbolic and not at all indicative of the current cyber conflict situation. For there to be war, there needs to be violence and death. We have yet to see this in cyberspace therefore the preferred term to describe ongoing cyber operations is cyber conflict. I also avoid the term cyber-attack since it is so overused to the point that the term is meaningless and can describe any digital attack. Instead we use the term cyber incident and cyber dispute to describe specific cyber operations. See Valeriano, Brandon and Ryan Maness. 2014. "The Dynamics of Cyber Conflict between Rival Antagonists." *Journal of Peace Research*. 51(3): 347-360

and restraint, however, is often in danger of being upset without maintenance, attention paid to individuals as they interact in cyberspace, and the overestimation of potential cyber effects from offensive actions. Make no mistake, political warfare aided by cyber technologies is a threat to the nation-state, but how we react to it (or in some cases overreact), can harm the evident stability displayed to this point.

The Universe of International Cyber Threats

There are three key threat actors in cyberspace: states, non-state actors and state-based proxies, and cyber criminals. Each has distinct motivations, abilities, and limitations. It makes little analytical sense to lump them together into one unified cyber threat actor. Behavior varies by actor; motivations are driven by geopolitics, funding sources, or economic gains, and also level of aggression and willingness to cause chaos.

Here I speak mainly of state actors and state-supported cyber proxies. These actors are the most dangerous, prepared, funded, and capable. While there is a willingness of non-state cyber forces, especially terrorists, to use physical force as directed by cyber methods, there is no evidence any of these actors are capable of violent harm. Their limitations in cyberspace generally constrain them to using cyber tools to cause light chaos or as a method of recruitment and promotion. Criminal actors are less likely to seek to cause physical harm and generally are motivated by peer group status or economic gain. The danger is when these forces become skilled enough to be recruited and supported by state-based actors in exchange for protection from prosecution and formal accusation, a practice that happens quite often autocracies.

State Based Cyber Conflict: Who fights Whom

Perhaps the most compelling question in the cyber security arena is who is really fighting whom? The perception by many is that digital frameworks allow small powers to challenge major powers. This conjecture is made without evidence and we see few events where small powers seek to punch above their weight (most of these incidents involve North Korea or Iran). Instead, most digital contests are between relatively equal powers such as Pakistan and India, or South Korea and North Korea. We find that cyber conflict is mainly a regional phenomenon, the exception being incidents involving the United States given our global reach and interests.

The idea that the cyber domain allows non-state actors and individuals to challenge states is false. Of course, there will be breaches and intrusions, but this is mainly because the defender has not properly tested its possible avenues of attack and ensured that the systems they built are relatively secure. This is to be expected, as the internet has not been a key pathway to stability as currently composed. The internet was initially constructed to be open, not secure. New avenues such as cloud computing and blockchains are enhancements on old designs, but still introduce weaknesses into the system leaving all digital systems vulnerable.

The cyber domain, if it is to be considered a separate domain of conflict, generally allows state-based actors to continue with normal influence operations but also operating with plausible deniability. Attribution of state-based actors is not difficult in cyberspace. There are many indicators beyond language and IP addresses that might pinpoint digital aggressors. The real issue is with responsibility, who authorized the operations? Actors such as Russia cover digital aggression through compromised or complacent criminal actors. China either

uses its complex network of Communist Party-approved third parties as well as various groups in the People's Liberation Army (PLA). It can therefore become difficult to figure who really authorized what, which is exactly the advantage of cyber operations that our adversaries have been exploiting. It is not much of a secret who is doing what based on target, intent, and method, but it is difficult to establish responsibility for legal or conventional responses according to international law and norms. This is a problem than can only really be solved through on the ground intelligence assets in aggressor countries, in addition to digital forensics.

Cyber conflict has not ushered in a new way of conducting international affairs, only a new way of communicating threats and undertaking aggressive operations. There are no new digital avenues of conflict, we have yet to witness a cyber conflict where the genesis, fight, and resolution all occurred in cyberspace. Cyber conflict only extends traditional rivalry contests over common issues areas (control of space and place, resources, nationalism) to the digital domain.

Cyber methods are typically used as a method of coercion. Within coercion there is either deterrence, which is a status quo operation to prevent something from happening, or compellence operations which seek a change of behavior in the target. Deterrence in cyberspace is problematic as it depends on credibility, the ability to withstand basic attacks, communicating threats clearly to adversaries, and the willingness to display and use cyber weapons. Compellence is more common since it is thought that cyber operations can be a force of leverage to compel an adversary to change behavior. States then utilize cyber tools to create leverage against the opposition and change strategic calculations. The problem is that evidence of behavior change in cyberspace is rare.

Types of Cyber Conflicts: Disruption Operations

Cyber disruption operations are short term harassment operations meant to influence the opposition but at the same time, expend minimal effort and require few resources beyond coordination. Seeking to achieve outsized effects through simple operations, these attacks have short term time horizons and represent targets of opportunity against the opposition. The goal is to harass and provoke a change a behavior in the target through the simple escalation of costs associated with continuing to operate in the cyber domain.

Most these cases are website defacements and distributed denial of service (DDoS) operations, which flood servers with requests for information and result in denial of access. Simple email phishing operations that reveal passwords can also be considered disruptions. With basic protections, government associated targets can be hardened to withstand such attacks, but civilians and individuals remain at risk given their general lack of protection and proclivity for making basic mistakes. The recent Google Docs attack that spread quickly through email systems is a common example of this basic level attack that can wreak havoc on unsecure systems.[3]

The goal of these operations is to cause chaos and escalate costs on civilians and other targets to force the state to act. The Russian attack against Estonia in 2007 was an example of such an attack. Little damage was technically done but the Estonia did disconnect internet

[3] https://www.theverge.com/2017/5/4/15544608/google-docs-spam-phishing-email-hack-secure-account (accessed 5/7/2017)

services for a few days as a precaution. While this was traumatic for digitally advanced state, it also caused no long-term damage and did not result in capitulation to Russian demands.

Types of Cyber Conflicts: Espionage Activities

Espionage operations are long term activities meant to manipulate information. The goal is either to take, steal or alter information the target has in order to alter the bargaining situation between two parties. One sure way to alter the positional and status dynamics between two states is alter the information one side has on the other, with more access and information leading to greater ability to escalate costs on the opposition by leveraging vulnerabilities.

Espionage activities can also lead to one state adopting stolen technologies to reduce the perceived power gap, largely the goal of Chinese cyber activities. Chinese espionage is motivated by the desire to catch up to the United States in technological and military capabilities, and the large-scale theft of state secrets and intellectual property is a useful shortcut for this goal.

Russian espionage, on the other hand, is focused on the theft of information from private entities and then publishing this information for the public with complacent whistleblowing sites such as Wikileaks. This is technically data manipulation where information is both stolen selectively and also presented in such a way to highlight perceived flaws in the opposition. Altering information and presenting it in a biased manner is the more insidious danger that arises from cyber espionage because it can destabilize the foundations of a state.

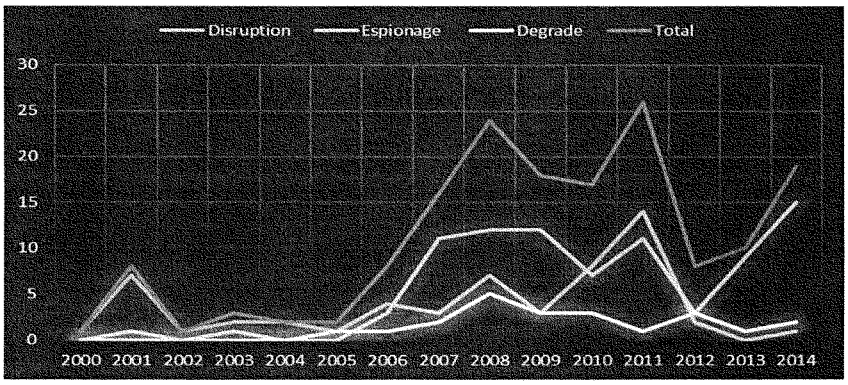


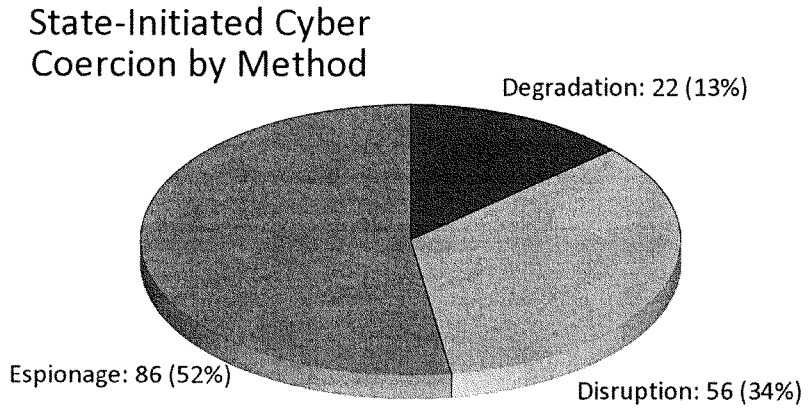
Figure 1: From *Cyber Coercion*, Forthcoming

Types of Cyber Conflicts: Degrade Campaigns

Cyber degradation campaigns are potentially the cyber operations with the highest impact, but they are also the costliest, most time intensive, and riskiest. By seeking to degrade the opposition's ability to maintain control of operations, destroy opposition targets, or sabotage procedures, degrade operations seek to punch at the heart of the target to escalate

costs in order to provoke a change in behavior. Such operations have likely been conducted against nuclear facilities (Stuxnet), resource production faculties (Shamoon), and strangely enough, movie studios (Sony Pictures).

These operations are the most famous cyber operations on record but they also attract a disproportionate amount of attention given that they are so rare. As Figure 2 below demonstrates, these coercive cyber events are the rarest of the three categories of cyber coercion. Only 13 percent of known cyber activities overall could be classified as degrade operations, with Figure 1 demonstrating no particular increase in use through time. Our ongoing research also demonstrates that while degrade operations can be effective, they mostly are useful as counterespionage operations. Success rates hover at around 30 percent with is about on par with conventional coercion efforts.



Cyber Threat Actors

Russia

Russia has demonstrated no great capability in cyber operations. As opposed to media coverage, it often shocking how low tech their techniques are (email spear phishing, tab spamming), and they often fail more than they succeed. However, their evident willingness to conduct political espionage and utilize information warfare tactics is a troubling aspect of Russian behavior for the United States and the West. Russia behavior is paradoxically norm breaking but also simple and near effortless.

In many ways, it seems that Russia is trying to remain relevant and active on the international scene when they have few capabilities to challenge the dominant powers conventionally. Long since caught in a quagmire in Ukraine and unable, so far, to gain traction as they attack European elections, Russia instead seems to be stuck sending cheap

signals towards the digital sky, crying out for attention.

A cheap signal is a method of offering viewpoint that seeks to suggest discontent, but is balanced by the attackers relative inability or lack of interest in pushing the issue further. The methods utilized require little resources, strain, or action. Instead, by using disruption methods, Russia seeks to do the most they can with little effort, akin to flicking at a mosquito with a finger rather than a swatter. The definition of "easy" in cyberspace is to try to affect elections and opinions through email dumps, botnets, and other coordinated influence measures that can be timed and automated.

There can be little doubt that Russia has actively sought to influence elections in the United States, Germany, and most recently France. We cannot normalize this practice, and assume it will continue to happen for any election in the Western world that does not match Russia's grand strategic ambitions. The cyber system we have created enables this process where an aggressor can sit back at home and seek to alter perceptions through simple email dumps and propaganda campaigns.

The only action that can effectively stop the practice is to ignore the curated and biased information released, designate electoral systems critical infrastructure systems, and seek to promote a norm of general revulsion to the practice of releasing private information. This is not to say those attacked do not bear some responsibility, and their systems need to be secure almost to the point of inconvenience. Potential victims also need to accept that digital communications are not private, and active protection needs to be arranged between government cyber operatives and potential political targets much in the same way Secret Service protection is granted to serious candidates.

Challenging Russia on the digital frontier is needed to prevent them from gaining disproportionate influence by utilizing cheap tactics. These tactics can be used right back against them, as the West can employ their own digital armies to counter disinformation with accurate information. But escalating beyond this is needlessly antagonizing, since they seem to the happy enough to continue with a path of least resistance. The Germans have suggested that Russian servers could be wiped out in response to incursions, but this would only invite the same by Russian operatives leading to a spiral of escalation. Even responding with Western troll armies presenting accurate information is potentially norm inducing and blurs the lines of state responsibility.

It must be remembered that Russian influence operations have been attempted in Ukraine in 2014, United States in 2016, and France in 2017 with no discernible effect on actual election outcomes. Each time they failed and generally provoke a reaction that both hardens the target for future attempts but also alerts the next target of the likely incoming attacks. The best way to counter Russia influence is to protect current systems that might provide information and seek to counter their disinformation campaigns with accurate information.

China

China employees thousands of hackers and by sheer numbers we would expect a much better yield of their efforts. Instead they seem perfectly content with probing networks and stealing information rather than outwardly expecting to achieve influence through cyber techniques.

China has entered into a cycle of probe, penetration, and retrenchment with the United States. Every few years the United States launches a successful counter-espionage operation that either halts China or forces them to reset their efforts because of the attention placed on them. The United States has also used criminal indictments to decent effect to compel China to change behavior. But this should be countered by the ability of the United States to drive behavior through simple diplomatic exchanges and meetings, such as the agreement on cyber norms between Presidents Obama and Xi in 2015. This led to a cooling off for Chinese espionage operations that has yet to resume.

Countering Chinese cyber espionage is needed but the first obvious step is to shore up Western weaknesses first, third party contractors and weak individuals (insider threats) willing to be bought are the prime vulnerabilities in the United States. As long as the United States has weak links domestically, it will continue to be probed and infiltrated by China.

China does maintain the ability to contest international decisions and actions that they feel go against their interests. They recently have been identified as seeking to infiltrate THAAD missile networks in South Korea.[4] The decision to provide these missile systems to South Korea was obviously contentious and their method of protest and preparation includes cyber infiltrations.

China also maintains active measures to sway public opinion and protest decisions that go against their quest of positive territorial acquisitions in the South China Sea. When operations happen that go against their interests, China can direct its operatives to protest digitally but so far has generally restrained their own activists. These measures are rather tame and to be expected, given the priority these issues have in China.

Iran

Iran is thought to be a serious and sophisticated cyber actor but evidence suggests the contrary to this conclusion. The Shamoon attacks on Saudi Arabia's Aramco systems were destructive, but did not impede operations or wipe out critical information. Likely launched in response to the Stuxnet operation, it also telling that the response by Iran was not to attack the alleged perpetrators directly, but to go after an ally indirectly, Saudi Arabia.

Recent attacks on Israel have been reported as another telling aspect of the sophistication of Iranian cyber operations, but the reality is that the state was using released malware from the Shadowbrokers info dumps and spear phishing techniques. Similar attacks on U.S. networks have failed more often than succeeded as well. To argue that these are sophisticated attacks betrays our ability to judge information and impact in cyber security operations.

Ongoing attacks on industrial and financial networks have recently been dubbed Shamoon 2.[5] Reports highlight that the new version of the operation builds on the 2012 attacks on Saudi oil networks and reuses 90 percent of the known code. This is not a highly new or original operation, but a continuation of old methods because targets are slow to

---

[4] http://thediplomat.com/2017/04/china-based-hackers-targeting-south-korea-over-thaad-report/ (access 5/6/2017)

[5] https://www.scmagazineuk.com/multiple-groups-likely-collaborating-on-shamoon/article/653411/ (accessed 5/5/2017)

update their systems and patch known vulnerabilities.

The main danger from Iran, just as it is in terrorism threat vector, is the high probability that Iran will use proxy actors to attack Western targets. Enabling these actors, one group being called the Syrian Electronic Army, might be dangerous if Iran was to transfer technology to these groups who could then use known vulnerabilities in their operations. But for now, Iran seems content to harass American allies, probe American networks, and reuse old malware to attack unprepared targets.

Steps Forward to Restore Resilience

Moving forward to protect the nation requires both the understanding digital threat projections and the recent history of cyber interactions that would match theory with reality. Cyber conflict is not generally new, distinct, or revolutionary. Instead it is a mostly banal continuation of international aggression through digital means. The manipulation of information is the most dangerous aspect of cyber conflict and introduces a new style of political warfare, but we should be not be shocked or unprepared to meet the challenge of cyber conflict.

Education on this recent history is clearly needed, but we often are distracted by the latest attack of the month rather than surveying known past actions. This represents a divorce with typical conflict scenario building where future threats are articulated based on past practices and behaviors. Instead, in the cyber world, we make up new threats, options, and opportunities with little awareness of what has come before or simply just react to the latest news.

Holistic Cyber Education

In education and analysis, we focus mainly on cyber actions through technological frameworks and fail generally to enable a general understanding of the cyber threat which would put it in its proper context. That would require building a cyber conflict history background, understand the political motivations for international cyber actions, understanding how rivals engage in conflict, diving into the psychology of cyber behaviors and threat perceptions, knowing the sociology of cyber threat actors, and finally, understanding the biological implications of our networked reality.

As we move forward and think about building a cyber academy on par with West Point or a separate cyber agency, we must remember the general holistic universe of cyber threat actions. This requires us to move beyond just technical understanding of the cyber threat. To do this we must encourage a diverse set of research on cyber issues that is generally not enabled through current National Science Foundation frameworks. Accreditation of cyber education teams by the NSA focuses purely on technical specifications and there is no broader framework to encourage the political, policy, historical, sociological, and biological understanding of cyber security. We will fall behind as a nation until these frameworks are encouraged and maintained.

With the focus on education would also come a much-needed reconceptualization of who operates our cyber security systems. Diversity is a key challenge in these networks as the groups who articulate and monitor critical systems tend to lack diverse perspectives. Diversity is critical in that outcomes are enhanced through diverse thought processes. We

would also need to think about how different types of people access and operate critical systems. The need to expand the cyber work force to include women and ethnic minorities becomes a critical priority. There is no tougher challenge in cyber security than diversifying who is hired to maintain networks and pass on the skills of the past to the future.

The Human Element

In attack after attack we witness the key element of weakness is the individual. While the opposition States are undoubtedly malicious actors, their success depends on mistakes and ill-advised behavior of the target. The step in ensuring a secure cyber future would be to focus on protecting the individual and ensure better behavioural process.

Damage in cyber security is often our own making because the greatest impact is psychological rather than reality-based. The overreaction and fear evidenced in reactions to cyber incidents drives the behavior of states seeking to respond to provocations. But can we really respond without shoring up the defensive frontier first? We must first look internally before we blame others for malicious cyber activities.

Basic cyber hygiene is needed, and this extends to the typical recommendations that have yet to be instituted widely: two factor authentication, finger print access, encryption of important machines, and secure card access are all easy adoptable measures that we can do prevent even the most basic attacks. But we also have to take a step back and re-examine processes, such as the high probability that people will click on links because they believe they come from trusted sources, weak web protection in visiting web sites that seek to harvest data, and the high probability that secure systems are accessed from unsecure locations like airports and hotel networks.

As a nation, we have done little at the societal level to reconceptualize how individuals respond to cyber threats. While is there is a much-needed, national conversation taking place regarding the stability of the critical infrastructure network, we have yet to begin a conversation about how re-established personal networks between individuals that can withstand the sure to come cyber-attacks of the future. Resiliency is a national project that requires both awareness of the coming threat but also a fair assessment of the extent and limits of cyber harm.

Cyber Security for Whom?

Just who are we seeking to protect? Moving forward and seeking to protect private enterprise is potentially dangerous in that it inserts the state in transactions between private entities. There is little conception of trying to protect the average citizen in cyber security and this remains a core problem with the field.

There are constant probes and intrusions in government systems, they have remained remarkably resilient in the face of cyber challenges. There has been no death and destruction in the domain. Any frame where this would happen generally would occur under the situation of massive war between great powers, hardly the scenarios articulated by cyber security practitioners. What is remarkable about the cyber domain is that despite its existence for over 30 years and during the ongoing wars between a plethora of actors, we have seen few instances of outright digital violence between states. That digital violence between states is

rare might suggest that we have gotten this era of cyber conflict wrong. It is much more stable, constrained and restrained that generally imagined. This would then relocate the danger towards the average citizen rather than the state as a whole.

Moving forward we need a holistic view of the cyber challenge. It cannot be studied as purely a technical domain, but as a domain that critical requires the consideration of the international conflict situation, the motivations of cyber criminals, the psychological impact of the cyber threat frame, the ethics of cyber action, the dynamics of coercion in security frameworks, and finally, the biological impact on human society. Moving beyond the simple war framework would expand just who we seek to protect and what we endeavor to stabilize as we progress with digital communication.

Active measures to defend the nation and go on aggressive attacks are often ineffective and counterproductive outside of counter-espionage operations. There is very little utility in cyber operations to compel the opposition to behave as expected or desired, as these operations might work, but they are costly and enable further digital malevolence by breaking down norms against cyber harm. Cyber deterrence is non-existent and an empty buzzword devoid of real meaning. Proactive measures to ensure a positive cyber future are critical. They include the focus on defensive measures, restoring resiliency in the civilian population, hardening popular targets, and seeking to better understand the process of cyber conflict.

We must strive not to normalize malicious cyber activities. Being hacked is not the price of running a government in the modern international system. It is a perverse outcome of building a structure and system that has little concern for security. Preventing these relatively rare occurrences of cyber violence from becoming common, accepted, and effective is the challenge we face moving forward. The consequences can be drastic in that these tools do not enable liberation technologies, but instead allow moderate reckless powers to seek to compete with stable great powers, allow states to leverage cyber tools to harm activities, protesters, and journalists, and generally seek to further destabilize the international system.

While we have not yet seen the advent of real cyber war and are unlikely to, this does not mean that our future will not be devoid of cyber conflict. In fact, it is becoming quite common and expected as methods of harassment and espionage, basically what Kennan called political warfare so long ago. This active process utilizing cyber tools for attempted coercive effect short of war will only continue to jeopardize our digital futures as cyber technologies fail to become a force for peace and stability but instead symbolize instability and recklessness.

Testimony of Kevin Keeney
"Cyber Threats Facing America: An Overview of the Cybersecurity Threat Landscape"
May 10, 2017

My name is Kevin Keeney and I was asked to testify before this committee due to the multiple hats I wear in the Cyber Security ecosystem. I'm here representing myself and my opinions are mine alone. I work full-time for Monsanto as the Director of their Cyber Incident Response Team (CIRT). My team there is made up of ten highly qualified cyber analysts on two different teams, one dedicated to the function of Cyber Security Monitoring (reactive) and the other to the function of Threat Hunting (proactive). I also work part-time for Missouri National Guard at the Chief of Operations for MOCYBER. The MOCYBER team is made up of 39 Army and Air National Guard members. We are broken down into three teams: A notional Mission Defense Team (MDT) with 10 positions that MG Danner has authorized to be created with no manning or funding, a Defensive Cyber Operations – Element (DCO-E) with 10 positions that has been part of the Missouri Army National Guard since 1999, and a partial Cyber Protection Team with 21 positions that will officially begin to form on 1 October 2017. Just like the notional MDT, MG Danner has allowed the positions to be filled in advance, understanding the threat we face as a nation. A threat which will not wait on our nation's current timetables.

I would like to thank the Committee for considering the issue of Cyber Security and the threats we face as a nation. I am particularly happy to hear that the committee members see an opportunity for the National Guard to bridge the gap between the public and private sector. I am humbled that you have invited me here today as a witness before the panel.

My goal is to provide some information about MOCYBER, and what it has been doing for the State of Missouri and nation. In addition, I hope to share some insights about the threat actors I am facing in my two roles. I am also aware that the panel is interested in discussing the Cyber workforce.

In the summer of 2009, I re-joined the Missouri National Guard with the goal of building the Missouri National Guard's Cyber capability. MG Danner was keenly interested in this effort, and empowered me and others to recruit and retain the best and brightest. MOCYBER has had its share of success and I believe it can be repeated at scale. Here are the two tenets that have enabled us:

1. Remember the "Special Operations Forces Truths"
    a. Humans are more important than Hardware
    b. Quality is better than Quantity
    c. Special Operations Forces cannot be mass produced
    d. Competent Special Operations Forces cannot be created after emergencies occur
    e. Most Special Operations require non-SOF assistance

2. Build a culture of Innovation
    a. In the Military problems abound
    b. Think big
    c. Start small

These tenets are what enable MOCYBER to recruit and retain people willing to travel from seven states to drill with us. They enable an environment where enlisted and officers collaborate as technical equals, freely and openly, to solve complex problems. This freedom to operate led my team to create ROCK (http://rocknsm.io), an open source project that has attempted to address the problem of Military personnel showing up at a Critical Infrastructure or Key Resource (CI/KR) provider to lend a cyber hand. In short order, ROCK has been adopted in the commercial sector, active duty military, and multiple federal agencies. All of this has been done with zero funding from the U.S. Government. It has been done on my soldier and airmen's personal time. Their passion to defend the nation is unmatched.

The threat actors I face in my corporate life are online extremists (hacktivist and eco-terrorists), industrial espionage (Nation States), and the occasional criminal. Since leaving the public sector in 2011, I've been surprised by how much I encounter Nation State actors in private industry. The challenges in dealing with extremists and criminal threat actors can be dealt with in most corporate environments through the use of traditional security countermeasures. However, with Nation State threat actors we as a country are far behind because we are defending against them the same way we do other threat actors while they are conducting warfare. It also goes well beyond just hacking and into more disciplined, strategic, and carefully curated espionage- we have nations playing the long game.

My hope is that this committee, Congress, and our country as a whole can start openly embracing the National Guard's role in defending the nation through closer integration of USNORTHCOM and the Department of Homeland Security. The nation's largest threat is to the private sector, not the public. The National Guard is uniquely postured to bring highly skilled operators and analysts to bear on both sides. The government and military need to move beyond trying to secure itself and move into an active and supporting role in defending America, just as it does in all other war fighting domains. We need to remove the seams between the military, government, and the private sector. The Internet-at-large doesn't work this way--fencing off public and private sectors--and we must defend it as it is, and not how we are organized.

Although the current Cyber Surge by the U.S. military is going well, it doesn't go far enough. It is not flexible and dynamic, which is specifically what is needed to address the problems we face. Recruiting, training, and retention all fight against each other which leads to a constant and chaotic talent churn. In addition, it has completely left out the most critical element of our society- the private sector which provides the tax base. This is where the wealth of our nation exists. The National Guard has, since before the origins of our nation,

provided for the defense of it communities. Let's reignite that strength that comes from within our communities.

My Specific recommendations:

Write legislation that creates and funds a new uniformed service called U.S. Cyber that is responsible for security of our Internet, not just .mil or .gov, and consolidate all cyber personnel, equipment and missions under it. This will enable a single organization to provide the needed focus on recruiting, training, doctrine, retention and care for its service members. U.S. Cyber should be made up of no more than 50% active, and no less than 50% reserve forces. Transitioning between the active and reserve should be as simple as applying for an opening and being accepted. The ability to move from Title 10/18/32/50 seamlessly is essential. This will achieve what all other warfare domains have- unity of command and unity of effort.

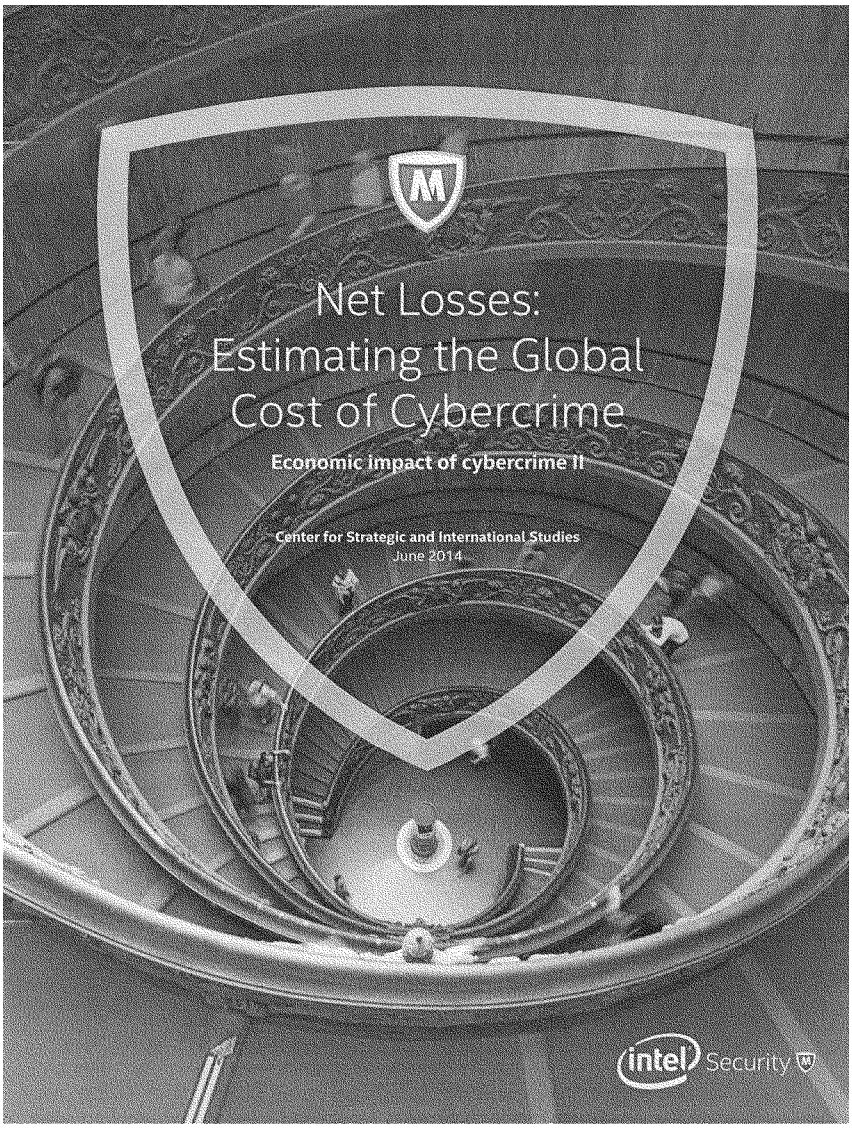
Effects achieved through the creation of U.S. Cyber:

1. Standards for recruiting and retention can be specifically tailored to the needs of U.S. Cyber service. Mental stamina is paramount, but being a double leg amputee has no impact on a potential recruit's ability to be trained.
2. U.S. Cyber service will be able to select from a broader sector of the population, which will enable more stringent selection for mental flexibility, problems solving skills, and aptitude.
3. U.S. Cyber can apply resources at tactical, operational, and strategic levels as needed without fighting for resources across multiple services.
4. Cyber effects can be provided to the entire nation to include the private sector, other uniformed services, intelligence communities, and National Command Authority in a synchronized, de-conflicted, and efficient manner.
5. The study of cyber as a warfighting domain and creation and testing of its doctrine would not be narrow as it is today.
6. New insights into our capabilities, our adversaries, and how they relate would be gained, as well as a more complete understanding of the problems that still need to be solved. Proper resources can then be advocated for and applied to the most important issues.
7. Deduplication of cyber training schools across all uniformed services. This cost savings would enable the creation of world class cyber ranges and realistic opposition forces.
8. Better trained cyber operators that can conduct fluid and full spectrum warfare, not just complete a checklist.
9. In the long term, significant cost reductions can be achieved through deduplication of facilities, personnel, and training.

While there is much to gain from the creation of a new uniformed service, there are some areas of focus that would need to be addressed:

1. In the short term, other strategic programs would receive less or zero funding. In the long term, in-fighting between the services about cyber missions would be reduced. This saved energy could be better used furthering the warfighting domain they are responsible for.
2. Possible degradation of cyber capabilities during the transition of cyber resources to U.S. Cyber.
3. Could temporarily weaken other instruments of national power, as information is known to be the underpinning for diplomatic, military and economic power.

In summary, the creation of U.S. Cyber could close the cyber capabilities gap more quickly than the current strategy. We need to build the foundation for a future that will most certainly include more, and not less, reliance on information dominance. The conflicts we have recently witnessed in the Ukraine and the South China Sea are well-executed examples of hybrid and full-spectrum warfare. If we are going to win against a peer, or near peer adversary, we must build a unified cyber force that can fight and win as an equal stakeholder in the battle. It is essential that we begin acting upon what we know is happening within our borders- the rampant theft of the Intellectual Property created and owned here in the United States. As Americans, we have the duty and honor to defend that. Thank you.


Net Losses:
Estimating the Global
Cost of Cybercrime
Economic impact of cybercrime II
Center for Strategic and International Studies
June 2014
intel Security

Contents

Cybercrime is a growth industry. The returns are great, and the risks are low. We estimate that the likely annual cost to the global economy from cybercrime is more than $400 billion.[1] A conservative estimate would be $375 billion in losses, while the maximum could be as much as $575 billion. Even the smallest of these figures is more than the national income of most countries and governments and companies underestimate how much risk they face from cybercrime and how quickly this risk can grow.[1]

Putting a number on the cost of cybercrime and cyberespionage is the headline, but the dollar figure begs important questions about the damage to the victims from the cumulative effect of losses in cyberspace. The cost of cybercrime includes the effect of hundreds of millions of people having their personal information stolen—incidents in the last year include more than 40 million people in the US, 54 million in Turkey, 20 million in Korea, 16 million in Germany, and more than 20 million in China. One estimate puts the total at more than 800 million individual records in 2013.[2] This alone could cost as much as $160 billion per year.[3] Criminals still have difficulty turning stolen data into financial gain, but the constant stream of news contributes to a growing sense that cybercrime is out of control.

For developed countries, cybercrime has serious implications for employment.[4] The effect of cybercrime is to shift employment away from jobs that create the most value. Even small changes in GDP can affect employment. In the United States alone, studies of how employment varies with export growth suggest that the losses from cybercrime could cost as many as 200,000 American jobs, roughly a third of 1% decrease in employment for the US.[5]

Using European Union data, which found that 16.7 workers were employed per million Euros in exports to the rest of the world,[6] Europe could lose as many as 150,000 jobs due to cybercrime (adjusting for national differences in IP-intensive jobs), or about 0.6% of the total unemployed.

These are not always a "net" loss if workers displaced by cyberespionage find other jobs, but if these jobs do not pay as well or better. If lost jobs are in manufacturing (and "the main engine for job creation"[7]) or other high-paying sectors, the effect of cybercrime is to shift workers from high-paying to low-paying jobs or unemployment. While translating cybercrime losses directly into job losses is not easy, the employment effect cannot be ignored.

The most important cost of cybercrime, however, comes from its damage to company performance and to national economies. Cybercrime damages trade, competitiveness, innovation, and global economic growth. What cybercrime means for the world is:

- The cost of cybercrime will continue to increase as more business functions move online and as more companies and consumers around the world connect to the Internet.
- Losses from the theft of intellectual property will also increase as acquiring countries improve their ability to make use of it to manufacture competing goods.
- Cybercrime is a tax on innovation and slows the pace of global innovation by reducing the rate of return to innovators and investors.
- Governments need to begin serious, systematic effort to collect and publish data on cybercrime to help countries and companies make better choices about risk and policy.

Estimating global loss from incomplete data

Deciding what counts as cybercrime affects the size of any estimate. Our estimate looks at both direct and indirect costs, and data used that takes into account the loss of intellectual property, the theft of financial assets and sensitive business information, opportunity costs, additional costs for securing networks, and the cost of recovering from cyberattacks, including reputational damage to the hacked company. These additional indirect costs show the full effect of cybercrime on the global economy. International agreement on a standard definition of cybercrime would improve the ability to collect consistent data. That said, even a broad definition leaves out important nonmonetary effects on innovation, national defense, and the long-term competitiveness of both countries and companies.

Our sources range from the German Office for the Protection of the Constitution, the Netherlands Organisation for Applied Scientific Research (TNO), China's Peoples Public Security University, the European Commission, the Australian Institute of Criminology Research, Malaysia's Chief Technical Officer, and estimates by government agencies in other countries and consulting and cybersecurity companies around the world.

Simply listing known cybercrime and cyberespionage incidents creates a dramatic narrative. We found hundreds of reports of companies being hacked.[8] In the US, for example, the government notified 3,000 companies in 2013 that they had been hacked. Two banks in the Persian Gulf lost $45 million in a few hours.[9] A British company reported that it lost $1.3 billion from a single attack.[10] Brazilian banks say their customers lose millions annually to cyberfraud.[11] India's CERT reported that 308,371 websites were hacked between 2011 and June 2013,[12] and the Indian experience is not unique. Simply adding up the losses from the known incidents would total billions of dollars, but this provides an incomplete picture.

Most cybercrime incidents go unreported. Few companies come forward with information on losses. When Google was hacked in 2010, another 34 Fortune 500 companies in sectors as diverse as information technology and chemicals also lost intellectual property.[13] Some of the information on the incident only came to light from documents made public by WikiLeaks. Only one other company reported that it had been hacked along with Google, and it supplied no details on the effect. Similarly, when a major US bank lost several million dollars in a cyberincident it publicly denied any loss, even when law enforcement and intelligence officials confirmed it in private. Few of the biggest cybercriminals have been caught or, in many cases, even identified.

G20 nations suffer the bulk of losses and losses from cybercrime for four largest economies in the world (the US, China, Japan, and Germany) reached $200 billion. Low-income countries have smaller losses, but this will change as these countries increase their use of the Internet and as cybercriminals move to exploit mobile platforms.

The lack of data means that any dollar amount for the global cost of cybercrime is an estimate based on incomplete data. A few nations have made serious efforts to calculate their losses from cybercrime, but most have not. This study assumes that the cost of cybercrime is a constant share of national income, adjusted for levels of development. We calculated the likely global cost by looking at publicly available data from individual countries, buttressed by interviews with government officials and experts. We looked for confirming evidence for these numbers by looking at data on IP theft, fraud, or recovery costs. In addition to a mass of anecdotes, we ultimately found aggregate data for 51 countries in all regions of the world who account for 80% of global income. We used this data to estimate the global cost, adjusting for differences among regions.

There was considerable variation in losses among countries, but this is consistent with other studies (based on surveys of individual companies), which found that companies in different countries lost different amounts per cyberincident, with US companies losing the most. Explaining these variations lies beyond the scope of this report, but one possibility is that cybercriminals decide where to commit their crimes based on an assessment of the value of the target and the ease of entry. The combination of high value, low risk, and low "work factor" (the amount of effort it takes to break into a network) makes cybercrime a winning proposition.

Not all data on cybercrime losses is of the same quality. For example, we found two divergent estimates for the European Union, one saying losses in the EU totaled only $16 billion, far less than the aggregate for those EU countries where we could find data, and another putting losses for the EU at close to a trillion dollars, more than we could find for the entire world. Japan is another interesting case. Credible survey data found that Japanese companies lost on average about half what US companies lost in hacking incidents, but if the rate of loss for Japanese companies is consistent with the rates for the US, China, or Germany, this means that the figure provided to us by officials from several ministries may underestimate the cost of cybercrime by two-thirds. The problem is even worse in the developing world, where most governments do not collect any data on cybercrime at all.

Why some nations lose more than others

One factor explaining why some nations appear to lose more than others has nothing to do with cybercrime. Differences in the thoroughness of national accounting appear to explain the variation. The alternate explanation—that some countries are miraculously unaffected by cybercrime despite having no better defenses than countries with similar income levels that suffer higher loss—seems improbable. National accounts in general need to be updated to better capture the value of intangible goods and services, and better collection of statistics on cybercrime is essential for managing this problem. Work by governments to improve the collection of data on the cost of cybercrime would make a valuable contribution to our ability to make better choices about risk, investment, and policy.

The cost of stolen Intellectual property (IP) is the most difficult to estimate for the cost of cybercrime, but it is also the most important variable for determining loss. Valuing IP is complicated, but firms place a value on IP every day. Countries where IP creation and IP-intensive industries are important for wealth creation lose more in trade, jobs, and income from cybercrime than countries that depend more on agriculture, extractive industries, or low-level manufacturing. Those countries still suffer losses from financial crime and from the theft of business confidential information on production, prices, or crop expectations that could be useful in contract negotiations, but their overall loss will be smaller than that of IP-intensive economies.

Along with the difficulty of valuing IP, other intangible losses are not easily measured. In addition to losses in business and consumer confidence, the effect of cyberespionage on national security is significant, and the monetary value of the military technology taken likely does not reflect the full cost to the nation. Underreporting and the difficulty of valuing IP are the most significant problems for estimating the cost of cybercrime. CERT Australia, for example, found that only 44% of victim companies reported the attacks,[14] and researchers in the Netherlands found a similar rate of underreporting. Many companies either don't know or won't report their losses. There are perfectly sound business reasons for this, but it produces an inherent bias towards underestimation.

A separate set of problems can be traced to the wide gap between what cybercriminals take and what they gain. This is true for both the theft of IP and many financial crimes and complicates estimation for key categories of cybercrime. We all know that a stolen bicycle may be a $500 loss for the owner and a $50 gain for the thief. The calculation is even more uncertain where cybercrime is concerned. Even if we know what was taken, in cases involving personally identifiable information or IP, criminals can't make use of all they have taken. It is harder (in some cases, much harder) to monetize the result of a successful hack than it is to the hack itself. Millions of individuals can lose their credit card data in a single incident, but only a fraction of those affected will experience financial loss.

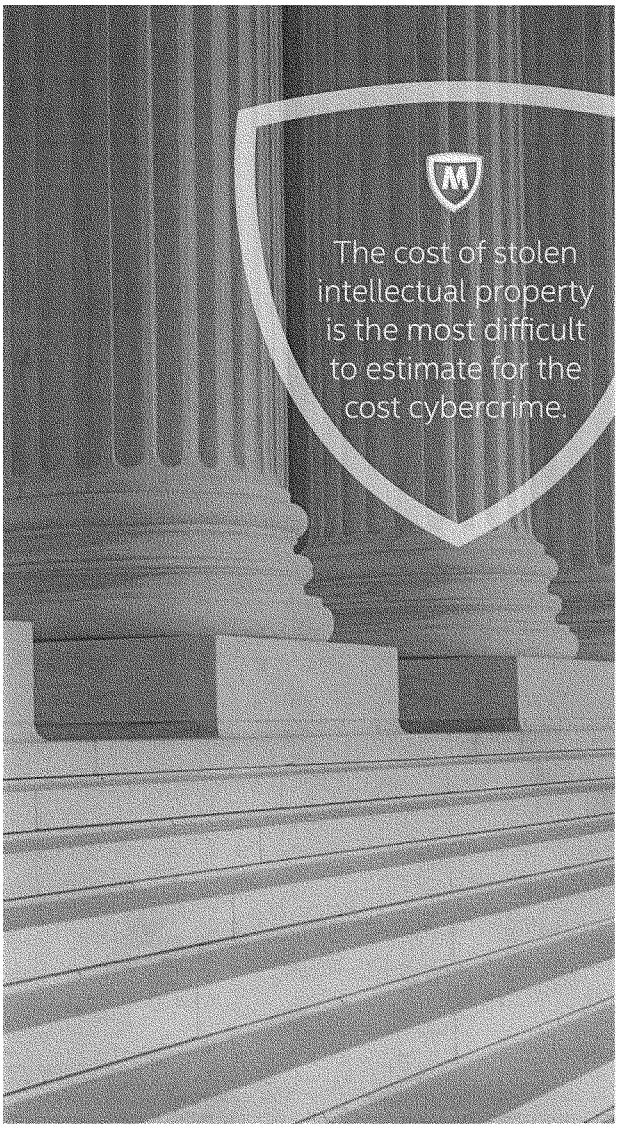
There are wide fluctuations in available national estimates. High-income countries lost more as a percent of GDP, perhaps as much as 0.9% on average. This may simply reflect better accounting, but rampant underreporting means that actual losses may be higher. For developing economies where IP plays a smaller economic role, the losses averaged 0.2% of GDP. The average loss among all countries for which we found data was 0.5% of GDP. Countries in Europe and North America lost more while countries in Latin American and Africa lost less. This may simply reflect better accounting in these countries, but it could also suggest that actual global losses may be higher than our estimate. The disparities we found are explained in part by the fact that the best hackers prefer to target richer countries.

The lack of broadband connectivity also affects the amount of cybercrime—one official we interviewed said that once a country (in Africa) gets broadband connectivity, usually without adequate defenses, cybercrime spikes within a few days. The overall effect of the spike on global losses is limited, as the less developed countries do not generate the bulk of global income, but the regional effect is significant. Wealthier countries are more attractive targets for hackers but they also have better defenses. Less-developed countries are more vulnerable.

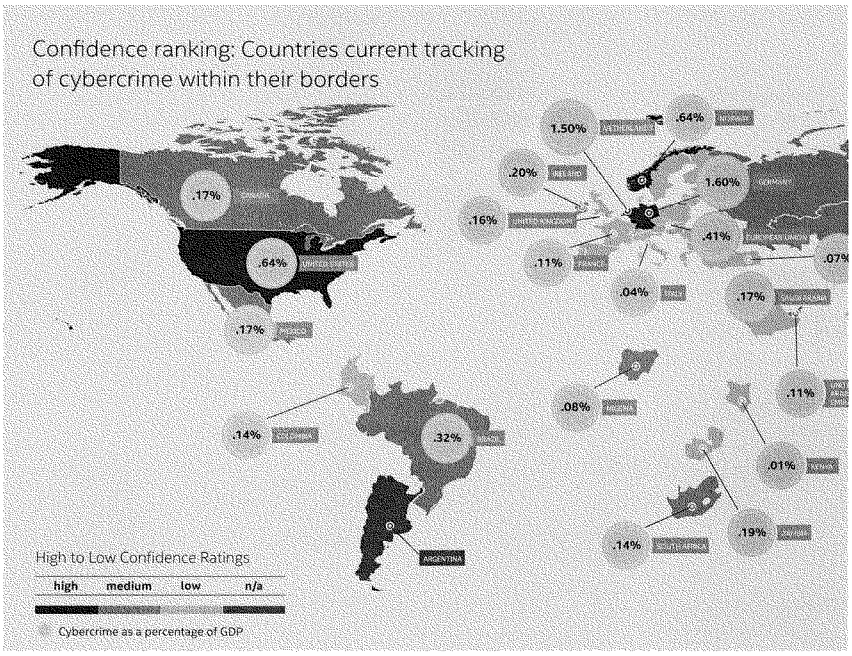
Extrapolating a global loss figure

If we used the loss by high-income countries to extrapolate a global figure, this would give us a global total of $575 billion. Another approach would be to take the total amount for all countries where we could find open source data and use it to extrapolate global costs. This would give us a total global cost of around $375 billion. A third approach would be to aggregate costs as a share of regional incomes to get a global total. This would give us an estimate of $445 billion. None of these approaches are satisfactory, but until reporting and data collection improve, they provide a way to estimate the global cost of cybercrime and cyberespionage.

Given the wide variation in estimates of loss and the difficulty of valuing IP, it is possible that we have overestimated the cost of cybercrime and cyberespionage, but the wealth of anecdotal data on the number of incidents and their effect suggests otherwise. If anything, data on crimes related to the theft of "intangible" sources of value suggest it is more likely that we have underestimated the effect. These intangible costs include the loss of military advantage by the victim country, increased military advantage for the acquiring nation, and the costs to repairing any damage. They also include increased competition for international arms sales, as the acquiring nation's products improve in quality. For example, press reports suggest that intrusion into an American advanced fighter aircraft program led to cost increases in the tens of millions of dollars and delays as software was rewritten or replaced.[15]



Studies estimate that the Internet economy annually generates between $2 trillion and $3 trillion, a share of the global economy that is expected to grow rapidly. If our estimates are right, cybercrime extracts between 15% and 20% of the value created by the Internet.



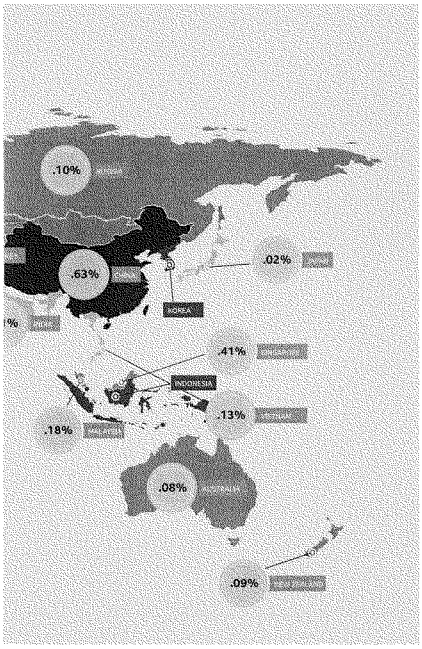
Regional variations

Unsurprisingly, North America, Europe, and Asia lost the most, while Africa lost the least. Income levels are a good predictor of cybercrime, as wealthier countries (or firms) are more likely to be targets—it takes roughly the same amount of work to hack rich and poor targets, but rich targets produce a better return on effort.

There are strong correlations between national income levels and losses from cybercrime. It is not surprising to find that places with more money are more likely to be robbed if they are no more secure than places with less money. The best explanation is that since the risk for cybercriminals is the same whether they go after a rich target or a poor one (small in both cases), they naturally gravitate to the places where value online is highest. This may change as low-income countries increase their access and use of the Internet for commercial purposes and as cybercriminals continue to refocus their activities onto mobile platforms, the preferred source for connectivity in the developing world.

There are important variations within regions. Brazil, Mexico, and Argentina are the most affected countries in Latin America, according to the Amparo Project of the regional Internet Service Provider organization LACNIC.[16] A survey of Brazilian companies found that a third had been victims of cybercrime. Dr. Marcos Tupinamba, a Brazilian information security expert estimates that at least 5% of Brazilian companies suffer monetary losses from cybercrime; the number of attempts is, of course, far greater. In February of 2012, a group calling itself "Anonymous Brasil" launched a denial-of-service attack, which took down a number of Brazilian financial websites, including that of Citigroup.[17] In another attack, Brazilian hackers compromised 4.5 million home DSL routers.[18] Using the hacked routers and careful social engineering, the criminals encouraged users to provide sensitive personal information or to install malware.

Like many computer-literate countries, Brazil's hacker community is active and sophisticated. Brazilian hackers' social engineering skills and the lack of security awareness among companies and consumers explains cybercrime losses in Brazil.



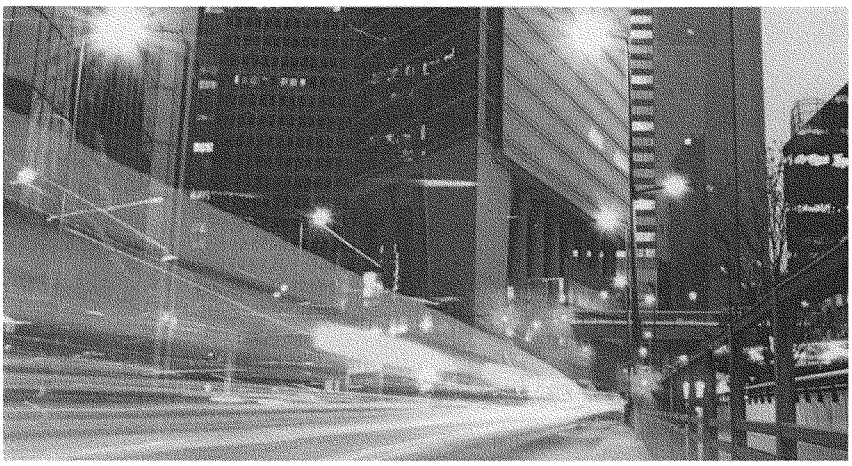
G20 Countries
Australia (.08%)
Brazil (.32%)
Canada (.17%)
China (.63%)
European Union (.41%)
France (.11%)
Germany (1.60%)
India (.21%)
Japan (.02%)
Mexico (.17%
Russia (.10%)
Saudi Arabia (.17%)
Turkey (.07%)
United Kingdom (.16%)
United States (.64%)

Other Countries
Argentina (n/a)
Colombia (.14%)
Indonesia (n/a)
Ireland (.20%)
Italy (.04%)
Kenya (.01%)
Korea (n/a)
Malaysia (.18%)
Netherlands (1.50%)
New Zealand (.09%)
Nigeria (.08%)
Norway (.64%)
Singapore (.41%)
South Africa (.14%)
United Arab Emirates (.11%)
Vietnam (.13%)
Zambia (.19%)

Many experts agree that Brazil's weak laws for cybercrime and intellectual property protection means that domestic hackers, who have become increasingly professionalized, face little risk of arrest or prosecution.[19] These factors make Brazilian cybercriminals successful locally, but there is little to prevent them from turning to a global crime. Brazil also faces external cyberthreats, and information on the Brazilian economy from key crops—from soybeans to oil production—are targets.

Among high-income countries, Germany and the Netherlands had higher than average losses (as a percent of GDP). Japan and Australia had lower than average losses. This probably reflects difference in the methodologies used to calculate cost, along with difficulties in acquiring information from companies on losses (something that officials in all countries we interviewed complained about). Japanese officials also say that the difficulty for foreign hackers to understand Japanese provided a natural layer of defense. It is easier to estimate IP losses for the US because its government has made a significant effort to identify what IP foreign hackers have taken.

Just as the G20 produces the bulk of global income, the G20 suffers the bulk of losses from cybercrime and cyberespionage. Interestingly, the rate of loss from cybercrime was roughly the same (as a percentage of GDP) among three of the four largest economies in the world (the US, China, and Germany).[20] These countries lost more than $200 billion to cybercrime. In contrast, few low-income countries had data on losses and the few where we were able to find data had small losses as a percent of national GDP. This will change as low-income countries increase their access to and use of the Internet for commercial purposes and as cybercriminals continue to refocus their activities onto mobile platforms, the preferred source for connectivity in the developing world.



Incentives explain cybercrime's growth

The incentives in cybercrime are classic in that they encourage attack and discourage defense. Cybercrime produces high returns at low risk and (relatively) low cost for the hackers. The two most common exploitation techniques—social engineering, where a cybercriminal tricks a user into granting access, and vulnerability exploitation, where a cybercriminal takes advantage of a programming or implementation failure to gain access—are both surprisingly cheap. Criminals know that risk and cost are low while rewards are high. The rate of return on cybercrime favors the criminal; the incentive is to steal more. The rate of return per victim on cybercrime can be very low, but because the costs and risks of engaging in it are even lower, cybercrime remains an irresistible criminal activity.

The opposite is true for defenders. The response to cybercrime is a business decision. Companies and individuals make decisions on how to manage the potential for loss from cybercrime by deciding how much risk they are willing to accept and how much they are willing to spend to reduce that risk. The problem with this is that if companies are unaware of their losses or underestimate their vulnerability, they will underestimate risk.

Several factors determine the risk that a company will be a victim of cybercrime. These include the ease of penetrating the target networks and the attractiveness of the target to hackers (determined by its value found on its networks). As people, businesses, and governments become more reliant on computer networks and devices, as more economic value is digitized and stored on networks, as manufacturing capabilities increase around the world, losses from cybercrime will grow if there is no improvement in international cooperation.

Hackers see low risk from cybercrime, with the added benefit that as manufacturing and research capabilities improve around the world, the return on stealing IP will increase, giving people more reason to hack—better indigenous manufacturing capabilities mean a greater return from hacking. Defenders lack the incentive to do more because they underestimate risk; the incentive for cybercriminals is to do more, as the rate of return is increasing. Absent a change in the incentives equation, the loss from cybercrime will increase.

Acceptable loss from cybercrime

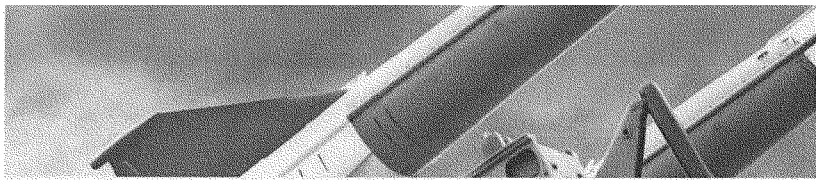
Our initial report suggested that countries will tolerate malicious activity as long as it stays at acceptable levels, less than 2% of national income. If cybercrime and cyberespionage cost more than 2% of GDP, we assume it would prompt much stronger calls for action as companies and societies find the burden unacceptable. With that as a starting point, we compared losses from cybercrime to losses from other kinds of crime and mishaps to set upper and lower bounds for credible estimates of cybercrime losses. This helped us identify credible estimates.

Our May 2013 report set upper and lower "bounds" for the cost of cybercrime by comparing it to other kinds of crime and loss. We used several analogies where other organizations have quantified the costs. These provide an idea of the scope of the problem, allowing us to set a ceiling and a floor for the cost of cybercrime. Analogies are a "proxy" number rather than a direct measurement. In our first report, we looked at car crashes, maritime piracy, "pilferage," and the drug trade. The costs these imposed on society average roughly about 1% of national income. Using these analogies we decided that it was unlikely that cybercrime cost more than $600 billion, the estimated cost of the global drug trade.

One way to think about the costs of cybercrime is that societies bear the cost of crime and loss as part of doing business and a tradeoff for convenience and efficiency. Companies and individuals have decided that the net gain of using automobiles and giant merchant ships outweigh the potential cost. The problem with these analogies is that many companies do not know the extent of their losses from cybercrime, leading them to make the wrong decisions about what is an acceptable loss.

It is worth asking if money is the right metric. There are intangible costs that may not be captured by monetary losses. Business and consumer confidence could be one such cost, although it seems unlikely. The effect on national security is another, where the monetary value of the military technology taken likely does not reflect the full cost to the nation. In both cases, we can imagine a model that estimates how much Internet use or military investments would be worth if they were unaffected by cybercrime. Our assumption is that businesses, consumers, and governments implicitly accept a lower expected value for future cyberactivities because of the risk of loss and change or reduce their investments and activities accordingly. The question this report raises is whether those company assessments of risk are accurate or if they underestimate the effect of cybercrime.

Activity	Cost As % of GDP
Maritime Piracy	0.02% (global)
Transnational Crime	1.2% (global)
Counterfeiting/Piracy	0.89% (global)
Pilferage	1.5% (US)
Car Crashes	1.0% (US)
Narcotics	0.9% (global)
Cybercrime	0.8% (global)



IP theft and innovation cannibalism

Cybercrime damages innovation. A company invests in research and development (R&D) to create new intellectual property (IP). They expect a certain return from their investment. If a competing product based on stolen IP appears in the market (an important qualification, as all stolen IP can be used), the expected return to the developer will be smaller than expected. In most cases, the value of research and development is the head start it gives companies in the market. New products and features attract new customers until competitors catch up. If the research is stolen, and the lead lasts only three months rather than a year, then the return on investment is a quarter of what it would have been absent cybercrime.

IP theft can range from paint formulas to rockets. The loss from IP theft is also the most difficult component of the cost of cybercrime to estimate. Valuing IP is an art form, based on estimating the future revenue IP will produce, or the value the market places on IP (which are not always the same). The actual value of intellectual property can be quite different from the research and development costs incurred in creating it. Hackers can take a company's product plans, its research results, and its customer lists, but the company may not even know that it has suffered loss.

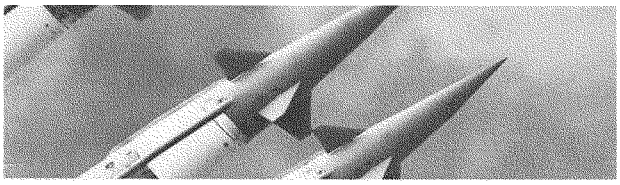
Putting a dollar figure on IP is a normal practice in pricing a company for sale or merger. These calculations can be based on a prediction of how much future income the IP will produce or how much it would fetch if offered for sale. These estimates provide a guide for estimating loss, but companies may not know what has been taken and the cybercriminals may not be able to make full use of what they have taken. Valuing IP is one of the hardest problems for estimating the cost of cybercrime, but it is not impossible. As cybertheft of IP becomes a recognized part of the business landscape, we can expect merger and acquisition (M&A) specialists to develop better tools for evaluating both the risk of compromise and the risk of successful exploitation by competitors.

The cost to companies varies from among sector and by the ability to monetize stolen data (whether it is IP or business confidential information). Although all companies face the risk of loss of intellectual property and confidential business information, some sectors—finance, chemicals, aerospace, energy, defense, and IT—are more likely to be targeted and face attacks that persist until they succeed. Losses are higher for sectors where it is easier to monetize the stolen data, as with the chemical industry, where proprietary formulas can be easily duplicated or with sensitive business information on business negotiations. A former German intelligence official told us that "first [hackers] hollowed out our clean energy industry; now they are going after our car companies."

The most important loss from cybercrime is in the theft of IP and business confidential information, as this has the most significant economic implications. IP theft is a central problem for the information economy and not limited to cybercrime. A US Department of Commerce report found that IP theft (all kinds, not just cybercrime) costs US companies $200 to $250 billion annually.[21] The Organization for Economic Development (OECD) estimated that counterfeiting and piracy costs companies as much as $638 billion per year.[22] Hacking to steal IP is an outgrowth of two larger problems: the vulnerable nature of the Internet and weak protections for IP in many countries. Putting the two together creates a global problem. IP is a major source of competitive advantage for companies and for countries. The loss of IP means fewer jobs and fewer high-paying jobs in victim countries. The effect of IP theft is to subsidize competitors and hurt competitiveness. IP theft from cybercrime works against innovation and slows the global rate of technological improvement.

We know that balanced IP protection incentivizes growth. This is why nations have, for 150 years, put in place agreements to protect IP. Weak IP protections reduce growth and IP theft over the Internet by increasing the scale of theft to unparalleled proportions; this both lowers and distorts global economic growth. By eroding IP protection, the effect of cybercrime is to depress the overall global rate of innovation while also reducing the ability of companies to gain the full return from their inventions, so they turn to other activities to make a profit. The impact of IP theft is not only to shift returns away from innovators, but also to reduce the overall rate of innovation. The beneficiary of IP theft grows somewhat faster, but the rest of the world grows more slowly.

Even the beneficiary of IP theft may suffer in the long run. Companies that benefit from stolen IP have less reason to invest in R&D. More importantly, they may never learn how to effectively manage R&D investments. For example, rather than invest in



US Department of Commerce report found that IP theft (all kinds, not just cybercrime) costs US companies $200 to $250 billion annually. The Organization for Economic Development (OECD) estimated that counterfeiting and piracy costs companies as much as $638 billion per year.

R&D, a company could rely on cyberespionage to gain new IP. Even if a company invests in R&D, it might use cyberespionage as a crutch if it ran into insurmountable technical problems, stealing a solution rather than creating the processes, internal research disciplines, and making the investments needed for innovation. That works until the other companies wise up or go bankrupt. A thief whose victims go broke is likely to starve along with them.

The result is to reduce returns to IP creators, since they will face competing products and get a smaller than expected revenues. A study[23] by the World Intellectual Property Organization (WIPO) found that the global IP market now produces $180 billion a year in fees and royalties. This means that the lost revenues from the theft of IP through hacking could be almost as much as the value of legitimate IP transactions. The effect of smaller returns is to diminish investment in R&D. One way to think about the cost from cybercrime is to ask how investors would react if the returns on IP and innovation were doubled.[24] Companies would invest more in R&D, and the global rate of innovation and technological improvement would increase. By eroding the returns on IP, cybercriminals hurt the victim company, but also their own country (which has less incentive to build an innovation infrastructure) and the world.

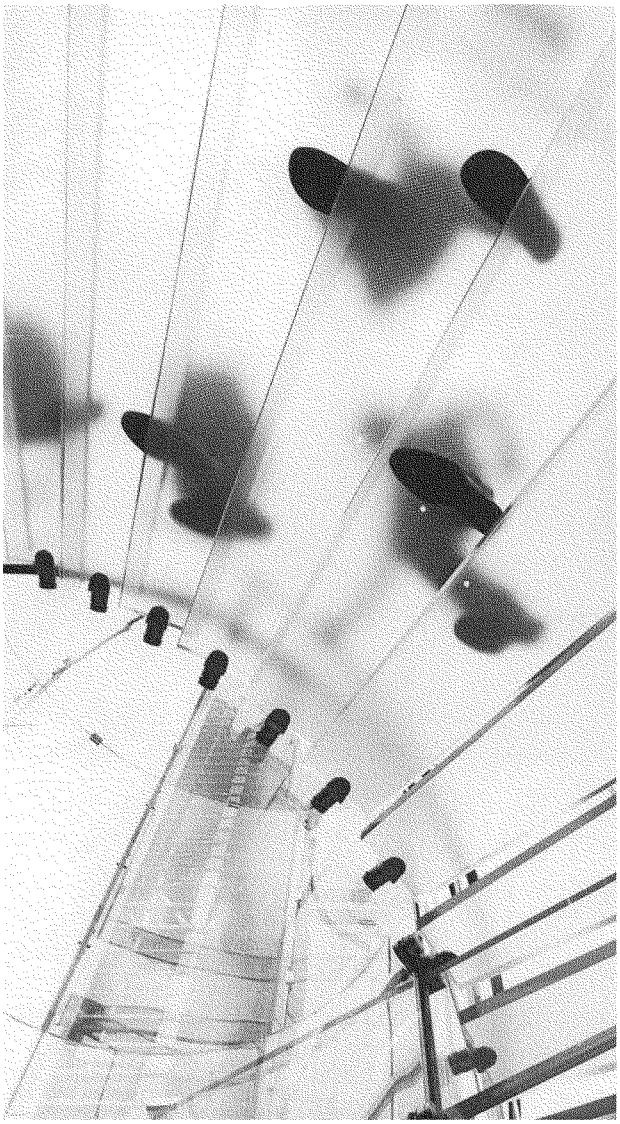
Given the nature of IP, however, this damage can be almost invisible to the victims. There is usually a delay between when IP is taken and when a competing product appears, although this varies among industry sectors. The delay between theft and production can be measured in years for technology products. Unlike the theft of a physical product, the company that created the IP is not prevented from making use of it after it has been taken, and so it cannot identify, let alone estimate, its losses. The man whose bicycle is stolen knows exactly what he has lost the next morning. The factory owner whose bicycle plans are stolen doesn't know he's lost anything until his competitor's bicycle reaches the market.

This means that companies underestimate loss and therefore underestimate their risk. Nortel's patents brought in $4.5 billion when they were sold.[25] Nortel has suffered for years from cyberespionage, with cyberspies sitting unnoticed on their networks for months at a time—this helps give an idea of the cost to an individual firm. Another firm with 800 employees had to cut its workforce in half after hackers stole its IP and a competing product appeared on the market.[26]

The limiting factor on the damage from IP theft is the ability of the acquirer to actually use the stolen technology. In the chemical sector, for example, the loss of a formula for a particular product can allow a competitor to quickly introduce a competing and potentially lower-cost product. Chemical companies are among the top targets for cybereconomic espionage. In sectors where advanced manufacturing capabilities are required, such as semiconductors or jet engines, it may be years before the theft of intellectual property produces a competing product. The value of stolen IP might be zero in the first few years only to increase dramatically when the acquirer gains the ability to use it.

One reason that the loss has been so great comes from the involvement and support of governments in the theft of IP and business confidential information. We can take as given—especially after Snowden—that nations spy on each other and have some idea of what others have been able to extract from their national networks. When senior US cybersecurity officials say that hacking is the greatest transfer of wealth in human history, they are basing that assertion on their inside knowledge of what has been taken from American companies and been copied onto another intelligence agency's servers. Hundreds of thousands of pages of designs, business plans, blueprints, and other forms or intellectual property have been taken from companies.

Some argue that the damage from espionage is tolerable, part of the cost of doing business in the world's fastest growing markets, and that companies in developed countries can "run faster," to create new technologies and so minimize any loss. There is an economic rationale for this, in that near-term gain for an individual firm outweighs long-term costs. But several dubious assumptions underlie this defense. Illicit technology transfer, even if the technology is dated by Western standards, accelerates military modernization. It accelerates improvement in indigenous industrial and technological capabilities, making the recipient better able to absorb stolen technology and faster at creating competitive products. On a national scale, IP theft translates into damage to trade balances, national income, and jobs. The theft of IP is a kind of immediate subsidy to the acquirer and distorts trade balances and national employment. Countries, like companies, have likely underestimated the risk they face.



Countries, like companies have likely underestimated the risk they face.

Penalty-free financial crime

Financial crime—the theft of financial assets through cyberintrusions—is the second largest source of direct loss from cybercrime. It is a high-profile crime. When millions of people have their credit card information stolen by hackers, it gets immediate attention. Privacy laws that require reporting when personal information is compromised mean that there are numerous anecdotes of successful attacks. These attacks can cost the victim companies more than $100 million in recovery costs for large incidents, even if the actual amount gained by cybercriminals is much smaller.

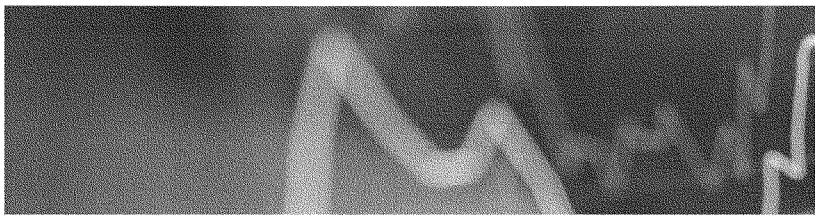
The best data on cybercrime, unsurprisingly, comes from the financial sector, which is regulated, pays serious attention to cybersecurity, and can easily measure loss. In Mexico, banks lose up to $93 million annually just to online fraud.[27] The National Police Agency estimates that Japanese banks lose about $110 million annually. The 2013 hack against the US retailer Target, alone cost banks more than $200 million, and this does not count associated costs for the retailer and its customers.[28] High-profile cyberheists that garner tens of millions of dollars from banks get a lot of attention and are a global phenomenon.

Financial crime usually involves fraud, but this can take many forms to exploit consumers, banks, and government agencies. The most damaging financial crimes seek to penetrate bank networks, with cybercriminals gaining access to accounts and siphoning money. Extortion, which appears to be more common outside of North America (and is a growing crime in India—one report stated, "India appears to be the 'ransomware' capital of Asia Pacific") can involve threats to either disclose stolen information or shut down critical services if the criminal is not paid. Sometimes the payments can run into the hundreds of thousands of dollars.

Retailers are a favorite target for cybercriminals. In 2013, a series of high-loss attacks added to a list of past attacks that includes TJ Maxx, Sony, and others. UK retailers reportedly lost more than $850 million in 2013. Similar large-scale attacks have occurred against retailer, hotel chains, media companies, an airline, and financial service companies in Australia, with losses averaging more than $100 million per company. Stolen personally identifiable information (PII) and credit card data are hard to monetize, but cybercriminals appear to be getting better at this. While tens of millions of individuals have had their data compromised, the numbers of cases where these compromises have led to financial loss are lower. Cybercriminals can use the PII themselves, or they can sell it on the black market to groups who specialize in exploiting stolen information.

The theft of financial assets can be easiest to monetize, particularly when a criminal can transfer funds directly to an account they control. In other cases, cybercriminals must rely on an intermediary to monetize their crime. They use "mules" or "cashers" (low-end criminals used to monetize stolen information) to launder money, often relatives or acquaintances of the hackers, or mules can be people hired under false pretenses who think they are working for a legitimate company. The hackers will transfer funds to the mules' accounts; the mules will take a "commission" (often between 5% to 10% of the total) and forward the rest to overseas accounts. The theft of $45 million from two banks in the Middle East involved the recruitment and use of 500 mules around the world, in this case, by using cloned debit cards to withdraw money from ATMs, keep a portion for themselves, and send the rest back to the hackers.[29] Cybercriminals will drain an account, and then they access bank networks to replenish it and drain it again.[30]

These crimes are carried out by professional gangs, some with significant organizational abilities. One European intelligence official told us that there are "20 to 30 cybercrime groups" in the former Soviet Union that have "nation-state level" capacity. These groups have repeatedly shown that they can overcome almost any cyberdefense. Financial crime in cyberspace now occurs at industrial scale.



Confidential business information and market manipulation

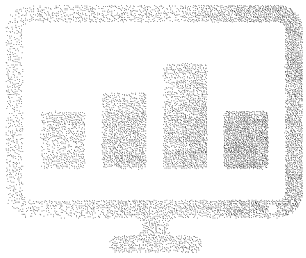
The theft of confidential business information is the third largest cost from cybercrime and cyberespionage. Business confidential information can be turned into immediate gain. The loss of investment information, exploration data, and sensitive commercial negotiation data can be used immediately. The damage to individual companies runs into the millions of dollars. Hacking of central banks or finance ministries could provide valuable economic information on the direction of markets or interest rates.

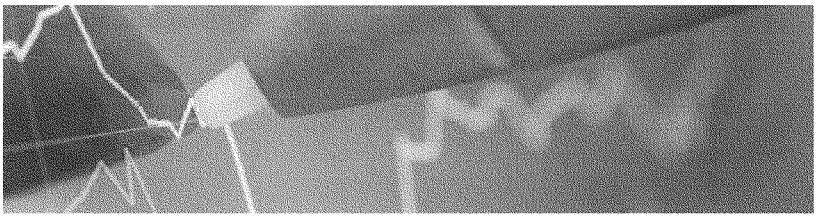
One European company told of going to negotiate a contract only to find that the other side already knew their bottom line. The company later discovered that it had been hacked. The CEO of a major oil company said privately that the loss of oilfield exploration data by hacking cost the company hundreds of millions of dollars. The director of a European security service described cyberespionage as a "normal business practice" in some parts of the world.[31]

One example would involve the theft of sensitive negotiating data that would give one party an advantage in a business deal. One UK company told British officials that it incurred revenue losses of $1.3 billion through the loss of intellectual property and disadvantages in commercial activities.

Anecdotes about loss come from every major economy. In 2010, three leading Australian mining firms were hit by cyberattacks that disrupted operations and, in one instance, were used to gain confidential information related to major contract negotiations.[32] Australian authorities said there were more than 200 attempts to hack into one mining company's networks that began with the onset of contract negotiations and continued for their duration. Similar stories from companies in the US, Europe, Asia, and Latin America are easy to find. Loss of client information is the biggest cost involved for Indian companies.[33] A BBC report found that cybercrime could cost Indian companies as much as 5% of their profits.[34]

Stock market manipulation is a growth area for cybercrime. By breaking into a company's networks or into the networks of its lawyers or accountants (which can sometimes be an easier target), cybercriminals can acquire inside information on acquisition and merger plans, quarterly revenue reports, or other data that could affect a company's stock prices. Criminals taking advantage of this information for trading could be hard to detect, as it might look like a normal trade, especially if it was carried out in another stock market. Using chat rooms and social media for "pump and dump," is a well-established technique, with criminals providing false information about a company's prospects and then cashing in when the market reacts. Turkey's financial regulators, for example, found suspicious activity intended to manipulate markets and stock prices that went beyond "pump and dump" schemes.[35] For high-end cybercriminals, cybercrime may be morphing into financial manipulation that will be exceptionally difficult to detect.





Opportunity cost and cybercrime

Opportunity cost is the value of forgone activities—opportunities or benefits that cannot be realized because resources have been expended elsewhere. Three kinds of opportunity costs determine the losses from cybercrime: reduced investment in R&D, risk averse behavior by businesses and consumers that limits Internet use, and increased spending on network defense.

For companies, the largest opportunity cost may be in the money spent to secure their networks. While companies would always spend on security even if risk in the digital environment was greatly reduced, there is a "risk premium" that they pay for using an inherently insecure network. The rate at which spending on cybersecurity increases reflects not only an increased use of network technologies, but also an increased awareness of the threat. We can use the rate of change in cybersecurity spending as an indicator of opportunity cost and a "risk premium." For example, if companies spent $1 dollar in 2011 on cybersecurity, they increased this to $1.15 in 2012. By comparison, companies spend much less than 1%[16] of the total values of shipping to protect themselves from maritime piracy.

Another way to look at the opportunity cost of cybercrime is to see it as a share of the Internet economy. Studies estimate that the Internet economy annually generates between $2 trillion and $3 trillion,[1] a share of the global economy that is expected to grow rapidly. If our estimates are right, cybercrime extracts between 15% and 20% of the value created by the Internet, a heavy tax on the potential for economic growth and job creation and a share of revenue that is significantly larger than any other transnational criminal activity.

IDC estimates that the total addressable market (a measure of market size) for cybersecurity products and services has increased by 8.7% since 2011, from $53 billion to $58 billion in 2013 (see Appendix B). Business demand for cybersecurity products increased by 14.7% in the same period, and consumer demand increased by 10.7%. Much of this growth is the result of the increased awareness of cybersecurity risks among firms. As awareness of cyberrisks grows, companies can better assess risk and spend more to manage, but if the problem were getting smaller, the market would be shrinking. Companies will keep spending to secure their networks no matter what, but smart companies realize they must spend more than they would otherwise. The real cost is measured by looking at the additional amount they have to spend. Judging from the growth in cybersecurity spending, this could be $10 billion more annually in addition to the monetary losses from cybercrime.

Cybercriminals do not always seek to extract value from their attacks. A cybercriminal can use an Internet attack to disrupt the provision of a key service. We saw this in 2012, when criminals permanently erased the data from 30,000 computers at a large oil producer and launched similarly disruptive attacks against South Korean banks and media outlets that also erased the data on thousands of hard drives.[17] These companies and their customers experienced harm that went beyond the cost of cleaning up and repair. The threat of service disruption can be part of an extortion scheme or a potential area of risk for some critical infrastructure.

Numerous surveys of companies have also found that the cost of recovering from cyberattacks, including reputational damage, where the trust in a company decreases and their brand loses value, is also increasing.[18] A 2012 survey estimated, based on the value that victims of cybercrime placed on time lost due to the incident, that this amounted to an additional $274 million to the hacked company.

The opportunity cost arising from the failure to take full advantage of information technology is harder to measure. The use of IT in healthcare has been slowed by the fear, valid or not, that health information could be stolen, patient data could be manipulated, and devices interfered with by hackers. The same may prove to be true for self-driving automobiles and other valuable technologies.

Recovery costs

Cleaning up in the aftermath of cybercrime is expensive, often more expensive than the crime itself. The cost to individual companies of recovery from cyberfraud or data breaches is increasing. While we know criminals will not be able to monetize everything that they steal, the victim has to spend as if they could monetize all the data or PII that was taken. As with spending on security, the aggregate cost to nations may be higher than monetary losses or the gain to cybercriminals.

One study of the cost of cybercrime for Italy found that while the actual losses were only $875 million, the recovery and opportunity costs reached $8.5 billion.[39] The effect on a business can include damage to brand and other reputational losses and harm to customer relations and retention. In the UK, 93% of large corporations and 87% of small businesses reported a cyberbreach in the past year, with a breach estimated to cost large companies as much as $1.4 million and small companies more than $100,000.[40] The cost of the cleanup of a cyberincident is made public in many cases. The range of expenditures can be great (from $3 million for the State of Utah to $171 million for Sony Corporation). One estimate puts the losses to the retail chain, Target, as up to $420 million, including reimbursement, the cost of reissuing millions of cards, legal fees, and credit monitoring for millions of customers.[41]

Companies experience reduced valuation after they have been hacked. The effect on stock prices can be significant—a fall in value of between 1% and 5%—but the decline is not permanent, and prices usually recover within a quarter or two. This stock price recovery may change in the future if companies are required to report major hacking incidents and describe what has actually been lost. There is also a possibility best practices and standards of care for cybersecurity become more common, companies may face increased liability and lawsuits over a lack of due diligence.[42]

The future: storms ahead, and continued growth for cybercrime

If this were a static situation, we could say that cybercrime is just another social ill, diverting at most an eighth of a percent of global income from legitimate to illegal activities. This picture is wrong. First, as more business activities move online and as more consumers around the world connect to the Internet, and as autonomous devices are connected ("the Internet of things"), the opportunities for cybercrime will grow. Cybercrime remains a growth industry. Second, losses stemming from the theft of IP will also increase as acquiring countries improve their ability to make use of it to produce competing goods.

This means that companies that fail to adequately protect their networks will be at an increasing competitive disadvantage. There are also costs to nations in jobs and trade balances, and a global cost as cybercrime slows the pace of global innovation by reducing the rate of return to innovators and investors. Countries that can't strengthen their cyberdefenses will be at a disadvantage. Over time, if nothing else changes, losses from cybercrime will grow.

Predicting the future becomes a comparison of probabilities—the probability of improved defense and better international cooperation compared to the probability of increased development around the world. The latter is certain; the former remain an area for additional work. It seems safe to say that even if the level of loss from financial crime remains constant, the level of loss from IP theft can only increase.

The situation is not irreparable, however, and it is worth asking what would change this picture. Better technology and stronger defenses could reduce the loss from cybercrime. Agreement and application of standards and best practices for cybersecurity could also reduce the cost of cybercrime. International agreement on law enforcement and on state behavior that included restraints on crime could also reduce losses, particularly if this included agreement to observe existing international commitments (such as World Trade Organization [WTO] commitments to protect IP). Making progress on these changes will require governments to do a better job accounting for loss and companies to do a better job assessing risk. These are well within the realm of the possible if people decide to treat cybercrime seriously and take action against it.

Absent these changes, we think there are two possible outcomes. In the first, the cost of crime for developed countries would stay largely flat, at least as a percentage of GDP, but the global cost would increase as new entrants and developing countries accelerate their use of the Internet. In the second, the cost to developed economies would increase as even more activities move online and as hackers improve their ability to monetize what they can steal. We do not see a credible scenario in which cybercrime losses diminish. The outlook for the world is increased losses and slower growth.

Appendix A: Economic impact of cybercrime

Brazil has been undergoing profound changes in the last 30 years, with the democratization of the country in the 1980s, inflation stabilization during the administration of President Fernando Henrique Cardoso in the 1990s, and more recently with social policies that were expanded in the 2000s during the administration of President Luiz Inácio Lula da Silva and were started in the previous government.[43]

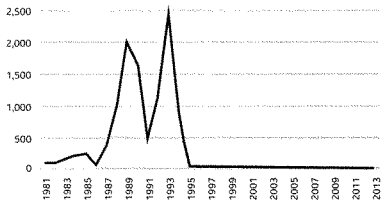
Today Brazil is one of the largest economies in the world (in 2012, it was seventh largest, behind only the US, China, Japan, Germany, France, and the UK), the largest in Latin America (its GDP is 40% of the GDP in Latin America), and is part of the group of emerging countries known as BRICS (Brazil, Russia, India, China, and South Africa). The Brazilian population, with almost 200 million people, is the fifth largest in the world (behind only China, India, the US, and Indonesia) and the largest in Latin America (34% of the population of Latin America).[44] The unemployment rate in Brazil is low (5.4% in 2013),[45] and there is a very strong social mobility, where the poorest segment of society (classes D and E) decreased from 55% of the population in 2003 to 34% in 2011. The middle class (class C) increased from 37.5% to 54% of the population in the same period, and the wealthier classes (A and B) also increased from 7.5% to 12.0%.[46]

With the dramatic growth of the Brazilian economy, very large population, low unemployment, and social mobility, most Brazilians are Internet users and cybercrime is now rampant. According to 2012 data, more than 88 million Brazilians were users of the Internet, which accounts for more than 45% of the population.[47] In comparison, the percentage of the population of Latin American Internet users is 43% (which corresponds to 10.5% of the world population of Internet users), and 34% of the world population of Internet users. Comparing absolute numbers, Latin America had nearly 255 million users in 2012, 32% of them Brazilians. North America had nearly 274 million users (78.6% of the US population). Another important factor is the increase in the percentage and number of Internet users in Latin America—18 million people in 2000 to almost 255 million in 2012, which represent 1300%.[48]

Given this scenario, with all the economic improvements that have occurred over the years, the country is also wrestling with the problem of cybercrime. Today, cybercrime is one of the top four economic crimes in the world. In Brazil, cybercrime is in second place.[49] According to data from FEBRABAN (Brazilian Federation of Banks), Brazil had losses of R $1.4 billion in 2012 (US $591 million),[50] down 6.7% over the previous year. It is also important to note that although the absolute number is impressive, it represents only 0.06% of bank transactions.[51] It reflects, among other factors, weak laws and lack of awareness among businesses and consumers on this subject. According to the *Global Economic Crime Survey 2011—Brazil*, 40% of Brazilian respondents said they had never received any training in cybersecurity, 57% of Brazilian companies said they do not have the resources to fight cybercrime or know if they are capable of cybercrime investigatations, and 50% of Brazilians said they didn't know that their companies could detect and prevent cybercrime.[52]

Brazil lived with hyperinflation during the 1980s and into the early 1990s, and this reached its peak with inflation of nearly 2,500% in 1993 (Graph 1),[53] the year before the implementation of the Real Plan, which put an end to the serious economic problems that plagued the country for so long. On this issue of hyperinflation, both the government and the financial system were forced to make changes. One of the key changes was that financial institutions embraced electronic systems and online banking.[54]

Inflation in Brazil (%)



According to the 2013 BSA Global Cloud Computing Scorecard, because Brazil had been struggling with the cybersecurity issue for a while, it adopted modern laws against cybercrime, but most of these measures are inadequate. In Brazil, where organized crime is rife and laws to prevent cybercrime are few and ineffective, the country is becoming a laboratory for cybercrime, with hackers committing crimes such as identity and data theft, credit card fraud, and piracy, as well as online vandalism. According to the mi2g Intelligence Unit, a digital risk consulting firm in London, several notorious groups of vandals and Internet criminals originated in Brazil.[55]

According to the Business Software Alliance (BSA), existing criminal laws in Brazil are out of compliance with international standards for digital crime. Brazil has gaps in the protection of intellectual property and has not signed the WIPO Copyright Treaty, an international treaty on copyright law adopted by the member states of the World Intellectual Property Organization (WIPO). Brazil needs to create strong laws to end impunity for hackers, promote good data management, and encourage the growth of e-commerce.[56] This is currently under discussion in the Brazilian National Congress through the Marco Civil da Internet, which will establish a "constitution" of the global network of computers in Brazil, with rights and duties of users and companies.[57]

Appendix B: Total addressable market for cybersecurity

Product Areas	2011	2012	2013	% Change 2011–2013
Email Gateway	2414	2447	2622	8.6%
Next Generation Firewall	2249	2721	3217	43.0%
Intrusion Prevention Systems	1890	1859	1906	0.8%
Firewall	2356	2631	2576	9.3%
VPN	941	725	746	-20.7%
Web	1914	1991	2122	10.9%
Total IAM	4019	4418	4860	20.9%
Corporate Endpoint	3225	3447	3692	14.5%
Consumer	4451	4638	4916	10.4%
Vulnerability Assessment	837	916	1008	20.4%
Forensics	221	305	369	67.0%
Proactive Endpoint Risk Management	465	482	506	8.8%
SIEM	1308	1434	1594	21.9%
Policy and Compliance	801	875	962	20.1%
Security Device Systems Management	201	179	166	-17.4%
Consulting Services		4366	4694	7.5%
Integration Services		8109	8529	5.2%
Other Security (2012)		12073	13788	6.9%
Total Security (Product/Services)				
Total Available Market		53611	58267	8.7%
Total Security Product Total Available Market	28048	29872	32071	14.3%
Total B2B Product Total Available Market	23597	25233	27155	15.1%

Source: Multiple IDC Security Products and Services reports, 2013. All 2013 figures are forecast estimates.

Appendix C: Cybercrime as a percent of GDP

Country	% of GDP	Confidence	G20 Countries
Argentina	N/A		
Australia	0.08%	M	X
Brazil	0.32%	M	X
Canada	0.17%	M	X
China	0.63%	H	X
Colombia	0.14%	L	
EU	0.41%	L	X
France	0.11%	L	X
Germany	1.60%	H	X
India	0.21%	L	X
Indonesia	N/A		
Ireland	0.20%	M	
Italy	0.04%	L	
Japan	0.02%	L	X
Kenya	0.01%	L	
Korea	N/A		
Malaysia	0.18%	M	
Mexico	0.17%	M	X
Netherlands	1.50%	H	
New Zealand	0.09%	M	
Nigeria	0.08%	M	
Norway	0.64%	H	
Russia	0.10%	M	X
Saudi Arabia	0.17%	L	X
Singapore	0.41%	M	
South Africa	0.14%	M	
Turkey	0.07%	L	X
United Arab Emirates	0.11%	M	
United Kingdom	0.16%	L	X
United States	0.64%	H	X
Vietnam	0.13%	L	
Zambia	0.19%	L	

Appendix D: Select bibliography on cybercrime

"Internet Value Chain Economics," AT Kearney, last modified May 2010, Last Accessed: 2/10/2014, http://www.atkearney.com/paper/-/asset_publisher/dVxv4Hz2h8bS/content/internet-value-chain-economics/10192.

Ross Anderson, Chris Barton, Rainer Böhme, Richard Clayton, Michel J.G. van Eeten, Michael Levi, Tyler Moore, Stefan Savage, "Measuring the Cost of Cyber Crime" (paper presented at the Weis 202 Workshop on the Economics of Information Security Berlin, Germany, June 25-26, 2012), Last Accessed 2/10/2014, http://weis2012.econinfosec.org/papers/Anderson_WEIS2012.pdf.

Dennis Blair, Jon Huntsman Jr., Craig Barrett, Slade Gordon, William J. Lynn III, Deborah Wince-Smith, Michael K. Young, "The IP Commission Report: The Report on the Commission of the Theft of American Intellectual Property," (Seattle, Washington, National Bureau of Asian Research: 2013), Last Accessed: 2/10/2014, http://www.ipcommission.org/report/IP_Commission_Report_052213.pdf.

Brian Cashell, William D. Jackson, Mark Jickling, Baird Webel, "The Economic Impact of Cyber-Attacks," (Washington, D.C., Congressional Research Service: 2004), Last Accessed: 2/10/2014, http://congressionalresearch.com/RL32331/document.php.

DAKA Advisory, "Meeting the cyber security challenge in Indonesia: An analysis of threats and responses," (Jakarta, Indonesia, British Embassy in Indonesia, 2013), Last Accessed: 2/10/2014, http://dakaadvisory.com/wpcontent/uploads/DAKA-Indonesia-cyber-security-2013-web-version.pdf.

Financial Action Task Force, "Money Laundering & Terrorist Financing Vulnerabilities of Commercial Websites and Internet Payment Systems," (Paris, France Financial Action Taskforce OECD: 2008), Last Accessed: 2/10/2014, http://www.fatf-gafi.org/media/fatf/documents/reports/ML%20TF%20Vulnerabilities%20of%20Commercial%20Websites%20and%20Internet%20Payment%20Systems.pdf.

Dinei Florêncio, Cormac Herley, "Sex, Lies, and Cyber-crime Surveys," Microsoft Research (2013), Last Accessed: 2/10/2014, http://research.microsoft.com/pubs/149886/sexliesandcybercrimesurveys.pdf.

Hogans Lovells International LLP, "Report on Trade Secrets for the European Commission," (Brussels, Belgium, Hogans Lovells International LLP: 2013), Last Accessed: 2/10/2014, http://ec.europa.eu/internal_market/iprenforcement/docs/trade-secrets/120113_study_en.pdf.

International Telecommunications Union, "Understanding Cyber Crime: Phenomena, Challenges, and Legal Response," (New York, N.Y., I.T.U.: 2012), Last Accessed: 2/10/2014, http://www.itu.int/ITU-D/cyb/cybersecurity/docs/Cyber crime%20legislation%20EV6.pdf.

KPMG International, "Cyber Crime – A Growing Challenge for Governments," Issues Monitor 8 (2011), Last Accessed: 2/10/2014, http://www.kpmg.com/Global/en/IssuesAndInsights/ArticlesPublications/Documents/cyber-crime.pdf.

William Lehr, "Measuring the Internet: the Data Challenge," OECD Digital Economy Papers No. 194 (2012), Last Accessed: 2/10/2014, http://www.oecdilibrary.org/docserver/download/5k9bhk5fzvzx.pdf?expires=1392049778&id=id&accname=guest&checksum=9751668C60F33441C4B87B4B04712747.

Avner Levin, Daria Ilkina, "International Comparison of Cyber Crime," (Toronto, Canada, Ryerson University: 2013), Last Accessed: 2/10/2014, http://www.ryerson.ca/tedrogersschool/privacy/documents/Ryerson_International_Comparison_ofCyber_Crime_-March2013.pdf.

James A. Lewis, Stewart Baker, "Estimating the Cost of Cyber Crime," Center for Strategic and International Studies, Washington, D.C., June 2013), Last Accessed: 2/10/2014, https://csis.org/event/estimating-cost-cyber-crime-andcyber-espionage.

Emma McClarkin, "Cyber Crime- New Investigation Strategies and New Technologies," (Brussels, Belgium, Special Committee on Organized Crime, Corruption, and Money Laundering: 2012), Last accessed: 2/10/2014, http://www.europarl.europa.eu/meetdocs/2009_2014/documents/crim/dv/mcclarkin_/mcclarkin_en.pdf.

Norton by Symantec, "2012 Norton Cyber Crime Report," (Mountain View, CA, Symantec: 2012), Last Accessed: 2/10/2014, http://now-static.norton.com/now/en/pu/images/Promotions/2012/cybercrimeReport/2012_Norton_Cyber crime_Report_Master_FINAL_050912.pdf.

Ponemon Institute, "2013 Cost of Data Breach Study: Global Analysis," (Traverse City, Michigan, Ponemon Institute: 2013), Last Accessed: 2/10/2014, http://www.symantec.com/content/en/us/about/media/pdfs/bcost-of-a-data-breach-global-report-2013.en-us.pdf?om_ext_cid=biz_socmed_twitter_facebook_marketwire_linkedin_2013Jun_worldwide_CostofaDataBreach.

TrendMicro, "Latin America and Caribbean Cybersecurity Trends and Government Responses," (Washington, D.C., Organization of American States: 2013), Last Accessed: 2/10/2014, http://www.trendmicro.com/cloudcontent/us/pdfs/security-intelligence/white-papers/wp-latin-american-andcaribbean-cybersecurity-trends-and-government-responses.pdf.

United Nations Office on Drugs and Crime, "Comprehensive Study on Cyber Crime," (New York, N.Y., United Nations: 2013), Last Accessed 2/10/2014, http://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBER CRIME_STUDY_210213.pdf.

The Australian Business Assessment of Computer User Security (ABACUS) survey: methodology report, http://www.aic.gov.au/publications/current%20 series/rpp/100-120/rpp102.html.

Latin American and Caribbean Cybersecurity Trends and Government Responses http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp-latin-american-and-caribbean-cybersecurity-trends-andgovernment-responses.pdf http://www.welivesecurity.com/wp-content/uploads/2014/01/informe_esr13.pdf

Information Security in Swiss Companies: A Survey on Threats, Risk Management and Forms of Joint Action, http://www.css.ethz.ch/policy_consultancy/products_INT/DetailansichtPubDB_EN?rec_id=1396

Impact of cyber crime on businesses in Canada, https://www.icspa.org/media/icspa-news/icspa-news-publications/article/icspa-releases-study-tomeasure-the-impact-of-cyber-crime-on-businesses-in-canada-43/abp/3/

Data Breaches: Greater frequency, Greater Costs for All Companies, http://www2.trustwave.com/rs/trustwave/images/2013-Global-Security-Report.pdf.

Tim Stapleton, Zurich National, "Data Breaches: Greater frequency, Greater Costs for All Companies," http://www.zurichna.com

Trustwave, 2013 Global Security Report, http://www2.trustwave.com/rs/trustwave/images/2013-Global-Security-Report.pdf

1 Which reached $72 trillion in 2012.

2 John Hawes, "2013 An Epic Year For Data Breaches With Over 800 Million Records Lost," *Naked Security*, February 19, 2014, http://nakedsecurity.sophos.com/2014/02/19/2013-an-epic-year-for-data-breaches-with-over-800-million-records-lost/

3 http://www.ponemon.org/news-2/23

4 While a subject of debate, economist Arthur Okun found that for every 1% increase in unemployment, GDP will be roughly 2% lower.

5 International Trade Administration, "Jobs Supported by Exports: An Update," March 12, 2012, http://www.trade.gov/mas/ian/build/groups/public/@tg_ian/documents/webcontent/tg_ian_003639.pdf

6 N. Sousa, J. M. Rueda-Cantuche, I. Arto, and V. Andreoni, "Extra: EU Exports and Employment," *Chief Economists Note, European Commission, Trade*, Issue 2, 2012, http://trade.ec.europa.eu/doclib/docs/2012/may/tradoc_149511.%202_24.05.2012.pdf. See also: "Unemployment Statistics," *European Commission: Euro Stat*, http://epp.eurostat.ec.europa.eu/statistics_explained/index.php/Unemployment_statistics; epp.eurostat.ec.europa.eu/cache/.../3-31012014-AP-EN.PDF

7 "Extra - EU Exports and Employment," trade.ec.europa.eu/doclib/html/149511.htm

8 Statement by Dennis McDonough at the White House.

9 "Six Arrested Over 45 Million Cyber Heist on Middle East Banks," *Al Arabiya*, November 19, 2013, http://english.alarabiya.net/en/business/banking-and-finance/2013/11/19/Six-arrested-over-45-million-cyber-heist-on-Middle-East-banks.html

10 Tom Whitehead, "Cyber Crime A Global Threat, MI5 Head Warns," *The Telegraph*, June 6, 2012, http://www.telegraph.co.uk/news/uknews/terrorism-in-the-uk/9354373/Cyber-crime-a-global-threat-MI5-head-warns.html

11 Jordan Robertson, "Why Are Hackers Flooding Into Brazil?" *Bloomberg*, September 13, 2013, http://www.bloomberg.com/news/2013-09-13/why-are-hackers-flooding-into-brazil-.html

12 Pavan Duggal, "The Face of Indian Cyber Law in 2013," *The Business Standard*, December 30, 2013, http://www.business-standard.com/article/technology/the-face-of-indian-cyber-law-in-2013-113123000441_1.html

13 Notable companies include Yahoo, Symantec, Adobe, Northrop Grumman, and Dow Chemical. See: Ariana Eunjung Cha and Ellen Nakishima, "Google China Cyberattack Part of Vast Espionage Campaign, Experts Say," *The Washington Post*, January 14, 2010, http://www.washingtonpost.com/wp-dyn/content/article/2010/01/13/AR2010011300359.html

14 "Cyber Crime and Security Survey Report 2012," *CERT Australia*, https://www.cert.gov.au/system/files/614/679/Cyber%20Crime%20and%20Security%20Survey%20Report%202012.pdf: 5

15 http://defensetech.org/2012/02/06/did-chinese-espionage-lead-to-f-35-delays/; http://breakingdefense.com/2013/06/top-official-admits-f-35-stealth-fighter-secrets-stolen/

16 Patricia Prandini and Marcia L. Maggiore, "Panorama del ciberdelito en Latinoamérica," *Project Amparo*, June 2011, http://www.proyectoamparo.net/files/LACNIC-PanoramCiberd-VsFinal-20110701.pdf: 72

17 Gerald Jeffris, "Citi Hit in Brazilian Hacker Attack," *The Wall Street Journal*, February 4, 2012, http://online.wsj.com/news/articles/SB10001424052970203889904577200964142208498

18 Dan Goodin, "DSL modem hack used to infect millions with banking fraud malware," *Ars Technica*, October 1, 2012, http://arstechnica.com/security/2012/10/dsl-modem-hack-infects-millions-with-malware/

19 For example, Business Software Alliance, http://www.forbes.com/sites/ricardogeromel/2012/03/02/hackers-stole-1billion-in-brazil-the-worst-prepared-nation-to-adopt-cloud-technology/, also PWC, *Global Economic Crime Survey 2011—Brazil*

20 Incomplete figures for Japan were provided in interviews with Japanese officials from NISC, NPA, and METI.

21 "Stolen Intellectual Property Harms American Businesses Says Acting Deputy Secretary Blank," *The Commerce Blog, U.S. Department of Commerce*, November 29, 2011, http://www.commerce.gov/blog/2011/11/29/stolen-intellectual-property-harms-american-businesses-says-acting-deputy-secretary-

22 Robert J. Shapiro and Kevin A. Hassett, "The Economic Value of Intellectual Property," *Sonecon*, http://www.sonecon.com/docs/studies/IntellectualPropertyReport-October2005.pdf: 3

23 *World Intellectual Property Report 2011—The Changing Face of Innovation*

24 Ibid.

25 Alastair Sharp, "Apple/RIM Group Top Google in $4.5 Billion Nortel Sale," *Reuters*, July 1, 2011, http://www.reuters.com/article/2011/07/01/us-nortel-idUSTRE7600PF20110701

26 "Trade Secrets: Supporting Innovation, Protecting Know-How," *European Commission Conference*, June 29, 2012, http://ec.europa.eu/internal_market/iprenforcement/docs/conference20120629/ts_summary_consolidatedfinal20120913_en.pdf

27 University of Pennsylvania Wharton School of Business, "Latin American Reaches a Crossroads for Guarding Against Cyber Crime," July 24, 2013, http://www.wharton.universia.net/index.cfm?fa=viewfeature&id=2384&language=english

28 "Target Data Breach Cost for Banks Tops $200M," *Associated Press*, February 18, 2014, http://www.nbcnews.com/business/business-news/target-data-breach-cost-banks-tops-200m-n33156

29 Jessica Dye, Joseph Axe, and Jim Finkle, "Huge cyber bank theft spans 27 countries," *Reuters*, May 9, 2013, http://www.reuters.com/article/2013/05/09/net-us-usa-crime-cyber crime-idUSBRE9480PZ20130509; "Six Arrested Over 45 Million Cyber Heist on Middle East Banks," *Al Arabiya*, November 19, 2013, http://english.alarabiya.net/en/business/banking-and-finance/2013/11/19/Six-arrested-over-45-million-cyber-heist-on-Middle-East-banks.html

30 http://krebsonsecurity.com/2013/11/feds-charge-calif-brothers-in-cyberheists/

31 "The Olympics and Beyond," *Address at the Lord Mayor's Annual Defence and Security Lecture by the Director General of the Security Service, Jonathan Evans*, June 25, 2012, https://www.mi5.gov.uk/home/about-us/who-we-are/staff-and-management/director-general/speeches-by-the-director-general/the-olympics-and-beyond.html

32 "Chinese Cyber Attack on BHP Billiton, Rio Tinto, and Fortescue Metals Group," *News.com.au*, April 20, 2010, http://www.news.com.au/finance/chinese-cyber-attacks-on-bhp-billiton-rio-tinto-and-fortescue-metals-group/story-e6frfm1i-1225855748114; Jennifer Hewett, "Miners fear secrets stolen by Chinese cyber-spies," *The Australian*, April 20, 2010, http://www.theaustralian.com.au/business/mining-energy/miners-fear-secrets-stolen-by-chinese-cyber-spies/story-e6frg8df-1225855718533; interview with Australian Federal Police

33 Zahra Khan, "India Tops Cyber Crime Hit List," *The Live Mint*, November 20, 2013, http://www.livemint.com/Specials/ZrC7Ol3QsLMIkiFbAfoL7O/India-tops-cyber crime-hit-list.html

34 "Cyber Crime Warnings for India," *BBC*, May 6, 2012, http://www.bbc.com/news/business-17979980

35 See Cyber Crime in Turkey www.spk.gov.tr/displayfile.aspx, slides 20-41

36 Peter Chalk, *The Maritime Dimension of International Security: Terrorism, Piracy, and Challenges for the United States*, (Rand: Santa Monica, 2008), http://www.rand.org/content/dam/rand/pubs/monographs/2008/RAND_MG697.pdf

37 Ryan Sherstobitoff, "Dissecting Operation Troy: Cyberespionage in South Korea," *McAfee*, 2013, http://www.mcafee.com/us/resources/white-papers/wp-dissecting-operation-troy.pdf

38 Ponemon Institute, "Cost of Cyber Crime Study 2013: The United States," October 2013: http://media.scmagazine.com/documents/54/2013_us_ccc_report_final_6-1_13455.pdf: 16; "Reputational Risk And IT: How Security And Business Continuity Can Shape the Reputation and Value of Your Company," *2012 IBM Global Reputational Risk and IT Study*, September 2012, http://www-935.ibm.com/services/us/gbs/bus/html/risk_study.html

39 "The World's Community and the War on Cyber Crime—What About Italy?" slide 12, https://www.securitysummit.it/upload/file/Atti/22.03.12_JART%20ARMIN.pdf

40 "Keeping the UK safe in cyber space," March 14, 2014, https://www.gov.uk/government/policies/keeping-the-uk-safe-in-cyberspace

41 "Target Hackers Broke in Via HVAC Company," Krebs on Security, February 14, 2014, http://krebsonsecurity.com/2014/02/target-hackers-broke-in-via-hvac-company/

42 Lawrence A. Gordona, Martin P. Loeba, and Lei Zhoua, "The impact of information security breaches: has there been a downward shift in costs?" *Journal of Computer Security*, Vol. 19, 2011 http://iospress.metapress.com/content/n3054376432h7358/fulltext.pdf: 33-56

43 Economist of the Brazilian Institute of Economics/Getulio Vargas Foundation (IBRE/FGV)

44 Data about GDP and population: World Economic Outlook of the International Monetary Fund (WEO/IMF), http://www.imf.org/external/pubs/ft/weo/2013/02/weodata/index.aspx

45 http://saladeimprensa.ibge.gov.br/en/noticias?view=noticia&id=1&idnoticia=2575&busca=1&t=desocupacao-foi-4-3-dezembro-fecha-2013-media-5-4

46 http://www.bcb.gov.br/pec/appron/apres/CarlosHamilton_CAE_09-11-20112.pdf

47 http://www.internetworldstats.com/stats2.htm

48 http://www.internetworldstats.com/stats.htm

49 http://www.pwc.com.br/pt/publicacoes/assets/pesquisa-crimes-digitais-11-ingles.pdf

50 Exchange rate of R $ / U.S. $ 2.37 (average of 2014, until 03/25/14)

51 http://www.ciab.com.br/_pdfs/publicacoes/2012/43-Dez2012.pdf

52 http://www.pwc.com.br/pt/publicacoes/assets/pesquisa-crimes-digitais-11-ingles.pdf

53 Source: IMF

54 Davidson, James Dale. Brazil is the New America: How Brazil Offers Upward Mobility in a Collapsing World, 2012. http://books.google.com.ph/books?id=8muXHC8xQBIC&pg=PT125&img=1&zoom=3&hl=en&sig=yf3cfKKtQR&sig=ACfU3U1214BNCrmKbjl6ora5b4ccY-OF1Ow&w=685

55 http://www.nytimes.com/2003/10/27/business/technology-brazil-becomes-a-cyber-crime-lab.html?src=pm

56 http://www.forbes.com/sites/ricardogeromel/2012/03/02/hackers-stole-1billion-in-brazil-the-worst-prepared-nation-to-adopt-cloud-technology/

57 http://g1.globo.com/politica/noticia/2014/03/governo-e-camara-dizem-que-marco-da-internet-sera-votado-nesta-terca.html

About CSIS

For 50 years, the Center for Strategic and International Studies (CSIS) has developed practical solutions to the world's greatest challenges. As we celebrate this milestone, CSIS scholars continue to provide strategic insights and bipartisan policy solutions to help decision makers chart a course toward a better world.

CSIS is a bipartisan, nonprofit organization headquartered in Washington, DC. The Center's 220 full-time staff and large network of affiliated scholars conduct research and analysis and develop policy initiatives that look to the future and anticipate change.

http://csis.org/

About McAfee

McAfee, part of Intel Security and a wholly owned subsidiary of Intel Corporation (NASDAQ:INTC), empowers businesses, the public sector, and home users to safely experience the benefits of the Internet. The company delivers proactive and proven security solutions and services for systems, networks, and mobile devices around the world. With its Security Connected strategy, innovative approach to hardware-enhanced security, and unique Global Threat Intelligence network, McAfee is relentlessly focused on keeping its customers safe.

http://www.mcafee.com

2821 Mission College Boulevard
Santa Clara, CA 95054
888 847 8766
www.mcafee.com

61162rpt_csis-econ-cybercrime_0614

epic.org

Electronic Privacy Information Center
1718 Connecticut Avenue NW, Suite 200
Washington, DC 20009, USA

+1 202 483 1140
+1 202 483 1248
@EPICPrivacy
https://epic.org

May 8, 2017

The Honorable Ron Johnson, Chairman
The Honorable Claire McCaskill, Ranking Member
U.S. Senate Committee on Homeland Security & Government Affairs
340 Dirksen Senate Office Building
Washington, DC 20510

RE: Hearing on Cyber Threats Facing America: An Overview of the Cybersecurity Threat Landscape

Dear Chairman Johnson and Ranking Member McCaskill:

We write to you regarding the "Cyber Threats Facing America: An Overview of the Cybersecurity Threat Landscape" hearing.[1] EPIC has an active interest in this effort. Weaknesses in cyber security threaten both consumers and democratic institutions.[2] We welcome your leadership on this critical issue and look forward to opportunities to work with you and your staff.

EPIC is a public interest research center established in 1994 to focus public attention on emerging privacy and civil liberties issues.[3] EPIC is also a leading advocate for civil liberties and democratic values in the information age. In response to the finding of the Intelligence Community that the Russian government interfered with the 2016 Presidential election, EPIC launched a new project on Democracy and Cybersecurity.[4] Our goal is to determine the extent of Russian interference and ensure that the U.S. government takes necessary steps to safeguard political institutions against future attack.

Data protection and privacy should remain a central focus of the cyber security policy of the United States. It is precisely the extensive collection of personal information without adequate safeguards that places the United States at risk from cyber criminals and foreign adversaries. In 2015, more than 22 million records of federal employees, including 5 million digitized fingerprints and the sensitive form SF-86, were compromised. So-called "credit

---

[1] *Cyber Threats Facing America: An Overview of the Cybersecurity Threat Landscape*, 115th Cong. (2017), S. Comm. on Homeland Security and Gov't Affairs, https://www.hsgac.senate.gov/hearings/cyber-threats-facing-america-an-overview-of-the-cybersecurity-threat-landscape (May 10, 2017).
[2] *See* Democracy and Cybersecurity: Preserving Democratic Institutions, EPIC, https://epic.org/democracy/.
[3] *See* EPIC, *About EPIC*, https://epic.org/epic/about.html.
[4] *See* EPIC, *Democracy and Cybersecurity*, https://epic.org/democracy/.

monitoring services" are an insufficient response to the ongoing risk to the financial records, medical records, and private communications of Americans.

Strong encryption policy and robust technical measures must be enacted to safeguard personal data. Weaknesses in security standards create vulnerabilities for American businesses and consumers that will be exploited by foreign adversaries. Where it is possible to minimize or eliminate the collection of personally identifiable information, the risk to the American public will be reduced.

The Cyber Security Information "Sharing" Act is now in force. That law facilitates the transfer of customer and client data from the private sector to the government, raising widespread concerns among technical experts and privacy organizations about the protection of personal information. While we favor a cooperative relationship between companies and the federal government concerning cyber security, the federal government must respect the privacy obligations of private companies and ensure the transparency of its own conduct. In the cyber security domain, as with other programs supported by taxpayer dollars, the government must uphold the law and remain open and accountable.

Finally, *Congress should strengthen the federal Privacy Act*. Personal data stored in federal agencies remains one of the key targets of criminal hackers and foreign adversaries. Significant steps were taken by the last administration to establish a Federal Privacy Council and to coordinate privacy protection across the federal agencies. Still, more should be done, including updates to the federal privacy law and the establishment of a data protection agency in the United States.

We ask that this Statement be entered in the hearing record. EPIC looks forward to working with the Committee on these issues of vital importance to the American public.

Sincerely,

/s/ *Marc Rotenberg*
Marc Rotenberg
EPIC President

/s/ *Caitriona Fitzgerald*
Caitriona Fitzgerald
EPIC Policy Director

KASPERSKY lab

United States Senate
Senate Committee on Homeland Security and Governmental Affairs
Hearing entitled, "Cyber Threats Facing America: An Overview of the Cybersecurity Threat Landscape"

May 10, 2017

Statement for the Record

Introduction

Chairman Johnson, Ranking Member McCaskill, and other esteemed Members of the Senate Committee on Homeland Security and Governmental Affairs, thank you for holding today's hearing entitled, "Cyber Threats Facing America: An Overview of the Cybersecurity Threat Landscape." As a global cybersecurity company protecting consumers, businesses, critical infrastructure, and governments worldwide since 1997, Kaspersky Lab has seen cyberattacks grow into an immense global threat in recent years. For example, there is the exponential increase, over the past two decades, in the number of observable malware incidents, with Kaspersky Lab initially seeing one new virus per hour in the early 1990s to seeing over 320,000 new malware samples a day today.[1] In addition to the proliferation of malware, we have all seen the significant damage that malware can cause, from the release of an individual's personally identifiable information to the complete blackout of a city's electrical grid. These constantly evolving cyber threats know no geographical or virtual borders, as cyberattacks are truly a global issue, and to that end, every individual, business, industry, and country can become a victim.

I. Nature of the Threat

There are a number of trends that Kaspersky Lab has identified with regards to the cyber threat landscape that we would like to highlight for the Committee as it considers this important topic.

A. Ransomware

62 new ransomware families appeared in 2016, and the number of new ransomware modifications increased 11-fold from Q1 to Q3.[2] 75 percent of these new ransomware families related to Russian-speaking groups or individuals.[3] During that same time frame (Q1 to Q3 of 2016), Kaspersky Lab observed that ransomware attacks on individuals increased from one every 20 seconds to one every 10

[1] Dark Reading, "Kaspersky Lab: 323,000 New Malware Samples Found Each Day," *Dark Reading*, 7 December 2016. Link: http://www.darkreading.com/vulnerabilities---threats/kaspersky-lab-323000-new-malware-samples-found-each-day/d/d-id/1327655.
[2] Kaspersky Security Bulletin 2016, "Story of the Year: The Ransomware Revolution," *Securelist* blog post, 8 December 2016. Link: https://securelist.com/files/2016/12/KSB2016_Story_of_the_Year_ENG.pdf.
[3] Kaspersky Lab, "A Look into the Russian –Speaking Ransomware Ecosystem," *Securelist* blog post, 14 February 2017. Link: https://securelist.com/analysis/publications/77544/a-look-into-the-russian-speaking-ransomware-ecosystem/.

KASPERSKY lab

seconds, while attacks on businesses increased from one every 2 minutes to one every 40 seconds.[4] In addition to the increase in the number of ransomware families, variants, and attacks, 2016 also saw this particular type of malware grow in sophistication, with cybercriminals writing ransomware in scripting languages like Python and AutoIT, deploying ransomware that can encrypt all of a system's files at once, and pairing ransomware with other malware functionality like spyware or key-loggers to infect systems in more than one manner.[5] Furthermore, the ease with which to deploy a ransomware attack, along with such attacks' high profitability, has attracted significant interest from cybercriminal groups, including some advanced persistent threat (APT) actors and other targeted attackers, who are incorporating such malware more and more in their toolkits.[6]

B. Cyberattacks Continue to Go Mobile

As individuals continue to embrace the use of devices they can hold in their hands to manage their daily lives, cybercriminals will continue to find ways to attack those devices. Last year, Kaspersky Lab observed a three-fold rise in mobile malware detections compared with 2015, with more than 8.5 million malicious installations identified.[7] A significant 2016 trend for mobile device threats was the exploitation of known vulnerabilities to grant Trojans root access and other super-user privileges to install malicious advertising applications or other malware on the devices.[8] Some of these Trojans were found as applications in the operating system application stores,[9] such as the "Guide for Pokémon Go" application that was downloaded over 500,000 times late last year. Other trends include a growth in mobile-based ransomware, with detection rates 8.5 times over 2015, accompanied with a 1.6 times increase in mobile banking Trojans that are constantly finding ways to bypass a system's security mechanisms during the same time period.[10] While cybercriminals who engage in targeted or persistent attacks have primarily used mobile attacks as one component of their toolkits, we fully expect that as people shift to more and more handheld devices, mobile-specific cybercrime campaigns will increase as a result.[11]

C. Internet of Threats

The distributed denial of service (DDoS) attacks, perpetuated by the Mirai botnet in Q4 of 2016, rightfully raised significant public concerns about the security, or lack thereof, in connected and Internet-enabled devices and products. While this is an important area of focus, and we appreciate the efforts by the Department of Homeland Security in its Strategic Principles for Securing the Internet of

---

[4] Kaspersky Security Bulletin 2016.
[5] *Ibid.*
[6] Kaspersky Lab, "Ransomware in targeted attacks," *Securelist* blog post, 4 April 2017. Link: https://securelist.com/blog/sas/77877/ransomware-in-targeted-attacks/.
[7] Kaspersky Lab, "Mobile Malware Evolution 2016," *Securelist* blog post, 28 February 2017. Link: https://securelist.com/files/2017/02/Mobile_report_2016.pdf.
[8] *Ibid.*
[9] *Ibid.*
[10] *Ibid.*
[11] Kaspersky Security Bulletin, "Predictions for 2017: 'Indicators of Compromise are Dead," 16 November 2016. Link: https://kasperskycontenthub.com/securelist/files/2016/11/KL_Predictions_2017.pdf.

KASPERSKY lab

Things (IoT),[12] among other U.S. government initiatives in this space, Kaspersky Lab maintains that it is equally important to think beyond the products and devices themselves, and also consider that the Internet of Things and cyber-physical systems are key enablers in the deployment of smart communities/cities and their related infrastructure. Therefore, the lack of security in so-called "smart" devices, products, and technologies can exacerbate cybersecurity risks in these communities and cities as they strive to more efficiently deliver services to their citizens and serve other public needs. For example, Kaspersky Lab participates in the Securing Smart Cities initiative,[13] which seeks to raise awareness about, and produce research regarding, cybersecurity risks and known vulnerabilities in technologies as commonplace as traffic cameras and automated kiosks[14] to more emerging use cases like municipal drones for emergency management or infrastructure protection purposes.[15] We assert that local and state governments need to account for security concerns throughout the planning and implementation stages relating to smart cities technology deployment, not only to better ensure that their efforts meet their intended objectives, but also to protect the security, privacy, and in some cases, safety of their residents.

D. Critical Infrastructure Remains a Target

Legacy industrial control systems, used in numerous critical infrastructure sectors such as the energy, electricity, telecommunications, transportation, manufacturing, water and wastewater, chemical, and agriculture sectors, are increasingly being connected to the Internet without appropriate security controls, and therefore, exposing those sectors to increased cybersecurity risks. In the second half of 2016, Kaspersky Lab detected approximately 20,000 different malware samples representing over 2,000 malware families in industrial automation systems, including spyware, backdoors, key-loggers, ransomware, other financial malware, and wipers.[16] The top three sources of cyber-threats to industrial systems included Internet connectivity (22 percent), infected removable storage devices (10.9 percent), and malicious email attachments/malicious scripts embedded in emails (8.1 percent).[17] In addition to these malware detections, Kaspersky Lab also identified 75 vulnerabilities in industrial control systems components, nearly 80 percent of which had a CVSS 3.0 severity score of 7.0 or higher (*i.e.*, high severity).[18] The capabilities of these identified vulnerabilities include remote code execution, denial of service, code injection, file manipulation, and user access account manipulation.[19] According to the

[12] Department of Homeland Security, "Strategic Principles for Securing the Internet of Things," 15 November 2016. https://www.dhs.gov/sites/default/files/publications/Strategic_Principles_for_Securing_the_Internet_of_Things-2016-1115-FINAL_v2-dg11.pdf.

[13] Securing Smart Cities is a not-for-profit global initiative that aims to solve existing and future cybersecurity problems of smart cities through collaboration between companies, governments, media outlets, other not-for-profit initiatives and individuals around the world. For more information, please see here: http://securingsmartcities.org.

[14] Securing Smart Cities, "Fooling a Smart City," 15 September 2016. Link: http://securingsmartcities.org/wp-content/uploads/2016/09/Fooling-smart-city_in_template.pdf.

[15] Securing Smart Cities and Cloud Security Alliance, "Establishing a Safe and Secure Municipal Drone Program," 2 February 2017. Link: http://securingsmartcities.org/wp-content/uploads/2017/02/municipal_drones_FINAL.pdf.

[16] Kaspersky Lab ICS-CERT, "Threat Landscape for Industrial Automation Systems in the Second Half of 2016, "28 March 2017. Link: https://ics-cert.kaspersky.com/wp-content/uploads/sites/6/2017/03/KL-ICS-CERT_H2-2016_report_FINAL_EN.pdf.

[17] *Ibid*.

[18] *Ibid*.

[19] *Ibid*.

World Economic Forum in its Global Risks Report 2017, "[A]s different infrastructure networks become more interdependent, there is also growing scope for systemic failures to cascade across networks and affect society in multiple ways."[20] Kaspersky Lab fully agrees with the Forum when it notes that cyberattacks can contribute to these types of systemic failures.[21]

E. Advanced Persistent Threats (APTs)

Advanced persistent threat (APT) actors continue to increase the sophistication of their attacks by moving away from general, commodity malware and employing customized toolkits that meet their specific needs relating to a particular target. Such customization enables these actors to infect systems in a manner that evades detection because traditional indicators of compromise are less effective.[22] In addition to this evolving level of sophistication, Kaspersky Lab has observed a merger of tactics, techniques, and procedures (TTPs) between APT actors and financially-motivated cybercriminals. For example, these actors are harnessing wipers, both for cyber-enabled sabotage operations and for removing their tracks after cyberespionage operations. Such activity has largely targeted entities in the Middle East, as we saw in the recent Shamoon 2.0 attacks, but Kaspersky Lab has identified similar activity in Europe as well.[23] The Lazarus group, considered by many to be behind the Sony Pictures attack in late 2014, has been linked to a sub-group called BlueNoroff that is actively attacking financial institutions in different regions, including a high profile attack in Poland, and is believed to be behind the infamous Bangladesh Central Bank heists.[24] In addition to cyberespionage and sabotage operations merging with sophisticated financial crime, Kaspersky Lab has identified the use of fileless malware by targeted attackers, where instead of appearing on systems' hard drives, the malicious software hides in the systems' memory. Both targeted threat actors and cybercriminals in general are employing this tactic, which enables them to avoid detection and makes forensic investigations harder.[25]

II. Policy Recommendations to Address Evolving Cyber Threat Landscape

While the cyber threat landscape continues to expand and evolve, there are a number of policy recommendations that Kaspersky Lab maintains will help address the nature of the threat and better protect the networks and systems that govern our daily lives.

A. Public-Private Partnerships for Cyber Threat Information Sharing

Real-time sharing of threat information within and between both the private and public sectors is critical to more effectively find, stop and apprehend cybercriminals; however, the need for collaboration extends far beyond the cybersecurity industry. Technology companies, regional and international governments, law enforcement, Computer Emergency Response Teams (CERTs), along with businesses

[20] World Economic Forum, "The Global Risks Report 2017, 12th Edition," January 2017. Link: http://www3.weforum.org/docs/GRR17_Report_web.pdf.
[21] *Ibid.*
[22] Kaspersky Security Bulletin, "Predictions for 2017: 'Indicators of Compromise' are Dead."
[23] Kaspersky Lab, "From Shamoon to StoneDrill: Wipers Attacking Saudi Organizations and Beyond," *Securelist* blog post, 6 March 2017. Link: https://securelist.com/files/2017/03/Report_Shamoon_StoneDrill_final.pdf.
[24] Kaspersky Lab, "Lazarus under the Hood," *Securelist* blog post, 3 April 2017. Link: https://securelist.com/files/2017/04/Lazarus_Under_The_Hood_PDF_final.pdf.
[25] Kaspersky Lab, "Fileless Attacks against Enterprise Networks," *Securelist* blog post, 8 February 2017. Link: https://securelist.com/blog/research/77403/fileless-attacks-against-enterprise-networks/.

from nearly every industry, should discuss the best ways to collaborate on defending cyber networks and protect against cyber offensive operations globally. As an international cybersecurity company protecting over 400 million users worldwide, Kaspersky Lab fully supports a concept like the Digital Geneva Convention espoused by Microsoft,[26] and Eugene Kaspersky, the company's CEO, has advocated for similar ideas throughout the past several years.[27] This proposal deeply resonates with the company's beliefs that cybersecurity should be separated from politics, and that the IT security industry should be impartial in protecting customers from all possible cyberattacks.

B. Educating the Public and Disrupting Cyber Adversaries

In addition to public-private partnerships to share cyber threat information and protect cyber networks, another key component is global cooperation to educate the general public about cyber hygiene and to empower individuals and enterprises to mitigate against cyberattacks. A successful example of such a partnership is the No More Ransom project, launched in July 2016. No More Ransom is an online resource portal aimed at informing the public about the dangers of ransomware and helping victims to recover their data without having to pay ransom to the cybercriminals.[28] Today, 76 partners from the public and private sectors have joined this global initiative, which has enabled over 10,000 ransomware victims to decrypt their affected devices using the free tools available on the No More Ransom platform without paying the ransom requested by cybercriminals.[29] This partnership is just a small example of the benefits that can result from sharing information, skills and technology to create a safer, more secure digital world.

Beyond No More Ransom, Kaspersky Lab is proud to collaborate with the authorities of many countries and international law enforcement agencies in fighting cybercrime. Examples of this collaboration include the company's continuous work alongside INTERPOL, EUROPOL, the National High Tech Crime Unit (NHTCU) of the Netherlands' Police Agency and The City of London Police, as well as CERTs worldwide. The company also routinely works with local and regional law enforcement to provide technical consultations and expert analysis of malicious programs during investigations and in compliance with court orders.

C. The Role of Cybersecurity Companies and Security Researchers in Protecting the Digital World

As the Committee considers the best technologies, strategies and tools for protecting America from cyberattacks, it is important to highlight the integral role cybersecurity companies play in safeguarding not only customers, but also the digital world overall. For this reason, no technology company should

---

[26] Brad Smith, "The Need for a Digital Geneva Convention," *Microsoft* blog post, 14 February 2017. Link: https://blogs.microsoft.com/on-the-issues/2017/02/14/need-digital-geneva-convention.

[27] Eugene Kaspersky, "Security Without Borders," *Forbes.com* blog post, 18 March 2015. Link: https://www.forbes.com/sites/eugenekaspersky/2015/03/18/security-without-borders/#200cb83210d6.

[28] No More Ransom, www.nomoreransom.org

[29] Europol, "No More Ransom Adds 15 New Decryption Tools As Record Number Of Partners Join Global Initiative," *Europol* Press Release, 4 April 2017. Link: https://www.europol.europa.eu/newsroom/news/no-more-ransom-adds-15-new-decryption-tools-record-number-of-partners-join-global-initiative.

ever help any government with its cyberespionage efforts. IT security companies specifically should investigate and report on any threats discovered, regardless of the origin or purpose.
Kaspersky Lab can say with 100 percent confidence that it has never, and will never develop or assist, any government with their offensive efforts in cyberspace. The company reports on any kind of threat discovered, regardless of which language the threat 'speaks' - Russian, Chinese, Spanish, Arabic, German, or English. To further that point, Kaspersky Lab experts have reported on at numerous attacks with Russian-language included in the code, and these threat actors include (but are not limited to) RedOctober,[30] CloudAtlas,[31] Miniduke,[32] CosmicDuke,[33] Epic Turla,[34] Penquin Turla,[35] CozyDuke,[36] Sofacy[37] and more. Nevertheless, while these language traces provide some insight, they do not conclusively attribute these threat actors to a specific country, as language traces can be deliberately planted in malware code to mislead investigators.

In addition, it is imperative that ethical security researchers, both independent and those employed by cybersecurity vendors, are encouraged to share their findings with governments and affected vendors in a responsible manner, without suffering any repercussions, as this leads to an open forum of strategic collaboration and faster software updates. To that end, Kaspersky Lab fully supports, and abides by, the industry best practice of confidentially reporting vulnerabilities discovered during cybersecurity research, along with relevant information and telemetry, in order to allow vendors adequate time to develop and release security updates that protect users. In addition, as a security vendor itself, Kaspersky Lab supports the use of coordinated vulnerability disclosure programs like bug bounties to incentivize security researchers to test and improve the resiliency of its own products. We applaud the government agencies that are participating in bug bounty programs, which will help identify and resolve security vulnerabilities associated with those U.S. government, public-facing websites.

Conclusion

When examining cyber threats facing America, it is important to consider not only the threats, but also the solutions to help address those challenges directly. One of the most important pieces of this complex puzzle is greater collaboration among governments and the private sector worldwide, which is

[30] Kaspersky Lab, "Red October" Diplomatic Cyber Attacks Investigation," *Securelist* blog post, 14 January 2013. Link: https://securelist.com/analysis/publications/36740/red-october-diplomatic-cyber-attacks-investigation/.
[31] Kaspersky Lab, "Cloud Atlas: RedOctober APT is back in style," *Securelist* blog post, 10 December 2014. Link: https://securelist.com/blog/research/68083/cloud-atlas-redoctober-apt-is-back-in-style/.
[32] Kaspersky Lab, "The MiniDuke Mystery: PDF 0-day Government Spy Assembler 0x29A Micro Backdoor," *Securelist* blog post, 27 February 2013. Link: https://securelist.com/blog/incidents/31112/the-miniduke-mystery-pdf-0-day-government-spy-assembler-0x29a-micro-backdoor/.
[33] Kaspersky Lab, "Miniduke is back: Nemesis Gemina and the Botgen Studio," *Securelist* blog post, 3 July 2014. Link: https://securelist.com/blog/incidents/64107/miniduke-is-back-nemesis-gemina-and-the-botgen-studio/
[34] Kaspersky Lab, "The Epic Turla Operation," *Securelist* blog post, 7 August 2014. Link: https://securelist.com/analysis/publications/65545/the-epic-turla-operation/
[35] Kaspersky Lab, "The 'Penquin' Turla," *Securelist* blog post, 8 December 2014. Link: https://securelist.com/blog/research/67962/the-penquin-turla-2/
[36] Kaspersky Lab, "The CozyDuke APT," *Securelist* blog post, 21 April 2015. Link: https://securelist.com/blog/research/69731/the-cozyduke-apt/
[37] Kaspersky Lab, "Sofacy APT hits high profile targets with updated toolset," *Securelist* blog post, 4 December 2015. Link: https://securelist.com/blog/research/72924/sofacy-apt-hits-high-profile-targets-with-updated-toolset/

why hearings and public discussions like the one today are crucial. They help to educate the U.S. public and organizations around the globe, on the importance of working together to address weaknesses in cybersecurity. Since cyber threats do not recognize geographical borders and the threat landscape is constantly evolving, collaboration is the necessary path to protect our digital lives, economy and critical infrastructure. Kaspersky Lab appreciates the opportunity to share some its learnings from 20 years in the IT security industry, as well as possible solutions to help address the cyber threats facing America. If the company may provide additional information or serve as a resource in the future, please let us know.

June 26, 2017

The Honorable Ron Johnson
Chairman
United States Senate
Committee on Homeland Security
& Governmental Affairs
Washington, DC 20510

The Honorable Claire McCaskill
Ranking Member
United States Senate
Committee on Homeland Security
& Governmental Affairs
Washington, DC 20510

Dear Chairman Johnson and Ranking Member McCaskill:

It was a privilege to testify before the recent Committee on Homeland Security and Governmental Affairs hearing on "Cyber Threats Facing America: An Overview of the Cybersecurity Threat Landscape." Attached are my responses to the Questions for the Record.

Thank you again for the opportunity to testify and to provide these further responses.

Sincerely,

Jeff Greene
Senior Director, Global Government Affairs and Policy
Symantec Corporation

Post-Hearing Questions for the Record
Submitted to Jeff Greene
Senator Claire McCaskill

"Cyber Threats Facing America: An Overview of the Cybersecurity Threat Landscape"

May 10, 2017

Understanding the Threat

Adversaries are becoming increasingly audacious in their attacks. The Deputy Director of the National Security Agency Richard Ledgett described efforts to push attackers, reportedly the Russians, out of the State Department's systems as "hand to hand combat."

Other sophisticated cyber adversaries like China and Iran are becoming more aggressive, as well. As these bad actors broaden their targets beyond the government, it seems natural that the private sector is next.

- How can the government better improve its ability to combat these threats?

As cyber-attacks become increasingly more sophisticated the immediate reaction is to counter with equally sophisticated defenses. This is important – and necessary – but even the most sophisticated defense relies to some degree on getting the fundamentals of cybersecurity right. So even as we develop sophisticated defenses we should not neglect the basics, which must include upgrading legacy systems that are not, and often cannot be, protected. Within the government, the DHS Continuous Diagnostics and Mitigation (CDM) Program, and the NIST Cybersecurity Framework (CSF) both start with cybersecurity fundamentals and build to more advanced protections. Emerging defensive tools include machine learning, artificial intelligence, and automation. Good hygiene and practices combined with these cutting-edge tools are the way to keep pace with the attackers.

- Are you seeing in the private sector that adversaries are becoming more aggressive in the threat landscape?

Adversaries have definitely become more aggressive and audacious in their attacks over the last few years. Over the last 18 months we have seen a multi-million dollar virtual bank heist, explosive growth of ransomware, attempts to disrupt the US electoral process by state-sponsored groups, some of the biggest distributed denial of service (DDoS) attacks on record powered by a botnet of Internet of Things (IoT) devices, and the global WannaCry Ransomware epidemic last month that impacted Britain's National Health Service (NHS) and Spanish telecom provider Telefonica. After a day, WannaCry had infected more than 230,000 computers in over 150 countries. Symantec linked the WannaCry attacks to the Lazarus Group, which the FBI has associated with North Korea. There is little doubt that attackers are evolving and becoming more aggressive.

Improving the Cyber Workforce

In my opinion, cybersecurity is more about people than technology. The federal government, state governments, and the private sector are struggling to recruit and retain qualified cybersecurity professionals.

- Do you believe our education system is producing qualified cybersecurity professionals and what are your recommendations for improvement? (See below)

Congress has done a lot in recent years to provide the federal government with additional authorities to hire cybersecurity professionals, but agencies have been slow to implement them.

- What suggestions do you have on ways the federal government could recruit and retain a qualified cybersecurity workforce?
- Do you have suggestions on how to make the federal government a more enticing place for cyber professionals to work?

Today, there are an estimated 1 million cybersecurity jobs in the U.S. that supposedly cannot be filled. We believe that many of these can in fact be filled and that a new approach to how we train and promote IT professionals generally will help solve this problem. There are many general IT professionals in both government agencies and in businesses around the world, and with in-house training they could become specialized security professionals. Their roles could in turn be filled by junior IT professionals or even recent graduates. Looking to existing IT staff to train for a security roles has several benefits – these personnel will already know an organizations' systems, and providing another opportunity for career growth will improve retention and job satisfaction. Training the current IT workforce in cybersecurity is also fiscally smart, as it allows governments and enterprises to cut down their contract workforce and train from within, leading to a more secure IT environment.

We do this at Symantec, in part by conducting an annual "Cyber War Games" exercise. This exercise takes IT professionals from 10 regions around the world and creates scenarios to encourage innovative thinking and growth in cybersecurity skills. These types of activities allow us to find hidden expertise in current employees as well as new expertise to bolster our own workforce. In addition, Symantec created the Symantec Career Connection (SC3). SC3 is an innovative program designed to help close the cybersecurity workforce gap while creating meaningful career paths for underrepresented young adult and veterans. Through targeted classroom education combined with hands on training, SC3 graduates are working amongst many of the world's largest companies.

Security of Devices

- What steps can be taken to incentivize better security on Internet of Things (IoT) devices, despite that many are not produced in the United States, and U.S.-only standards will not fully address this problem?

Several years ago I attended one of the first IoT-focused conferences, and one of the few security-related presentations was built around a simple rule: "Don't be Dumb." The presenter elaborated, saying that "[t]he basics of internet security haven't gone away." This is absolutely true, and applies equally to the incentive structures around securing the IoT; we need to be smart about incentivizing security, and we need to look at what worked – and did not work – to incentivize internet security.

Today most market incentives actively work against security; they are heavily skewed towards being "first to market," and there is rarely a benefit to being "secure to market." Government can shift these incentives a number of ways, including through legislation and regulation, changes in liability, and its purchasing power. Foreign manufacturers who wish to do business in the United States are subject to US laws, and any changes in US policy should be structured to maximize our influence with them.

But security must also be a mindset, and an over-emphasis by some on offering organizations incentives to secure their data and systems has sent the wrong message. Businesses do not lock their doors at night because they were offered an incentive to do so; they lock their doors so their goods are not stolen. It is a basic security step that they would be foolish not to take. We are far past the point where organizations should be viewing cybersecurity similarly – a basic security precaution that must be taken. In the IoT context, manufacturers need to start designing security into devices, and if government focuses too heavily on creating incentives to do so it is sending the not-so-subtle message that security is somehow an "extra" or an "add-on" rather than a foundational piece. It is therefore important to make sure that any incentives are structured to foster, and not undermine, a security mindset.

Role of the Government

The governmental plays a critical role in cybersecurity. The responsibility of guarding our nation's cyber infrastructure falls to a number of different agencies.

- In your opinion, is the United States government properly organized to protect against a cyberattack?
- Is there a national cyber strategy in place to combat cyber threats and keep the country safe?
- Do you think we need a national cyber strategy and if so, what should it involve?
- What are your recommendations on how to improve the organization of federal agencies to combat cyber threats?

Our national security apparatus was organized long before cybersecurity was seen as a major threat vector. With that said, the two previous Administrations recognized the growing importance of cybersecurity and tried to work within existing structures to respond to the threat. President Bush's Comprehensive National Cybersecurity Initiative and President Obama's Cybersecurity National Action Plan set the foundation for a whole-of-government approach to the problem. The recent Executive Order entitled Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure (E.O. 13800) built on this work. We believe that working toward a broader national strategy is worthwhile – but it is important that the underlying operational work that is now going on not be paused while the plan is being developed.

In terms of civilian agencies, the government has matured greatly over the past decade and has handled recent incidents such as WannaCry and others relatively well. We believe that a civilian agency should take the lead on working with the private sector, and DHS has made significant strides in this area. However, we do believe that DHS's efforts could be enhanced if its cyber capabilities were grouped together in a single, operational component.

Deterrence

In a January 6, 2017 report issued by the Office of the Director of National Intelligence (ODNI), the Central Intelligence Agency (CIA), the Federal Bureau of Investigations (FBI), and the National Security Agency (NSA) assessed with high confidence that Russia launched a robust influence campaign in the United States. The report explained that the purpose of the campaign was "to undermine public faith in the US democratic process," and that "Russia's intelligence services conducted cyber operations against targets associated with the 2016 US presidential election."

- Do you have any reason to doubt the Intelligence Community's assessment that, "Russia's intelligence services conducted cyber operations against targets associated with the 2016 US presidential election, including targets associated with both major US political parties"?

No.

- What mechanisms are most effective to deter nation-state cyberattacks?
- What steps should the United States take to prevent similar cyberattacks in the future?

Like their criminal counterparts, nation-state actors can best be deterred by increasing the overall cost associated with their behavior. To do so the government should use all appropriate levers of national power. Defense is also a part of deterrence, and neutralizing the less sophisticated actors by disrupting known, preventable attacks will drive up the cost for any attacker. This also allows us to focus on the more sophisticated nation-state actors. At the same time, the US Government should work to establish internationally recognized cyber norms to help promote "rules of the road" and help deter nation-state attacks. In cyberspace, as in the physical domain, norms will not deter rogue Nations, but rather create lanes that allow law-abiding countries to know when others have crossed the line. They also provide a basis for the international community to publicly rebuke the offending state actor. The Administration should use other tools at their disposal as well, such as using sanctions described in Executive Order 13757 (Taking Additional Steps to Address the National Emergency With Respect to Significant Malicious Cyber-Enabled Activities) where appropriate and criminal prosecution whenever possible. Direct negotiations have had some positive results in the past. For instance, it was widely reported that the Obama-Xi cyber accord in 2015 led to a decline in China-based economic espionage against US interests.

Post-Hearing Questions for the Record

Submitted to Jeff Greene
Senator John McCain

"Cyber Threats Facing America: An Overview of the Cybersecurity Threat Landscape"

May 10, 2017

In your prepared remarks you state: "Cybersecurity is the proverbial journey, not a destination. Understanding the threat, how it is changing, and where it is going, is essential if we are going to stay on track in this journey. This hearing is an important step in advancing that understanding."

- Do you believe that the United States is on the 'right track' on the journey to secure our cyberspace? If not, what would you do differently?

We are making slow, incremental progress on the journey – awareness of the threat has increased, defenses are improving, the NIST Cybersecurity Framework created a common nomenclature for assessing cyber risk, some economic espionage activity declined dramatically in recent years, and cybercriminals are being indicted and at least one occasion extradited to the US for prosecution. Conversely, every day brings press coverage of another major breach; attacks are growing more sophisticated, too many organizations are still failing to take basic security precautions, and some in government (and industry) still use older, unsecurable systems.

To continue the journey analogy, we are broadly moving in the right direction – but constant course corrections are necessary. Some are relatively minor, such as educating the public in new threats or adapting defenses to stop crypto-ransomware instead of just scareware. Some are in our mindset, such as viewing cybersecurity as a foundational fact of doing business (like locking a store's doors at night to protect inventory) rather than an option or an "add-on."

Some, however, are significant, such as rethinking how we protect key government and national security systems. To date we have relied largely on commercial tools. At minimum, we should be asking hard questions about whether this approach has worked and whether it will continue to work. In order to protect our most critical national assets, it may well be necessary to build specialty protection tools.

- In developing a policy and strategy towards cyberattacks, what do you believe constitutes an act of war in cyberspace? To what extent does cyber work within the existing international legal framework?
- In your opinion, do you believe the new administration will be instrumental in the United States' approach to deterring and preventing cyber threats? And if so, how?

There is no generally accepted definition of "cyber war," but a common understanding includes actions by a nation state to attack and attempt to damage another nation's computers, information networks, or physical infrastructure through cyber means. Nation state attacks have increased in sophistication and number in recent years, and more nations are developing capabilities in this area. Some nations are testing the limits of what will be viewed as an attack. For this reason is it is essential that the US Government take the lead and work with their global partners to establish internationally recognized cyber norms to help promote "rules of the road" for the Internet. In cyberspace, as in the physical domain, norms will not deter rogue Nations, but rather create lanes that

allow law-abiding countries to know when others have crossed the line. They also provide a basis for the international community to publicly rebuke the offending state actor.

The US must take a leadership role in developing effective international strategies to deter and prevent cyber attacks. In addition to working with the global community in developing internationally recognized cyber norms, the US should use all of the tools of national power to deter and prevent cyber threats, such as sanctions and holding cybercriminals accountable no matter where they reside.

The prior administration placed a strong emphasis on developing defensive cyber strategies. While appropriate, I am concerned that a denial-only strategy is likely impossible.

- Do you agree that a deterrence strategy in cyber must include both offense and defense?
- What cyber policy questions do you believe are receiving enough attention and deserve additional consideration by this Committee or the Executive Branch?

Defensive measures alone are not deterrence; they are, as the name states, defensive. A comprehensive deterrence strategy is built on a good defense but must also include some elements that dissuade attackers. This is a role for government, whether through indictments, prosecutions, public "name and shame" efforts, or offensive measures.

Government needs to take a hard look at where the market has failed to drive cybersecurity. The Internet of Things is one example; billions of devices are coming online, most of which lack basic security. The Mirai Botnet last fall was the proverbial canary in the coalmine, and demonstrated how insecurity in the IoT could impact national and economic security. If this is not aggressively addressed, we will be living with the consequences for generations. Over the past years, voluntary, consensus-driven efforts such as the NIST Cybersecurity Framework have been very successful in improving both security awareness and actual security. But there is a limit to how far a voluntary process will go, and the Committee and the Executive Branch should identify any gaps – such as IoT security – and look for ways that government can address them.

Post-Hearing Questions for the Record
Submitted to Jeff Greene
Senator Jon Tester

"Cyber Threats Facing America: An Overview of the Cybersecurity Threat Landscape"

May 10, 2017

Rural Utilities

How do you recommend we increase the resiliency of our rural utility companies and cooperatives against cyber threats?

To your knowledge, does the federal government, whether through USDA's Rural Utilities Service or DHS, provide rural utility companies and cooperatives with the tools they need to improve reliability, resilience, and security of the electric grid against cyber attacks?

I am not familiar with a program focused on providing cybersecurity resources to rural utilities. However, electrical grids have long been identified as at risk, and both the Bush and Obama Administration took steps to mitigate vulnerabilities. The NIST Cybersecurity Framework is a good starting point for rural utilities to assess risk and develop plans to address any identified gaps. In addition NIST has released several publications on smart grid security, and some private entities have published use cases for the Framework in the electric grid.

Small Businesses

According to the Small Business Administration, there are more than 28 million small businesses across the U.S., and many of them in rural America are critically dependent on IT.

1. What general recommendations do you have to strengthen how small and medium-sized businesses can protect their networks and IT from cyber threats?

Cybercrime has continued to grow over the last few years, and we have seen an increased focus on small and medium sized businesses. Today many of the attacks plaguing large companies are also directed at small and medium sized businesses. There are a number of things a small business can do to help protect themselves, including:

1. ***Training employees in security principles and raising awareness of the threat.***
2. ***Deploying the latest security software, firewall, web browser, and operating system.***
3. ***Regularly backing up essential data.***
4. ***Securing Wi-Fi networks.***
5. ***Controlling access and creating individual user accounts for each employee.***
6. ***Deploying strong password and authentication standards.***

In addition, the Small Business Administration and the Federal Communications Commission (FCC) offer resources to help small and medium sized businesses protect themselves from cyber attacks.

2. Would better guidance from the National Institute of Standards and Technology (NIST) help small businesses fight digital threats?

Late last year NIST developed cybersecurity reference guidelines for small businesses. The guidelines ***were intended to present the fundamentals of a small business information security program in non-technical language. We need some time to assess this publication in practice before determining if***

additional guidance is needed. Too much guidance can be as paralyzing as too little – if this publication is working well we should focus on refining and updating it.

Election Hacks

How would you recommend that state U.S. election systems increase their resiliency to outside hacking or interference?

What countermeasures would you recommend that election boards, candidates, and state and local governments take to ensure that their data is secure and that they are not subject to the kind of foreign election interference we saw in 2016?

We need to secure the election system as we would any other critical infrastructure and employ a defense-in-depth strategy, which emphasizes multiple, overlapping, and mutually supportive defensive systems to guard against single-point failures. Other urgent priories should include updating legacy systems, employing modern security software and educating users about the potential threats.

United States Senate Committee on
Homeland Security and Governmental Affairs
Hearing Entitled "Cyber Threats Facing America:
An Overview of the Cybersecurity Threat Landscape"

May 10, 2017

Responses of Steven Chabinsky to
Post-Hearing Questions for the Record

I. Questions from Ranking Member Claire McCaskill

A. Understanding the Threat. Adversaries are becoming increasingly audacious in their attacks. The Deputy Director of the National Security Agency Richard Ledgett described efforts to push attackers, reportedly the Russians, out of the State Department's systems as "hand to hand combat." Other sophisticated cyber adversaries like China and Iran are becoming more aggressive, as well. As these bad actors broaden their targets beyond the government, it seems natural that the private sector is next.

Question 1: *How can the government better improve its ability to combat these threats?*
Response: It is my belief that the United States already has the ability to counter the full range of cyber threats, including those perpetrated by nation-state actors. However, it also is my belief that the proper framework is not yet in place with which to assess the government's full range of options and to improve decision-making. While significant progress has been made in terms of detecting and attributing incidents, less progress has been made in determining our options (both incentives and disincentives) to address threat actors.

In this regard, the following three steps would prove helpful:

(1) Identify and address high security environments that have low privacy requirements. In particular, improved cybersecurity across the critical infrastructure likely would result from focusing on the people, processes, and technologies required to enhance timely and effective detection, attribution, and penalty in response to attacks, and from the US leading the establishment of international norms regarding critical infrastructure cyber infiltration or attack. We are likely to find that many of the systems that require the greatest security coincidentally have the lowest privacy requirements as to user identification and activities, resulting in increased opportunities for public/private collaboration.

(2) Resource and train professional intelligence analysts across different branches of government to review cyber response options. Career cyber options intelligence analysts should be spread across and take into account the full DIME/LE range of

options and elements of national power (Diplomatic, Information, Military, Economic, and Law Enforcement) across government and the private sector. Response opportunities might be broken down further to account for the most effective roles of government operating without industry, industry working without government, and government and industry working in coordination with one another, both domestically and internationally. "Cyber Options Analysis" also should identify the intelligence gaps that exist with respect to confidence levels (how certain we are that a particular action would result in a particular outcome for a specific scenario) and should be part of the intelligence collection and analysis cycle; and

(3) Drive the cybersecurity problem further away from end users. Efforts should include (a) greater threat deterrence and response through the full range of DIME/LE options; (b) higher level threat and vulnerability mitigation solutions at the Internet Ecosystem level, starting with global botnet remediation efforts; (c) more secure hardware and software, beginning with labeling and rating systems; and (d) the collection, analysis, and distribution of better measures and metrics that demonstrate how our efforts are matching up against the evolving threat.

Question 2: *Are you seeing in the private sector that adversaries are becoming more aggressive in the threat landscape?*
Response: Yes, over time adversaries have become more aggressive and more destructive, and I believe this trend will continue. I also believe that our current cybersecurity strategy is, in large part, responsible for escalating the threat landscape. As long as our primary approach to countering hackers is to try to deny them unauthorized access to systems, rather than to identify and penalize them for attempting to access the systems, they will keep attacking.

B. Improving the Cyber Workforce. In my opinion, cybersecurity is more about people than technology. The federal government, state governments, and the private sector are struggling to recruit and retain qualified cybersecurity professionals.

Question 3: *Do you believe our education system is producing qualified cybersecurity professionals and what are your recommendations for improvement*?
Response: I agree that people are an important component of cybersecurity. I also think that our current reliance on people is a problem, because there never will be enough qualified cybersecurity professionals to stem the risks posed by our current cybersecurity strategy. Nor should there be. I am concerned that, because we are pursuing a failed strategy, we are encouraging and developing the few STEM minds our nation has to be part of the sunk costs of security. A successful cybersecurity strategy would reduce our need for a large cybersecurity workforce, not fulfill our need for a large cybersecurity workforce. By way of analogy, when faced with a town arsonist, we look to catch the arsonist (and perhaps improve building design and materials) rather than train an endless supply of firefighters. Still, until we improve our strategy, I believe that the best short term gains likely will be found by training individuals who can more effectively implement existing and emerging *technical* controls. For further information in this regard, I respectfully refer the Committee to my writings in *Security* magazine at:

http://www.securitymagazine.com/articles/87215-making-the-most-of-protective-cybersecurity-technology

I believe our education system is producing qualified cybersecurity professionals. I also believe that continuing education, and on-the-job-training, is essential in the development of these skillsets. In this regard, I commend the goals of the National Initiative for Cybersecurity Careers and Studies, and the National Cybersecurity Workforce Framework. Additionally, for years I have advocated that apprenticeships can be used to address more of our cybersecurity needs. In this regard, I fully support the recommendation of the Commission on Enhancing National Cybersecurity, Action Item 4.1.2, which calls for the current Administration to initiate a national cybersecurity apprenticeship program to train 50,000 new cybersecurity practitioners by 2020, and I fully support the goals of President Trump's Executive Order Expanding Apprenticeships in America, and similar considerations of apprenticeships within the Presidential Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure.

Question 4: *Congress has done a lot in recent years to provide the federal government with additional authorities to hire cybersecurity professionals, but agencies have been slow to implement them. What suggestions do you have on ways the federal government could recruit and retain a qualified cybersecurity workforce?*
Response: In order to recruit and retain a qualified cybersecurity workforce within the federal government, the following recommendations of The Commission to Enhance National Cybersecurity are noteworthy:

- The federal government should develop a mandatory training program to introduce managers and executives to cybersecurity risk management topics so that they can create a culture of cybersecurity in their organizations.
- The federal government should create an exchange program with private organizations (and State, Local, Tribal and Territorial governments) aimed at increasing the cybersecurity experience and capabilities of mid-level and senior-level employees.
- The Office of Personnel Management (OPM) should establish a Presidential Cybersecurity Fellows program for federal civilian agencies.
- NIST, the National Science Foundation (NSF), the National Security Agency (NSA), and the Department of Education should work with private-sector organizations, universities, and professional societies to develop standardized interdisciplinary cybersecurity curricula that integrate with and expand existing efforts and programs.
- Incentives should be offered to reduce student debt or subsidize the cost of cybersecurity education (and/or apprenticeships and certification courses) for government employees.

Question 5: *Do you have suggestions on how to make the federal government a more enticing place for cyber professionals to work?*
Response: The federal government can make significant strides by creating a model apprenticeship program that brings onboard individuals with little to no experience and follows a strict curriculum that offers them (a) solid training across numerous areas of expertise and within cutting edge lab environments, (b) hands-on experience, (c) mandatory rotational assignments with other government agencies (and perhaps the private sector), and at different skill levels throughout their career, and (d) promotional opportunities and salary increases based on work performance and obtaining industry-recognized certifications; all in return for committing to a set number of years working for the government.

C. Security of Devices

Question 6: *What steps can be taken to incentivize better security on Internet of Things (IoT) devices, despite that many are not produced in the United States, and U.S.-only standards will not fully address this problem?*
Response: I fully support the recommendation of the Commission on Enhancing National Cybersecurity, Recommendations 2.1 and 3.1, to include:

- Develop Guidelines. Agencies that currently regulate IoT devices should follow the example of the National Highway Traffic Safety Administration (NHTSA) and work with industry to develop voluntary and collaborative guidelines to secure IoT devices. For example, automotive manufacturers have called for a consistent set of federal guidelines for autonomous vehicles, and they have worked with the NHTSA on such rules;
- Empower Market Forces. To promote greater transparency in security design and deployment, and for voluntary adoption by major private sector and government purchasers of technology (including but not limited to IoT devices), the government should facilitate an independent organization to develop the equivalent of a cybersecurity "nutritional label" for technology products and services—ideally linked to a rating system of understandable, impartial, third-party assessment that consumers will intuitively trust and understand

D. Role of the Government. *The governmental plays a critical role in cybersecurity. The responsibility of guarding our nation's cyber infrastructure falls to a number of different agencies.*

Question 7: *In your opinion, is the United States government properly organized to protect against a cyberattack?*
Response: Yes. Or, stated differently, I do not believe that organizational issues are significant, and I believe that tendencies to reorganize help institutionalize and exacerbate rather than correct problems relating to strategy, resources, execution, and metrics.

Question 8: *Is there a national cyber strategy in place to combat cyber threats and keep the country safe?*
Response: There are multiple strategies, dating back to PDD 63 and the Comprehensive National Cybersecurity Initiative, the foundations of which remain in place to this day. However, it is fair to say that the largest resource allocations go into end-user vulnerability mitigation (including agency information security programs) rather than ecosystem-level remediation and threat mitigation.

Question 9: *Do you think we need a national cyber strategy and if so, what should it involve?*
Response: Yes, a cohesive strategy is necessary. I believe that significant strides could be made by updating our national strategy to include the recommendations offered in response to Question 1 above. In addition, we need to make consistent policy choices. For example, it is peculiar that we pass legislation financially incentivizing medical providers to digitize sensitive patient healthcare information (see the American Recovery and Reinvestment Act of 2009), while at the same time acknowledging that it is not "if" a company is going to get hacked, but "when." Essentially, through inconsistent policy choices, we have accepted and helped facilitate the inevitability of stolen, altered, or destroyed confidential medical records relating to every American.

Question 10: *What are your recommendations on how to improve the organization of federal agencies to combat cyber threats?*
Response: My view is that re-organization should be a last resort and at the moment a low priority. Instead, it would be far better to focus on improving metrics and execution, and reviewing resource allocation, of existing strategies within existing operational and organizational constructs. For example, years ago the budget allocated across agencies as part of the Comprehensive National Cybersecurity Initiative was tied to OMB-driven metrics, results were tracked and assessed by a multi-agency task force (over which I presided) within the Office of the Director of National Intelligence, and reports were presented quarterly to the President with recommendations. To my knowledge, that type of national-level strategic accountability and assessment no longer exists.

E. *Deterrence.* *In a January 6, 2017 report issued by the Office of the Director of National Intelligence (ODNI), the Central Intelligence Agency (CIA), the Federal Bureau of Investigations (FBI), and the National Security Agency (NSA) assessed with high confidence that Russia launched a robust influence campaign in the United States. The report explained that the purpose of the campaign was "to undermine public faith in the US democratic process," and that "Russia's intelligence services conducted cyber operations against targets associated with the 2016 US presidential election."*

Question 11: *Do you have any reason to doubt the Intelligence Community's assessment that, "Russia's intelligence services conducted cyber operations against targets associated with the 2016 US presidential election, including targets associated with both major US political parties"?*
Response: No.

Question 12: *What mechanisms are most effective to deter nation-state cyberattacks?*
Response: I believe that the incentives and disincentives to effect nation-state cyberattacks differ by country, and the identities of who best can influence nation-state behavior also differs by country. Unfortunately, it appears that we may not have adequately invested in understanding these motivations in relation to our elements of national power. For this reason, I recommend that we resource and train professional intelligence analysts across different branches of government to review cyber response options that take into account the full DIME/LE range of options and elements of national power (Diplomatic, Information, Military, Economic, and Law Enforcement). These options should be broken down further to account for the most effective roles of government operating without industry, industry working without government, and government and industry working in coordination with one another, both domestically and internationally. Cyber Options Analysis also should identify the intelligence gaps that exist with respect to confidence levels (how certain we are that a particular action would result in a particular outcome for a specific scenario) and should be part of the intelligence collection and analysis cycle. It is typical for Congress and the President to receive reports assessing the nature of a major incident, how it happened and who was responsible, all accompanied with levels of confidence. Unfortunately, it is relatively uncommon for the same reports to answer the question, "what are our options to address it, and what are the likely positive and negative outcomes?"

Question 13: *What steps should the United States take to prevent similar cyberattacks in the future?*
Response: Please refer to the prior response to Question 12 regarding enhancing the rigor of multi-disciplinary options analysis.

II. Questions from Senator John McCain

A. In your prepared remarks you noted that you were convinced we are currently going in the wrong direction and that if we continue at the current rate, the overall cyber threats against our country will continue to grow at unsustainable levels.

Question 14: *In your opinion what direction do you believe is the correct direction and how as a nation can we get there?*
Response: The single greatest change we can make in our strategic direction is to drive the cybersecurity problem further away from end users. The United States should help lead well-resourced, international, public/private efforts that include (a) greater threat deterrence and response through the full range of DIME/LE options; (b) higher level threat and vulnerability mitigation solutions at the Internet Ecosystem level, starting with global botnet remediation efforts; (c) more secure hardware and software, beginning with labeling and rating systems; and (d) the collection, analysis, and distribution of better measures and metrics that demonstrate how our efforts are matching up against the evolving threat and whether the totality of our cybersecurity is improving or getting worse over time. Unfortunately, instead of these initiatives, we spend inordinate time and money requiring agencies, industries, and consumers to

adopt risk management frameworks and protect their own systems against powerful, relentless adversaries.

Question 15: *Thus far, how successful have we been in deterring our adversaries and demonstrating that the consequences of an attack in cyberspace will outweigh the benefits?*
Response: Many of our adversaries have significant capabilities to harm our critical infrastructure, not only through military means, but through cyber means as well. Yet, none have. This would appear to be due to effective deterrence. Efforts under the prior Administration to define and implement norms relating to economic cyber espionage also appear to have been impactful. In addition, efforts to coordinate international law enforcement investigations and response also have shown positive results to counter cybercrime. The current Administration's focus on botnet remediation is encouraging, and can prove successful in identifying and deterring large scale criminal and nation-state cyber intrusions.

B. The prior administration placed a strong emphasis on developing defensive cyber strategies. While appropriate, I am concerned that a denial-only strategy is likely impossible.

Question 16: *Do you agree that a deterrence strategy in cyber must include both offense and defense?*
Response: Yes, a meaningful deterrence strategy in cyber should have the capacity to draw from all elements of national power, to include offensive and defensive capabilities.

Question 17: *What cyber policy questions do you believe are [not] receiving enough attention and deserve additional consideration by this Committee or the Executive Branch?*
Response: I believe that we are not focusing sufficiently on the market incentives and market failures of cybersecurity, and that we should financially incentivize the goal of resolving more cybersecurity risks at the source, before they spread to consumers, businesses, and critical infrastructure. By way of analogy, when faced with the Flint Michigan water crisis, a federal state of emergency was declared, and solutions are being put in place to repair and upgrade the city's water system and to replace the pipes. Nobody would imagine opting instead for a solution to require every home and every business operating in Flint to purchase their own state of the art water filtration system along with the experts needed to continuously monitor and upgrade them.

To move forward with purpose, the Federal government should publish a Request for Proposal seeking innovative solutions. Financially incentivizing the private sector to solve the problem should be considered a budget priority, with perhaps as much as ten percent of our roughly $600 billion defense budget being set aside for the advancement of higher level cybersecurity solutions. In addition, we should consider expanding the telecommunications model we have in place to Connect America, which created a fund to expand rural access to voice and broadband, by implementing a program to Protect America by establishing a fund to extend cybersecurity across all of America. We often

hear leaders say the private sector is on the front lines of cybersecurity. I agree, and it is well past time we pay them to defend us, and allow them to make a healthy profit doing so.

III. **Questions from Senator Jon Tester**

A. *Rural Utilities*

Question 18: *How do you recommend we increase the resiliency of our rural utility companies and cooperatives against cyber threats?*
Response: I support the goal of strong resiliency of our rural utility companies and cooperatives against cyber threats. Unfortunately, I have not had an opportunity to review the current state of their resiliency (either individually or as a whole) that would be necessary to support a view on whether current resiliency efforts are insufficient and what controls might be increased with cost effectiveness. It would be my privilege to help the Committee in support of such a review.

Question 19: *To your knowledge, does the federal government, whether through USDA's Rural Utilities Service or DHS, provide rural utility companies and cooperatives with the tools they need to improve reliability, resilience, and security of the electric grid against cyber attacks?*
Response: I have not had an opportunity to review USDA or DHS resources that may be available specifically for rural utility companies and cooperatives to better secure the electric grid.

B. *Small Businesses. According to the Small Business Administration, there are more than 28 million small businesses across the U.S., and many of them in rural America are critically dependent on IT.*

Question 20: *What general recommendations do you have to strengthen how small and medium-sized businesses can protect their networks and IT from cyber threats?*
Response: I support the recommendations found in NIST's current guidance entitled Small Business Information Security: The Fundamentals (NISTIR 7621). Also helpful, is the FCC's "cyberplanner" (developed with input from industry and other agencies).

Question 21: *Would better guidance from the National Institute of Standards and Technology (NIST) help small businesses fight digital threats?*
Response: NIST's current guidance entitled Small Business Information Security: The Fundamentals (NISTIR 7621) already provides helpful guidance. There is merit in NIST continuing to seek comment and revise the document over time to account for changes in technology and best practices. Since 2002, NIST along with the Small Business Administration and the Federal Bureau of Investigation's InfraGard program, has conducted research and outreach to small businesses. Continuation of those

efforts, with adequate resources, likely will lead to further revisions of NISTIR 7621, which in turn will provide sustained and improved guidance over time.

C. *Election Hacks*

Question 22: *How would you recommend that state U.S. election systems increase their resiliency to outside hacking or interference?*
Response: I would recommend that States participate in the testing and certification program of the U.S. Elections Assistance Commission (EAC), and that Congress ensure sufficient funding of EAC functions, the Voting System Test Laboratories, and the Technical Guidelines Development Committee. Congress also should ensure sufficient funding for States to meaningfully purchase, install, conduct security testing, and maintain certified voting systems, especially for any systems used in federal elections.

Question 23: *What countermeasures would you recommend that election boards, candidates, and state and local governments take to ensure that their data is secure and that they are not subject to the kind of foreign election interference we saw in 2016?*
Response: Certified voting systems should include adequate incident detection, logging and reporting functions, and security incident information should be shared with and assessed at the national level by DHS and the FBI.

///

Post Hearing Questions for Record
"Cyber Threats Facing America"
Committee on Homeland Security and Governmental Affairs

Brandon Valeriano, Ph.D.
Marine Corps University, Donald Bren Chair of Armed Politics
Niskanen Center, Adjunct Fellow of Cyber Security
drbvaler@gmail.com
June 16, 2017

I thank the Senate Homeland Security Committee for giving me the opportunity to provide testimony on cyber security issues. Since my testimony in early May of 2017, we have seen a proliferation of cyber incidents signifying a shift in the landscape. This shift further enhances the idea that are we are in a new era of cyber conflict where political warfare is the main strategy and information is the target. We continue to avoid all out "cyber war", but have seen a proliferation of disruption and manipulation events.

The goal now is to manipulate the enemy to change position, cause chaos, and prepare for possible future conflicts but infiltrating as many critical targets as possible. This new era moves us past the recent evident cyber restraint, where states have exhibited hesitancy to attack each other. Instead these low-level disruption and manipulation events are dangerous in that they suggest a breaking of traditional norms and the possibility of causing escalation, a process recently seen used against Qatar after a manipulation event attributed to Russia.[1]

These developments suggest that evidence, research, and talent are needed now more than ever. The current developing era of cyber conflict is not one where outright battles will be fought through hand to hand cyber combat, but behind closed doors, in secret to avoid evident responsibility for unleashing cyber malice. Preventing this new era of cyber conflict from negatively impacting the United States will require talent that must be utilized to reveal compromised systems, alert to deception efforts, and fight back against the manipulation of data. My answers to the questions below support this general theme and I welcome any further follow up questions.

Senator McCain
How would ambiguities in our definition of an act of war in cyberspace either benefit or impede our ability to develop a deterrence framework?

There is a clear ambiguity as to what constitutes an act of war in cyberspace. Many different actors have different standards. The term cyber war is thrown about so much it has little evident value as a statement at this point. There is some confusion that must be cleared up before we can progress forward with establishing a policy of cyber defense.

One simple thing we can do to limit the ambiguity of our responses to cyber threats is to declare it an act of war if a cyber action results in the death of any American. Any blurring of the line of war below that point unnecessarily restricts the nation to action in what might not be in accordance with the national interests.

Clear rules, definitions, and red lines beyond the death line can be limiting and unnecessarily harmful to national responses to aggressive action. The main thing to do is to make it clear that any action that rises to the level of death is forbidden, but beyond that we need not have any clear red lines for cyber actions lest it limit our options or lead to the United States being declared a hypocrite when it chooses not to act.

---

[1] http://www.cnn.com/2017/06/06/politics/russian-hackers-planted-fake-news-qatar-crisis/index.html

Deterrence frameworks are problematic in cyberspace. In the context of a nuclear action, they make sense in limiting and preventing the unthinkable, but cyber actions are thinkable and common at this point. You cannot prevent what has already happened and happens numerous times a day. The real issues, though, are with credibility, ambiguity of signals, and the complex nature of international conflict. We can dissuade antagonistic nations from taking aggressive action by establishing a clear policy of action and reaction in cyberspace.

For deterrence to work, credibility and resolve are required. All actors in cyberspace lack credibility at this point since there is no assured action. We are unclear generally how conflict will escalate in cyberspace. For example, when Iran was attacked with the Stuxnet worm, they responded by launching the Shamoon attack against Saudi Arabia's oil producer. Cyber responses can often be unclear and more of a shotgun attempt to attack anything that moves in the general direction of the target rather than precision attacks that are the clear foundation of current American strategy.

The issue really lies with the ambiguity of cyber signaling. The advantage of cyber conflict is the ambiguity of action and responsibility. We might know a certain actor committed a cyber atrocity, but we often have no way of knowing who exactly ordered the action. Deterrence is difficult under this framework; how do you deter an actor you now committed an aggressive act but have little evident proof?

Linkages and interconnections between states also remain a problem. North Korea is an aggressive actor in cyberspace but it mainly acts with the consent of China since its own networks are so slow that attacks are impossible to launch from North Korean territory. While it might be useful to threaten North Korea, how do you threaten China at the same time if there are other issues and demands that need to be considered to balance the relationship between the United States and China? We assume a free hand in cyberspace disconnected from other ongoing issues and disputes, an impossible situation.

The solution is to be clear as to what our course of response will be against any action that threatens the lives of any American. We cannot be ambiguous about this and roll this issue up with other concerns, the paramount issue is to protect the viability of critical infrastructure internationally. Attacks of these sorts must be off limits and this also means restricting our ability to act aggressively in this space. That said, death and attacks on critical infrastructure that can cause death are the clear red lines that need to be established. Luckily there does appear to be a norm against these attacks.

Recommendations call for the human element. What does this entail?

Often in cyber security we forget that the mission is about the interaction between a human and the machine. The weak link is not the machine, but the human. The WannaCry attack is evidence of this where the attack vector was ancient systems that had not been patched for three months since the security vulnerability was corrected. Simply updating the software of the operating systems could have saved a massive amount of lost time, work, and energy.

While the issue is obviously more complex than updating systems, the critical element is still the user and developer. Often business systems are stuck on antique platforms because it is either too costly to upgrade, too time intensive to make the switch, or the current system is too easy to utilize for the operator that a change is unthinkable. This is the human element; our own limitations create vulnerabilities and attack surfaces.

Fixing this issue will require a massive whole of nation problem to educate the population of computer vulnerabilities and how their own actions enable the attacker. The method of interaction we have with digital devices needs to be rethought, we inevitability

think these systems as safe and private when by definition they are the opposite of this, all digital interactions should be classified as public because they are technically public acts.

There is a psychological element to cyber security. Step one would be to remove the trust and dependence we have on digital devices in order to ensure our own security. Assuming trust is obviously dubious given the critical flaws in our systems. Dependence makes us vulnerable. Step two would be to manage the overreaction we tend to exhibit when digital violations inevitably occur. Digital violations are common and expected, under this frame it is important to carefully manage how we respond to inevitable abuses because often the overreaction to an issue can be more devastating than the initial threat.

Does our ultimate cyber strategy require specific tailoring for non-state actors?

The non-state actor threat is often overstated. States ultimately hold the majority of cyber capabilities and the real danger is when states help and enable non-state actors to cause havoc. The United States should be clear that any state aiding and abetting a non-state actor will suffer the consequences of enabling such attacks.

While the non-state actor threat is overstated, non-state actors are not limited in the ways states are limited to act. Consequences for a state versus a non-state actor are not the same, often non-state actors act below the international system and the typical tools leveraged such as sanctions, diplomatic censure, and general condemnation have no impact on non-state action. But it is a mistake to think that non-state actors do not have patrons that can be targeted to restrain non-state action in cyberspace. Adding a strategy of targeting patrons is a key shift that needs to be made.

Do you agree that deterrence strategy must include both offense and defense?

The key question about deterrence is how to implement it. If it were to work, the requirements would be complex and burdensome. Deterrence strategies are not about a choice between the offense and defense, but rather sound defense at the same time as pursuing an offensive strategy. There can be no offense without the defense first, this is the lesson from the architects of deterrence such as Schelling and Kahn.

Any vulnerability in a target is a source of weakness. Deterrence depends on the survival of the attacking state when faced with an initial strike or a retaliatory strike. Without proper defenses, deterrence is empty and non-existent. Therefore, there can be no attack without proper defenses otherwise there would be no option to attack.

The importance of defense is essential in cybersecurity. This would require a whole of nation approach to ensure that all potential critical targets, including civilian based, are prepared to withstand cyber actions. Recent attacks such as WannaCry and the Russian actions against power plants in Ukraine suggest we have a long way to go before we are properly secure. The offense and defense go hand and hand, but deterrence in cyberspace also requires a willingness to act and resilience in the face of coming attacks.

What cyber policy questions do you believe deserve addition consideration by this Committee and the Executive Branch?

The previously expressed human element concern must be a priority. Responding to eventual and coming cyber threats depends on the nation to be sure that its citizens can help withstand attacks and not be the critical source of vulnerability. At this point, the human element in the chain is the critical weakness. Human element flaws result in inefficient software design from a security standpoint, the absence of basic cyber hygiene practices, and

bureaucratic malaise that stifles responses to future threats. We need concise effort to ensure the citizenry is properly educated about the cyber threat, what they can do to protect the nation, and how to ensure that the weak link is no longer the average citizen, but rather the sheer number of targets that we need to protect. We will have some assurance of safety when the critical weakness moves away from the average individual.

One key policy question that has not garnered much attention, even in the expansive research requested in recent Executive Order on cybersecurity, is the vulnerability offered by reliance on third party contractors. Most major attacks on American systems come through third party systems and contractors. We have also seen major leaks come from contractors, likely enabling the bleeding of cyber tools to civilian space. This is a critical vulnerability. Between the average individual and our excessive reliance on third parties, it will continue to be a weakness until we eliminate this weakness in the supply chain of cyber security contracting.

Cyber security education is another critical weakness. We focus too much on technical aspects with little practice application and no policy application. There needs to be a bridge between the technical skills gained at the University level and the skills needed to actively work in the cyber security field. This would require that those institutions designated as NSA accredited institutions for cyber security demonstrate greater collaboration with private industry and government to actually implement their skills in the real world.

The other critical aspect is the complete lack of context-based training in cyber security at the University level. NSA accreditation makes no allowance for training in cyber security policy, international relations, criminology and behavioral analysis, and basic research and writing skills. These factors need to be enhanced and given at least twenty percent focus for a University to be considered a premier outlet for cyber security training. Pushing a holistic approach to cyber security will train well rounded students to be critical producers of cyber security capacity.

There is also a need for greater access and collaboration between private industry and the National Guard and the conventional service branches. We need to be able to utilize civilian talent in critical aspects of security, with cyber security being a key point of access and support from civilian space. Establishing a way for private individuals with cyber security skills to support that national mission through service is a key task. Currently we are limited by the requirements of service and rejection of members of the cybersecurity community who might use causal drugs or have disabilities (diabetes or mobility issues should not be an impediment to national service in cyber security). The talent pool in cyber security is deep, but we need to examine how we utilize and funnel talent towards national service instead of away from it.

Senator McCaskill
Other sophisticated cyber adversaries like China and Iran are becoming more aggressive. It seems natural that the private sector is next. How can the Government better improve its ability to combat these threats?

The private sector is clearly a critical target in the United States. The technological capacity of American industry makes it ripe for plunder. We can expect more private sector attacks, especially as there is confusion as to what is a legitimate and non-legitimate target in cyberspace. The country needs to do a review to identify what are critical targets that would enable government support when future cyber-attacks do occur.It is concerning that electoral systems were only recently designated critical infrastructure and that there is some debate about this.

There is no general evidence that China and Iran are becoming more aggressive, data

suggests that China is either generally complying with the agreement with Obama forged in 2015, or hiding its intrusions better. Iran seems willing to attack American allies and support non-state actors in cyberspace, but there is no general evidence they are willing to attack the United States directly after the banking sector attacks of the past.

The states that do appear more aggressive seems to be Russia in their willingness to attack elections or hack the credibility of governments as seen in the recent Qatar attack. North Korea also seems more willing to attack the banking sector with their attacks on Asian banks in early 2017, but they are having trouble converting their criminal activities to direct cash as seen with the WannaCry attack where over $200,000 has been left sitting in an account for about a month now.

The private sector will remain a target, but my forthcoming research demonstrates that state based attacks on the private sector are even less likely to achieve coercion than attacks on public systems. Public-government targets are more likely to achieve their ends, making these targets more critical than private industry.

The key concern would be in linking responsibility for private sector attacks to the government. This would insert the government in front of the private sector and delineate responsibility for safety of the private sector to government which has little direct ability to compel private actors to behave in ways that might enhance their security. While generally a good idea in theory, in practice inserting government as the vanguard of all industry is problematic and government must first ensure that critical infrastructure projects are protected.

One way to help protect the private sector would be to enhance and investigate the cyber security insurance industry. Is the market providing services that make private systems more secure? Are they providing advice and resources to support the public? Are they paying out when attacks happen or is the industry blaming these actions on "acts of God" out of the control of the private-sector actors? No one has investigated these questions and it is time to start to regulate their new market. The insurance industry can be a great benefit to the private sector if they encourage good behavior, but it's unclear just what standards they are encouraging.

The main way government can enhance security in both the public and private sector is to delineate lines of control and responsivity. In short, no one knows who to call when breaches happen, the FBI? CIA? Cyber Command? We need to be clear as to what happens when public services are breached, who is responsibility, and what support government can offer. NIST guidelines are useful for the government sector, but how would these be implemented in private sector?

We also need to encourage more research on the impact of cyber actions. The literature is sparse on the economic impact of cyber incidents, as is the limited empirical research on the impact of military actions in cyberspace. While there are many avenues to encourage public sector investment in cyber security research, most of this is technical and avoids the question of impact of cyber actions on military effectiveness, psychological impact, and economic effects. If we are going to ensure the National Science Foundation is enabling research that can help answer critical national security questions, these issues should be core foundational research prompts, instead they are excluded and these issues rarely are supported by government funding.

Do you believe our education system is producing qualified cybersecurity professionals and what are your recommendations for improvement?

Broadly speaking our education sector is producing qualified technology specialists. We can see this by the great burst in productivity in sector and the number of patents

produced that originate in the United States. But if the question is if the United States is producing qualified cyber security professionals, then the answer is no. We have an issue in the transition from the education system to cyber threat intelligence in practice. In short, the people trained in the education sector have the skills but lack applied knowledge. This is even true in the military where past cyber engagements are classified so heavily it is if difficult to extract lessons and applied knowledge from these incidents.[2]

One way to enhance our ability to generate applied knowledge is to provide for better linkages between government and industry to the education sector. Government agencies can easily do this by providing for more internships, but this is complicated by the security clearance issue. Congress can jumpstart this process by providing for funds to help link government service to advanced cyber security education. These programs could help ensure the pipeline issue is fixed and we produce a steady stream of prepared cyber security professionals.

The other failing of the education sector is the inability of cyber security researchers to produce contextual qualifications of their work. Many are skeptical of the threat Russia or North Korea poses to the United States because they lack the proper International Relations background to effectively do their job. One cannot be a cyber security professional without understanding basic international history and criminology.

In addition to lacking contextual knowledge, it is also dubious if cyber security professionals can complete their jobs without the most basic of training in policy analysis or legal processes. Cyber security professionals are constrained by legal statutes that many seem unaware of, while basic policy analysis is required to either write impact reports or understand government dictates. We need to do better to provide holistic education in addition to technical background training.

The National Center of Academic Excellence program in Cyber Security advanced through the National Security Agency needs to be enhanced.[3] It should be directed out of the Homeland Security department or the Intelligence Community as a whole. There needs to be established links between Universities granted certification and both private and public government to provide students with skills to apply their educational training. An extensive review of these programs and how to enhance national security is clearly warranted and critical at this time.

What suggestions do you have on ways the federal government could recruit and retain a qualified cybersecurity workforce?

In the prior question, I suggested Congress work to enhance the National Center of Academic Excellence program to include collaborations between private/public industry and education outlets. In making this step, we can provide connections and linkages between government that would ensure that top cyber security student know that the government is a viable place to work in the cyber security sector. Exposure and contact are the main ways to ensure that there is an outlet for top talent to make its way to government service.

We also need to start early, the National Security Agency has GenCyber, a cyber security summer camp program to expand interest and engagement with young person's interests in cyber security.[4] Homeland security, the FBI, and CIA should also actively engage in this process to help identify talent, expand diversity, and increase overall societal awareness of cyber security issues. Communicating the viability of long term careers options

---

[2] https://warontherocks.com/2015/06/the-real-fog-of-cyberwar-operational-cyber-planning/

[3] https://www.nsa.gov/resources/educators/centers-academic-excellence/cyber-defense/

[4] https://www.gen-cyber.com/about/

in the public service sector is key and the nation is not doing enough currently.

One huge limitation is the clearance issue and time it takes to convert actively interested individuals into government employees. Every effort must be made to ensure this process does not take over six months because by that time, the top qualified individuals are likely already working in the private sector and making more in salary than they can in government service. The current timeline is too long and leads to bleeding applicants. There are simple things we can do fix this process like hire more people to clear cyber security professionals, taking less of an interest casual drug use common in this population, and ignoring college debt in order to place top individuals into critical public service jobs.

Retention is also a critical issue. There is currently a flexibility problem that limits who can work for government. The great majority of jobs are located in Washington DC and this means that anyone now willing to live in the DC metro area automatically is excluded from public service. We need to expand the range of workplaces that cyber security professionals can work, understanding that they likely will need to work out of secure facilities, focusing on sections of the entire United States rather than housing them in DC Metro government facilities.

Do you have suggestions on how to make the federal government a more enticing place for cyber professionals to work?

To make government service more enticing, a key issue that needs to be solved lack of trust in the government. Right now, we have record high levels of distrust in American institutions. There needs to be a greater effort to demonstrate what cyber security professionals are doing for the nation and how others can help. Right now, cyber security firms like FireEye and Crowdstrike are seen as top places to work in cyber security, not the CIA or NSA. This needs to change and the first step is reassuring the public that we have top individuals at the job trying to protect the nation.

Freedom is another key issue because quite a few cyber security professionals choose computer technology tracks because of the freedom the job provides. They do not like structure, in fact, a critical skill for cyber professional is the tendency to want to break things and build them back up. Traditional notions of control and subservience as often lacking in the best cyber security talent just based on the nature of their jobs, they seek to deconstruct the process. This ethos makes it difficult to recruit cyber security professionals into government service.

To ensure we get the right message across, we need to focus a bit more on the public relations side of the issue. Wired recently ran a piece called "Meet the Nerds Coding through the Afghanistan War."[5] An effort likely enabled by Department of Defense public relations personal, this article gets across that there can be some freedom to operate in the US government. The system is resistant of these processes, but they can happen when there is a great need and willingness to be flexible.

Another issue often avoided the complete lack of engagement broadly with the minority community on cyber security issues. These individuals need to be recruited and trained in cyber security practices. We are losing generations of talent by our general lack of attention in such communities. Diversity increases outcomes and thinking outside the box is a hallmark of minority communities often excluded from typical structures. These skills and outlooks are critical in the hacking community and the lost talent is staggering. The nation has made a strong effort to support Historically Black Universities but we need to do more to be inclusive of Asian communities and the Latino talent. This issue deserves special

[5] https://www.wired.com/2017/05/meet-nerds-coding-way-afghanistan-war/

attention and research because we are losing too many individuals who might be key sources of strength for the nation.[6]

In your opinion, is the United States government properly organized to protect against a cyber attack? Is there a national cyber strategy in place to combat cyber threats and keep the country safe? Do you think we need a national cyber strategy, and if so, what should it involve?

There is too much confusion with current government organization to suggest that it is properly organized to protect the American population. While functionally it has done a remarkable job to ward off and repair breeches after attacks, the dysfunction is problematic externally because we do not do enough to congratulate the government for what it has done to protect the nation in this domain. There have been serious lapses but these are often generated by third parties (Snowden, the OPM Hack), not government agencies.

Bureaucratic confusion dominates in the cyber security platforms supported by the public sector. No one knows who is responsible for what? This simple organizational coherence would be a critical step towards protecting the nation. Ensuring that the population knows exactly what is being done to protect that state is critical. There needs to be an effort to suggest clear organizational principles in cyber security policy.

A simple step that we can take is review the National Cyber Strategy and ensure that this document provides clear guidelines as to who is responsible for what, how the state protects both the public and private sector, and clear organizational missions of each agency as they might interact with the public.

Do you have any reason to doubt the Intelligence Community's assessment that "Russia's intelligence services conducted cyber operations against targets associated with the 2016 Presidential election"?

There is no reason to doubt the Intelligence Community's assessment. While likely backed up by traditional intelligence sources and signals intelligence, this report offers a remarkable degree of confidence about the action across all 17 intelligence services. This unprecedented level of cooperation demonstrates the high level of confidence each agency places on the opinion that Russia was actively trying to disrupt the American election.

Beyond government sources, there have been extensive reports and investigations by private individuals, including the recent report released by Citizen Labs out of the University of Toronto.[7] Clearly there is a remarkable confluence of information that Russia was indeed behind the hacks, including their much more brazen attacks on French and German systems in the run up to their elections. This suggests there should be no doubt that Russia was behind these attacks, sought to disrupt American elections systems, and has gone unpunished for these actions. Restraining an aggressive actor means that they know there are consequences for their actions, every effort should be made to identify the leaders of these efforts, to censure troll farms, shut down botnets, question the utility of RT operating in American space, and make it clear that reflexive measures enabled by Russia means that some Americans were parroting Russia propaganda dictates.

What mechanisms are most effective to deter nation-state cyber-attacks?

---

[6] https://warontherocks.com/2017/05/the-cyber-workforce-gap-a-national-security-liability/

[7] https://citizenlab.org/2017/05/tainted-leaks-disinformation-phish/

There are no mechanisms to deter a nation-state from committing a cyber action. This would depend on immaculate defenses, the foundation of American nuclear security. The age old construction of nuclear deterrence depends on first surviving a nuclear attack and also responding to such an attack was massive retaliatory power, it is unclear in the cyber domain if the United States can withstand the most basic committed attack on its infrastructure.

To deter, a state also needs to demonstrate capabilities so that the adversary knows that the defender is willing and able to launch a counterstrike. A better term has been advocated by Joseph Nye, who suggests we use the term dissuasion to better way to think about how to persuade the opposition to not launch cyber strikes.[8] This would depend more on diplomatic communication, economic threats and inducements, and conventional legal strategies to dissuade the opposition from committing attacks rather than relying on some form of rhetorical safety offered by deterrence.

We need to think beyond deterrence because it cannot be depended on to keep us safe in cyberspace.There is already a proliferation of cyber actions across all spectrums demonstrating that deterrence is hollow. Moving towards thinking about the positive and negative inducements we can offer to aggressors might expand the options we have in responding to future cyber conflicts. China seems to have backed off their espionage activities after a diplomatic agreement and criminal indictments of officers in the PLA, can these sorts of inducements provide greater results than threats? This basic question is often ignored for offense first policies that might be unworkable in cyberspace.

What steps should the United States take to prevent similar cyber-attacks in the future?

The most basic thing to prevent future cyber actions is to resolve to reconstruct our commitment to basic cyber hygiene. This is lacking now; the simplest route of attack is easy to implement sphere phishing or social engineering attacks. Through this method, perhaps 20 percent of the target surface is vulnerable through easy to mobilize attacks.

I have written quite extensively above on deterrence and dissuasion. While we cannot establish a clear and effective system of deterrence in cyberspace given the limitations of the domain, we have clearly articulated a system of dissuasion where the major attacks are prevented through norms, consequences, and diplomacy. These actions need to be enhanced. We seem to have entered in an era where the United States might be encouraging cyber actions in some ways. We have yet to respond to recent breaches against Qatar, the Philippines, and the UAE, demonstrating our commitment to allies is waning. To ensure a system of cyber security that enables all actors in the international system to benefit from digital interaction, we need to at least ensure our allies are protected.

Preventing future attacks largely depends on the development of talent able to fend off future cyber actions. To ensure this, we must enhance our avenues of education, the collaboration between private industry and government in prevent breaches and solving issues as they arise, and focusing on gathering prime cyber security talent, often currently missed through poor recruitment, weak training in the education sector, and the lack of collaboration between government training efforts and the private sector.

The focus on norms and dissuasion, education and talent, and the human element should go a long way to dealing with the low hanging fruit in the cyber security arena. Once we solve these basic questions, we can move towards dealing with more complex questions and issues.

---

[8] http://www.mitpressjournals.org/doi/pdf/10.1162/ISEC_a_00266

Post-Hearing Questions for the Record
Submitted to Captain Kevin Keeney
Senator John McCain

"Cyber Threats Facing America:
An Overview of the Cybersecurity Threat Landscape"
May 10, 2017

You note that the nation's largest threat in cyber is to the private sector, not the public. You also highlight that the National Guard is uniquely postured to bring highly skilled operators and analysts to bear on both sides of the challenge.

- What measures should the government take to improve public-private cooperation on cyber security and encryption issues? What would the costs be of this rapprochement?
- Is the current equilibrium tolerable or does this represent a major threat to national security?
- What is the National Guard's role in the new uniformed service called U.S. Cyber in which you recommend?

The prior administration placed a strong emphasis on developing defensive cyber strategies. While appropriate, I am concerned that a denial-only strategy is likely impossible.

- Do you agree that a deterrence strategy in cyber must include both offense and defense?
- What cyber policy questions do you believe are receiving enough attention and deserve additional consideration by this Committee or the Executive Branch?

The witness failed to respond to these questions for the Record by time of printing. Any responses that are subsequently received will be on file in the committee offices.

Post-Hearing Questions for the Record
Submitted to the Mr. Kevin Keeney, Jr.
From Senator Jon Tester

"Cyber Threats Facing America: An Overview of the Cybersecurity Landscape"
May 10, 2017

Rural Utilities
How do you recommend we increase the resiliency of our rural utility companies and cooperatives against cyber threats?

To your knowledge, does the federal government, whether through USDA's Rural Utilities Service or DHS, provide rural utility companies and cooperatives with the tools they need to improve reliability, resilience, and security of the electric grid against cyber attacks?

Small Businesses
According to the Small Business Administration, there are more than 28 million small businesses across the U.S., and many of them in rural America are critically dependent on IT.

What general recommendations do you have to strengthen how small and medium-sized businesses can protect their networks and IT from cyber threats?

Would better guidance from the National Institute of Standards and Technology (NIST) help small businesses fight digital threats?

The witness failed to respond to these questions for the Record by time of printing. Any responses that are subsequently received will be on file in the committee offices.

○