S. HRG. 113–827

CYBER THREATS: LAW ENFORCEMENT AND PRIVATE SECTOR RESPONSES

HEARING

BEFORE THE

SUBCOMMITTEE ON CRIME AND TERRORISM

OF THE

COMMITTEE ON THE JUDICIARY
UNITED STATES SENATE

ONE HUNDRED THIRTEENTH CONGRESS

FIRST SESSION

MAY 8, 2013

Serial No. J–113–17

Printed for the use of the Committee on the Judiciary

U.S. GOVERNMENT PUBLISHING OFFICE
98–755 PDF WASHINGTON : 2016

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

COMMITTEE ON THE JUDICIARY

PATRICK J. LEAHY, Vermont, *Chairman*

DIANNE FEINSTEIN, California	CHUCK GRASSLEY, Iowa, *Ranking Member*
CHUCK SCHUMER, New York	ORRIN G. HATCH, Utah
DICK DURBIN, Illinois	JEFF SESSIONS, Alabama
SHELDON WHITEHOUSE, Rhode Island	LINDSEY GRAHAM, South Carolina
AMY KLOBUCHAR, Minnesota	JOHN CORNYN, Texas
AL FRANKEN, Minnesota	MICHAEL S. LEE, Utah
CHRISTOPHER A. COONS, Delaware	TED CRUZ, Texas
RICHARD BLUMENTHAL, Connecticut	JEFF FLAKE, Arizona
MAZIE HIRONO, Hawaii	

BRUCE A. COHEN, *Chief Counsel and Staff Director*
KOLAN DAVIS, *Republican Chief Counsel and Staff Director*

SUBCOMMITTEE ON CRIME AND TERRORISM

SHELDON WHITEHOUSE, Rhode Island, *Chairman*

DIANNE FEINSTEIN, California	LINDSEY GRAHAM, South Carolina,
CHUCK SCHUMER, New York	*Ranking Member*
DICK DURBIN, Illinois	TED CRUZ, Texas
AMY KLOBUCHAR, Minnesota	JEFF SESSIONS, Alabama
	MICHAEL S. LEE, Utah

STEPHEN LILLEY, *Democratic Chief Counsel*
SERGIO SARKANY, *Republican Chief Counsel*

CONTENTS

MAY 8, 2013, 9:05 A.M.

STATEMENTS OF COMMITTEE MEMBERS

WITNESSES

MISCELLANEOUS SUBMISSIONS FOR THE RECORD

CYBER THREATS: LAW ENFORCEMENT AND PRIVATE SECTOR RESPONSES

WEDNESDAY, MAY 8, 2013

UNITED STATES SENATE,
SUBCOMMITTEE ON CRIME AND TERRORISM,
COMMITTEE ON THE JUDICIARY,
Washington, DC.

The Subcommittee met, pursuant to notice, at 9:05 a.m., in Room SD–226, Dirksen Senate Office Building, Hon. Sheldon Whitehouse, Chairman of the Subcommittee, presiding.

Present: Senators Whitehouse, Klobuchar, and Graham.

Also present: Senator Coons.

OPENING STATEMENT OF HON. SHELDON WHITEHOUSE, A U.S. SENATOR FROM THE STATE OF RHODE ISLAND

Chairman WHITEHOUSE. Good morning. I will call this hearing to order. I believe that Senator Graham will be joining us, but in the interest of getting underway on time, we have been cleared to proceed and await his arrival during the course of the hearing.

I would like to note today's hearing will consider Cyber Threats: Law Enforcement and Private Sector Responses. This, as press reports indicate every day, is an extremely important and timely topic. Indeed, I would like to add, without objection, to the record of this proceeding two pages from the Department of Defense Annual Report to Congress that just came out saying, among other things, China is using its computer network exploitation capability to support intelligence collection against the U.S. diplomatic, economic, and defense industrial base sectors that support U.S. national defense programs. Obviously, there is a lot more to this issue than just that, but it is an indication of the timeliness and importance of our concern here.

[The information referred to appears as a submission for the record.]

Chairman WHITEHOUSE. Technology continues to expand into every area of modern life. Our power stations, our dams, and, as the Defense report said, our defense industrial base are all online. And even everyday items like our cars, our home alarm systems, even our refrigerators, are increasingly connected to the Internet.

Unfortunately, these innovations have been accompanied by new threats to our prosperity, to our privacy, to our intellectual property, to our very national security.

This Subcommittee has heard previously about hackers who have taken over the web cams of unsuspecting Americans' computers. We have heard about hacktivists like Anonymous using distributed

denial-of-service attacks against financial institutions. We have heard about criminal rings that use botnets to send spam, to send spearfishing emails, to capture and sell Americans' credit card information, or to engage in click fraud, scareware, or ransomware schemes.

And, finally, we have heard about the advanced persistent threats that have allowed foreign entities to steal enormous quantities of American intellectual property and to worm their way into our American critical infrastructure.

This hearing will consider our Nation's law enforcement response to these threats. Our first panel will include witnesses from the Department of Justice and the Federal Bureau of Investigation. It will consider their strategies to combat the broad array of cyber threats and the resources that they have brought to bear to execute those strategies.

The second panel will discuss the private sector's role in responding to these threats. It will consider a recent investigatory report based solely on public information that indicates that members of the Chinese military have sponsored or engaged in sophisticated and extensive cyber espionage, including industrial espionage. And it will evaluate the role of the private sector in investigating, preventing, and responding to such crimes and intrusions.

I would start this discussion by noting that the Justice Department and the FBI both already have done some important work to address the cyber threats facing our Nation. In March 2012, for example, charges were unsealed against the former head of the hacktivist groups Anonymous and LulzSec and against four other members of Anonymous or LulzSec and a member of AntiSec, another hacking group.

Earlier this year, the Justice Department secured the conviction of a 25-year-old Russian who had operated and controlled the Mega-D botnet. And in April 2011, the FBI and the Justice Department engaged in a civil lawsuit to bring down the Coreflood botnet.

The Justice Department and the FBI also have developed the FBI's National Cyber Investigative Joint Task Force and the Justice Department's National Security Cyber Specialists' Network. I am glad that the Department and the FBI have taken each of these important steps, but much more, as the Department concedes, needs to be done.

I was disappointed to learn, for example, that the team that took down the Coreflood botnet was not kept together for the purpose of taking down other comparable botnets. The four-star general heading our military's Cyber Command has said that our country is on the losing end of the greatest transfer of wealth by illicit means in history. It is all well and good to complain about such thefts through diplomatic channels, but at some point you need to stop complaining and start indicting. The Justice Department has not indicted, to my knowledge, a single person for purely cyber-based trade secret theft.

I am sympathetic that the Justice Department and the FBI lack adequate resources to respond to the severe cyber threat. As the witnesses will testify shortly, these are immensely complex and challenging cases to put together. The administration, of course, agrees, and its 2014 budget includes a request for 60 new cyber

agents at the FBI, 16 new cyber attorneys in the National Security Division, and 9 new cyber attorneys in the Criminal Division.

As welcome as this request is to many of us, we must also ensure, however, that the resources are deployed wisely. Accordingly, I will be inquiring today if appropriate structures, whether task forces or centers of excellence, are being employed; whether attorneys and agents are properly dedicated to cyber work, not just carrying the badge of a cyber attorney and listening to the conference call on mute while they do their other work; whether they are tasked with goals of achievable scope; and whether the attorneys and agents are properly evaluated and recognized for that work.

I will close my opening remarks by adding that a law enforcement frustration and a frustration that has affected this very hearing is the unwillingness of many corporations to cooperate for fear of offending the Chinese Government and suffering economic retaliation. The shadow of China's heavy hand darkens the corporate world and has even shadowed this hearing.

I look forward to an important discussion on our Nation's response to the cyber threats that we face. I thank all the witnesses who are here to participate today, and I will call the first panel right now. I will introduce both now so that they can move from the testimony of one to the testimony of the next.

We will begin with Jenny Durkan. Ms. Durkan is the United States Attorney for the Western District of Washington. She is on the Attorney General's Advisory Committee of United States Attorneys, and she is the chair of the AGAC's Subcommittee on Cyber Crime and Intellectual Property Enforcement. Prior to beginning her service as U.S. Attorney in 2009, Ms. Durkan was in private practice representing a variety of clients in civil and criminal litigation. She is a graduate of the University of Notre Dame and received her law degree from the University of Washington.

With her today is Joseph Demarest. Mr. Demarest is the Assistant Director of the Cyber Division at the Federal Bureau of Investigation. In that role he manages over 600 employees dedicated to the investigation of both national security and criminal computer intrusions. He joined the FBI as a special agent in 1988 and has served in a number of roles within the Bureau, including as a SWAT team leader in the New York Division, as shift commander for the PENTTBOM investigation, and as Assistant Director of the International Operations Division.

I welcome both of the witnesses here, and before we ask you to begin your testimony, I will also welcome my wonderful Ranking Member, who has demonstrated intense interest and commitment to this issue, and invite him, if he wishes, to make any opening remarks he might care to.

OPENING STATEMENT OF HON. LINDSEY GRAHAM, A U.S. SENATOR FROM THE STATE OF SOUTH CAROLINA

Senator GRAHAM. Well, most of what I know about the cybersecurity threat comes from Senator Whitehouse—which is a damning indictment to him.

[Laughter.]

Senator GRAHAM. But, no, I have really enjoyed working with our Chairman here, who I think understands the threat as well as any-

one in the Congress and, when it comes to the private sector, has the most practical solution of trying to get the private sector to harden their critical infrastructure through voluntary standards, best business practices, with liability protection as the reward. So I am looking forward to the hearing.

Chairman WHITEHOUSE. Ms. Durkan, why don't you proceed with your testimony? We obviously will put your entire very comprehensive statement into the record of this proceeding, but if you could keep your oral statement to about 5 minutes, that would be helpful so that we can engage in some conversation afterwards and leave time for the next panel.

Ms. Durkan.

STATEMENT OF HON. JENNY A. DURKAN, UNITED STATES ATTORNEY, WESTERN DISTRICT OF WASHINGTON, SEATTLE, WASHINGTON

Ms. DURKAN. Thank you. Good morning, Mr. Chairman, Ranking Member Graham. Thank you for the opportunity to testify on behalf of the Department of Justice regarding the investigation and prosecution of cyber threats and the resources required to do so. I thank each of you for your leadership in this area. The articles you have written show your great grasp of the array of threats that we face.

As United States Attorney, I see the full range of threats that our communities and our Nation face. Few things are as sobering as the daily cyber threat briefing that I receive. Technology is changing our lives. We have witnessed the rapid growth of important businesses, life-saving technologies, and new ways to connect our society. Unfortunately, the "good guys" are not the only innovators. We have also seen a significant growth in the number and the sophistication of bad actors exploiting the new technology.

Seeking profit, international rings have stolen large quantities of personal data. Criminal groups develop tools and techniques to disrupt our computer systems. State actors and organized criminals have demonstrated the desire and the capability to steal sensitive data, trade secrets, and intellectual property.

One particular area of concern is the computer crimes that invade the privacy of every individual American. Every day criminals hunt for our personal and financial data which they use to commit other fraud or sell to criminals. As you will hear from the next panel, the potential victims range in the tens of millions.

The national security landscape has also undergone a dramatic evolution in recent years. Although we have not yet experienced a devastating terrorist cyber attack, we have been the victim to a range of malicious cyber activities that are testing our defenses, targeting our valuable economic assets, and threatening our Nation's security.

There can be no doubt: Cyber threat actors pose significant risks to our national security, our communities, and our economic interests. Addressing these complex threats requires a unified approach that incorporates criminal investigative tools, civil and national security authorities, diplomatic efforts, public-private partnerships, and international cooperation. Criminal prosecutions, whether in the United States or abroad, play a central and critical role in

these efforts. We need to ensure that throughout the country the Department of Justice's investigators and prosecutors have the resources and forensic capabilities they need to meet this evolving threat, and we thank this Committee for its support in those efforts.

The Department of Justice has organized itself to ensure we are in a position to aggressively meet this threat. The Criminal Division's Cyber Crime and Intellectual Property Section works with a nationwide network of over 300 Assistant United States Attorneys who are designated as "Computer Hacking and Intellectual Property" prosecutors. Mr. Chairman, we will address that question. They are doing the work in the field. They lead our efforts to investigate and prosecute cyber crime offenses.

The Department's National Security Division pursues national cyber threats through a variety of means, including counterespionage and counterterrorism investigations and prosecutions.

Recognizing the diversity of this threat, last year we did form what, Mr. Chairman, you have noted, the National Security Cyber Specialists. This network brings together the Department's full range of expertise in this area, drawing on experts from the National Security Division, the U.S. Attorney's Office, the Criminal Division, and other components. There is a national security cyber specialist designated in every United States Attorney's Office across the country. These combined efforts have led to great successes. I hope to address some of them later here today.

But, as said, despite these successes, the number of intrusions continues. Because of the very serious nature of the cyber threats and the pressing need to respond, the administration is asking for enhancement of the budget to target this critical program. Most of this is addressed to the FBI so that we can do more ground research. An additional request of the $92.6 million is to the National Security Division because we must address this increasing national security threat and to the Criminal Division so that we have the resources we need to deal with this internationally.

Mr. Chairman, Ranking Member Graham, thank you for the opportunity to testify here today. The country is at risk. There is much work to be done. But we look forward to working with your Committee.

Thank you.

[The prepared statement of Hon. Jenny A. Durkan appears as a submission for the record.]

Chairman WHITEHOUSE. Thank you very much, Ms. Durkan.

Assistant Director Demarest.

STATEMENT OF JOSEPH DEMAREST, JR., ASSISTANT DIRECTOR, CYBER DIVISION, FEDERAL BUREAU OF INVESTIGATION, WASHINGTON, DC

Mr. DEMAREST. Thank you, Chairman. Chairman Whitehouse, Senator Graham, and distinguished Members of the Committee, I am pleased to appear before you today to discuss the cyber threat, how the FBI has responded to it, and how we are marshaling our resources currently and strengthening our partnerships to more effectively combat the increasingly sophisticated adversaries we face in cyberspace.

As the Subcommittee is well aware, the 21st century brings with it new challenges, in which national security and criminal threats strike from afar through computer networks, with potentially devastating consequences. These intrusions into our corporate networks, personal computers, and Government systems are occurring every day. Such attacks pose an urgent threat to our Nation's security and economy. We face these significant challenges in our efforts to address and investigate cyber threats, and we are currently prioritizing our immediate and long-term needs for strategic development in order to best position ourselves for the future.

We have made great progress since the Cyber Division was first created in 2002. We have seen the value of its trusted partnerships and worked tirelessly to support and improve them. Providing the information that is needed to secure our networks demands cooperation, and cyber vulnerabilities are magnified when you consider the ever-connected, interdependent ecosystem of the cyber world.

We follow a one-team approach in our partnerships with the U.S. intelligence community, law enforcement, private industry, and academia. We significantly increased the hiring of technically trained agents, analysts, and computer scientists. We have placed cyber specialists in key global locations to effectively facilitate the investigation of cyber crimes affecting the U.S. And while we are pleased to report our progress, we recognize that we must be proactive in order to effectively address the threats that we face.

Next Gen Cyber. The FBI's Next Gen Cyber Initiative has enhanced the FBI's ability to collect, analyze, and act on information related to cyber intrusion investigations at FBI headquarters and throughout our 56 domestic field offices, 400 resident agencies, and with the intelligence community and law enforcement partners, both domestically and overseas. Implementation of the initiative is focused in four areas:

First, the NCIJTF, the National Cyber Investigative Joint Task Force, in Chantilly, Virginia. A key part of the intergovernmental effort is the FBI-led National Cyber Investigative Joint Task Force. Since its formulation in 2008 by Presidential directive, the NCIJTF has made significant progress in developing its capabilities and operational coordination as well as expanding its interagency leadership to now include increased personnel from 19 partner agencies and Deputy Directors from five key agencies.

A second key element on this initiative is the restructuring and expansion of the FBI's network of field office Cyber Task Forces, which emulate the successful Joint Terrorism Task Force model in our Counterterrorism Division. And just last year—just this past year, the FBI has formally established a Cyber Task Force in each of our 56 field offices, staffed by cyber-specialized agents, analysts, and other agency participants. In the future, each CTF, or Cyber Task Force, will continue to grow its capabilities, leveraging nationally developed systems, investigative efforts, and expanding its membership with a key focus to add additional State and local participants.

Third, the FBI is committed to advancing the capability of our cyber work force and the supporting enterprise infrastructure. We established our High-Technology Environment Training—HiTET—

initiative to enhance the technical proficiency of special agents, intelligence analysts, professional staff, and task force officers through online training. The current results of this effort are increased efficiencies and improved information analysis.

Since the rollout of Next Gen Cyber, the FBI has expanded visibility into the source of cyber threat activities and dramatically increased its cyber intelligence reporting.

Last but not least, the FBI is working to strengthen both local and national information sharing and collaboration to support success in investigation, intelligence operations, and disruption operations. To support this, we adopted an incident-reporting and collaboration system called "eGuardian," used successfully by our Counterterrorism Division and tailored it for cyber reporting.

Further, we are deploying a platform called "iGuardian" to enable trusted private industry partners to also report cyber incidents in a secure and efficient manner to the FBI, and we are leveraging intelligence from the NCIJTF to effectively identify and notify cyber victims.

As the Committee knows, we face significant challenges in our efforts to combat cyber crime. We are optimistic that by identifying and prioritizing strategic areas for change, the FBI will position itself to neutralize national security and criminal threats of the future. We look forward to working with the Committee and Congress, sir, as a whole to determine a course forward to ensure our success in addressing cyber threats.

Thank you once again, Chairman, for the invitation to appear before you today. I would be more than happy to take any questions you may have.

[The prepared statement of Joseph M. Demarest, Jr., appears as a submission for the record.]

Chairman WHITEHOUSE. Terrific. Well, first of all, let me thank you both very much. I immensely appreciate the work you are doing. Ms. Durkan, I know it is a considerable honor to be selected and confirmed as United States Attorney. It is an even greater honor when you are in the ranks to be selected to serve on the Attorney General's Advisory Committee, and your work to focus on cyber crime and cyber terror as the Chair of that Subcommittee I think is something that we should all be very proud of. And, Agent Demarest, you have been working this beat for a while. Nobody has more passion for it than you, so I am a little bit preaching to the choir, but I do want to try to give both of your organizations a bit of a shove through this hearing to be a little bit more forward on this issue.

One of the ways you measure legal outcomes is results. Your testimony, Ms. Durkan, talked about the importance of prosecution both as a deterrent and as a punishment. And yet the level of actual legal activity does not seem to be all that great. The Coreflood botnet was taken down I think well over a year ago. I think we are actually through the stage where the participants have had their Attorney General awards, and I am glad that they were recognized for that very important piece of work. But as I understand it, this was a group that was sort of cobbled together from a variety of different offices, and at the conclusion of that effort, it was basically

allowed to just disappear back to those original offices rather than continue the process of cleaning up and attacking botnets.

As you know, Microsoft has done at least four that I can think of, civil cases to go to court and get an order to clear botnets out of the system. So it is not impossible for the Justice Department to have done more than one.

On the side of our intellectual property theft, we have, I think, primarily the Chinese attacking exceedingly vigorously not only our national defense infrastructure in order to try to hack into things like how our jets work, how our guidance systems work, so that they can imperil our military in the event that we were to end up in a military conflict with them, but they are also just plain trying to steal stuff so they can give it to their companies so they can build it without either inventing it or paying us for the intellectual property rights. And that has been described as the biggest transfer of wealth in the history of humankind. And to my knowledge, the Department has done exactly zero cases involving a pure cyber intrusion to steal intellectual property and back out. They have done some intellectual property theft cases where somebody left with a CD in their pocket, kind of the old-school version, but they have not done any cases left yet. So the results are a little bit—do not send the signal yet that we are where we need to be.

When you try to look at the structure, it is not clear that the structure is firmly in place for this. This has been a considerable issue for some time, and yet it is, I think, last year that the expert corps began at the Department of Justice. Your testimony, Ms. Durkan, is that the Department is developing "threat focus" cells. The NCIJTF is a wonderful effort. I have been out there, and I think the people who are there are doing great work. But my impression of it was that they are working so hard out there just to try to figure out who is coming through the windows and trying to keep track of them and trying to warn businesses that somebody is now in their system that there really has not been the capability to sit down and take that information and turn it into a prosecution package and put it into play in a U.S. Attorney's Office and go and put somebody on the business end of an indictment. I am not even aware of any grand juries that are active in this area at this point.

So I think that I want to applaud—and I am sure it is thanks to both of your leadership that both the U.S. Attorney's Offices, the Department of Justice, and the FBI are rethinking the structure that needs to deploy this effectively. If this really is a national security threat of the type that every major administration figure says, if this really is the biggest transfer of wealth in the history of humankind through illicit means, we are still pretty underresourced for it when you put it up against—we have got a DEA just to deal with narcotics. We have got ATF just for alcohol, tobacco, firearms, and bombs. Where are we in terms of what are we doing about this new threat?

So I want to applaud you for your own personal commitment in this issue, but I really do want to continue to push both the Department and the Bureau to resource this up. We will do everything we can to support your efforts to enhance the resources in the way that the budget requests—at least I will firm up this struc-

ture so it is clear that the people who are on the list as doing cyber work are, in fact, doing cyber work and not just—I have been a U.S. Attorney, I know the drill. Somebody has to get on the phone, somebody who is the cyber person, out goes the conference call, and so there is an AUSA in the offices across the country sitting there listening with the call on mute. That is not the way to fight this battle, and we should not really be counting those—it is a valuable function, but we should not be counting them as full-time cyber folks if that is the sum of what they are doing.

I like this notion of the threat focus cells that are being developed. Could you tell me, both of you, a little bit more about the new steps, the new structure that you are looking at for implementing the cyber and where on the curve between behind the curve and way behind the curve that we are in terms of the resources necessary to do this? Ms. Durkan, why don't you go ahead first?

Ms. DURKAN. Thank you, Senator. Let me unpack that a little bit.

First, let me say that I want to talk a bit about results, structure, and grand juries. You know, in the last 3 years I have been United States Attorney and served in this role as a cyber crime task force, the threat has evolved enormously. But I will say also so has the Department's response and our forward-looking nature. There is no one solution to this cyber threat, and no one part of Government can fix it alone.

As Mr. Demarest said, we have to have a one-team approach so every aspect of Government is working together, and we have to work with the private sector.

For example, in my district we have a very strong outreach to private enterprise to see what they are doing, see what the threats they are seeing to see what we can address. If we can prosecute someone, believe me, we will do it, and we have done it.

I want to report that results actually have been very good, and I will use my own district as an example. Even in the areas of botnets, our district was the center of a botnet investigation. Some people know it as the Conficker botnet. It was one of the largest—I think even larger than Coreflood, but that is my district. It was, as you know, a very resource-intensive investigation. It required multiple agents and multiple districts in multiple countries. But we were able to work with our international partners across law enforcement, Secret Service, FBI. We took down the entire botnet at the same time in America and in several European countries. People were arrested in several European countries, and we were able to extradite one of those actors to my district, prosecute them, and put them in jail.

So we have had successes, and we will continue to have those successes. But we also understand to meet this threat, we will not be able to prosecute our way out of it. We have to have technology answers. We have to have efforts from the Department of Defense, the Department of State, and all across Government from the top down, I think every agency is committed to addressing this threat.

It is a big threat, but I think we have great successes to report, and I am proud that we do.

Chairman WHITEHOUSE. Let me ask Senator Graham to jump in because he has to step out for a moment and make a phone call and then return to the hearing. But let me ask him to jump in.

Senator GRAHAM. Well, thank you, and you can continue to answer his question, which I thought were great questions.

From a lay person's point of view, we have a pretty robust system to deal with bank robbers. Is that right, Mr. Demarest?

Mr. DEMAREST. Yes, sir.

Senator GRAHAM. And do you have any idea how many bank robberies there were last year that the FBI was involved in?

Mr. DEMAREST. No, sir.

Senator GRAHAM. Probably hundreds?

Mr. DEMAREST. Hundreds.

Senator GRAHAM. How many cyber thefts are there in the United States?

Mr. DEMAREST. Hundreds per days, weeks.

Senator GRAHAM. Okay, so thousands, if not hundreds of thousands a year?

Mr. DEMAREST. Yes, Senator.

Senator GRAHAM. So there are two ways you can have money taken, stolen from you. A guy can come in with a gun and say, "Give me your money." Or somebody can hack into the bank and steal your money. How many people have been prosecuted for hacking into the bank and stealing the money?

Ms. DURKAN. Can I answer that, Senator?

Senator GRAHAM. Please.

Ms. DURKAN. Actually, very many. Let me use an example from our district. One of the things we saw was a spike in not just hacking but ATM skimming where people would put devices, pinhole cameras, and were able to take millions of dollars from many, many customers. We put together a task force and were able to break down a Romanian ring, and we prosecuted those people. We had great success. In fact, for a period of time in my district, we drove down the incidence of skimming to almost virtually zero. But we did it not just through the prosecutions but by working with the banking industry, educating the public, and the others.

Senator GRAHAM. How many people were prosecuted?

Ms. DURKAN. There were, I think—I will have to get you the exact number, but it was the entire ring responsible for this group of thefts. And so it was more than a dozen.

Senator GRAHAM. Okay. Well, get back with me.

Senator GRAHAM. The point I am trying to make is I know you all are doing a good job of trying to up our game, but the resources we have provided over time to deal with bank robberies, compare that to the resources we have provided over time to deal with cyber theft, how would you equate the two?

Mr. DEMAREST. Well, the threat is certainly changing, so the FBI has a reallocated resource which we had in other programs internally to cyber. So we significantly—and we will talk about structure, the Chairman's question, and what we have done to actually develop the teams both at headquarters and national platforms and also in our local field offices' Cyber Task Forces.

Senator GRAHAM. Do you have the resources necessary to deal with this, what appears to be a rampant theft problem?

Mr. DEMAREST. Well, we are making do on what we have today.

Senator GRAHAM. And I think what we are telling you is let us not make do, let us treat this sort of like Bonnie and Clyde. Remember the Bonnie and Clyde, you know, the national bank robberies during the Depression, that really started the FBI. It was sort of its reason for being in existence. And that kind of focus of dealing with, you know, crime in the 1920s and 1930s, do you think we have that kind of focus now, Ms. Durkan?

Ms. DURKAN. I think, sir, I would like to—I describe it as the "buggy whip moment." It has changed so much to where crime that used to happen on the street is now moving online, including violent crime. We have more and more violent crime that is being set online. Victims are being targeted online. And we are addressing that threat, but we still have a great brick-and-mortar threat we have to address on the streets, which we are doing. But it is a time when we have to allocate and realign ourselves. We have done it. We need to do more. And with the help of this Committee and Congress and——

Senator GRAHAM. Do you need changes in our laws to make you more effective?

Ms. DURKAN. Yes, and I think that we have proposed some changes. I think there are other changes that Senators have proposed, and Congressmen, that we are working with them and your staffs to see what—to make sure we address those threats.

Senator GRAHAM. During the 1920s and 1930s, we fundamentally changed the role of the Federal Government's involvement in crimes that were committed across State lines and really created Eliot Ness-type groups. And I would—that is maybe not a good analogy, but to me we seem to be having a new emerging crime wave here, and when it comes to resources and legal infrastructure, would you say on an A-to-F rating, A being we are exceptionally prepared, F we are failing—where would you put us in terms of legal infrastructure and resources to deal with this new kind of crime?

Ms. DURKAN. I think we are much better off than we were 3 years ago. I think we have aligned ourselves to address it and have had successes, but I think we have to keep working, and we have to make sure that we are aligned also with private industry.

Senator GRAHAM. Give the Congress an A-to-F grade and give law enforcement——

Ms. DURKAN. I give Congress always an A grade.

[Laughter.]

Senator GRAHAM. Well, you would be the only one.

Chairman WHITEHOUSE. She is the one person in the country.

[Laughter.]

Senator GRAHAM. I wish you were my teacher. How would you say our infrastructure——

Mr. DEMAREST. I think today we are still facing the same threats we faced 10 and 20 years ago, but now we have this parallel threat, if not emerging new threat, in addition to the old crimes——

Senator GRAHAM. Well, that is what I am saying.

Mr. DEMAREST [continuing]. Responsible for it.

Senator GRAHAM. How far behind the curve, to use Senator Whitehouse's analogy, are we?

Mr. DEMAREST. As far as the community, we are much evolved, even from the time the Cyber Division was created in 2002 to where we are today, and even over the past, I would say, 6 months or a year, sir.

Senator GRAHAM. Well, I think both of us want us to kick in gear and get there quicker.

Mr. DEMAREST. Yes, sir.

Senator GRAHAM. And wherever the Congress is failing, we are willing to try to inform our colleagues we need to up our game, because if you have hundreds of bank robberies using force and you have maybe millions of thefts using cyber technology, it seems to me we are probably not where we should be.

Chairman WHITEHOUSE. I know Senator Graham has to jump out for a moment, and I would like to continue this.

One thing I am going to do, without objection, is to put in the op-ed piece that Senator Graham and I wrote together into the record of this proceeding.

[The op-ed appears as a submission for the record.]

Chairman WHITEHOUSE. I want you guys to know, we have just confirmed a new OMB Director. We have got a new Deputy Director in the process of confirmation. I have spoken to both of them about this problem and about the concern that I have that you guys are good scouts and do not go beyond the envelope that OMB and the White House allow you in the budget. But we have to have a serious discussion and sit down and figure out what the plan is for dealing with this and have we really resourced it enough. And I have been trying for some time to get OMB and the Department in the room together so that we can have this discussion without you guys being accused of talking out of school without OMB there and vice versa. So I hope to do that.

Senator Graham and I came very close to having a bipartisan agreement on a cyber bill. It fell apart, unfortunately, at the last minute for reasons beyond both of our controls. And the Executive order emerged, and now that the Executive order is out and the landscape has been changed by that Executive order, we are re-engaged on trying to do what needs to be done legislatively.

So please work with us on this. We will provide whatever cover you need to bring OMB in so we can have a grown-up discussion in which you do not have to be flinching from saying what your real needs are. But it is very clear to me that when you put the privacy and the criminal loss of all of our individual credit card and personal information that is being hoovered up out of the Internet and actually marketed on crooked websites where crooks can actually go and buy personal information so that they can run crooked schemes off that info, you stack that on top of the attacks on the banks that Senator Graham was referring to, you stack that on top of the theft of so many companies' secret, special, confidential information that they use to protect themselves and build their product and that is their own intellectual property and that is stolen by industrial espionage, you throw on top of that what is being done to our defense industrial base, which has both private theft and national security connotations, and you throw on top of that the viruses and worms and programs that have been inserted into our critical infrastructure so that the grid could be taken down, bank

records could be compromised, dams could be opened, gates and pipelines could be opened, all those sorts of things could take place—you stack all that up, that is a big problem set.

I know I do not want to get you in trouble for saying any more than you are authorized to, but you have at least the two of us who strongly believe that we need to have our Eliot Ness moment on this and get ready to put the resources into this problem set. And one measure of that will be when we see some significant indictments on this industrial espionage piece related to what the Defense Department has said is being done, related to what the Mandiant company has said is being done, and all of that.

I will give you a chance to respond to those thoughts. We are kind of having a bit of a back-and-forth here, but I really want to push you on this because I think as wonderful as the work is that you have done, we are not there yet, and we need to make sure we get there, because we cannot for long remain on the losing end of the biggest transfer of wealth in human history through illicit means.

I see that Senator Coons has arrived, so rather than continue my peroration here, go ahead. Thank you for being here, Senator Coons. Senator Coons has taken a very sincere and strong interest in this issue and worked very hard with me and others to try to get that bill to the finish line before it fell apart and before the Executive order came out, and so thank you very much.

Senator COONS. Thank you, Senator Whitehouse. Thank you for your invitation. And to you and to Senator Graham and so many others who have dedicated time and effort and leadership to trying to make sure that we in the Congress are doing our part, we will give ourselves a low grade for how we have done in terms of being able to bridge the differences between our parties and our chambers in terms of coming up with some functional structure for dealing with the cyber threat to our Nation. And I am grateful to Senator Whitehouse for his persistent leadership in this very complex issue that crosses a number of committees of jurisdiction. My own home State—Senator Carper obviously chairs Homeland Security, but this also has implications in addition to Judiciary, for intelligence, for defense, for many others.

Let me just, if I could at the outset, ask a few questions. I have a piece of legislation I want to talk about, but if you would, help me understand in the run-up to some of this legislative work last year, a great deal was made about our military's unique capabilities to defend the United States in cyberspace and their advantages over other agencies in Government, civilian agencies, in terms of their capabilities and capacities.

What unique advantages do civilian agencies or the companies that the next panel will represent have in the realm of cybersecurity?

Ms. DURKAN. One unique ability we have is to put them in jail, and we are trying to do that more. But, again, I think that our ability to investigate and prosecute in these arenas I think forms a couple of important things.

Number one, we deter further activity, and believe me, when we are able to extradite someone who is a foreign national vacationing

in a different jurisdiction and we arrest them and bring them to Seattle and put them in jail, it sends a message.

Two, we try to disrupt because we do not have the capability to put all the bad actors in jail. So part of our strategy has to be to disrupt this activity anywhere we can do it.

And the third is we have to hold people accountable, which we are trying to do more and more. So I think that some of the unique capabilities we have is in our system we have the ability through the grand jury process, subpoena process, and investigative tools to get information that others do not have. And so—but, again, looking at the Department of Defense, we have to use a whole Government approach. Senator Whitehouse is exactly right that the nature of this threat frankly cannot be overstated. But it cannot be answered by any one part of Government or Government alone. It has to be private-public sector partnerships; it has to be Department of Defense, diplomatic efforts, and our civilian efforts to prosecute people.

Mr. DEMAREST. Senator Coons, the FBI is uniquely positioned based on statutory authorities, and cyber you know is cross-cutting, so it is a program that we have within the FBI that looks across criminal, counterintelligence, and also counterterrorism. So we are able to incorporate the subject matter expertise from each of those divisions and looking at the various threats. It is not just one area in counterintelligence, but it is a broad array.

And, again, getting back to Ms. Durkan's statements, too, DOD plays a key role along with NSA, the intelligence community writ large, and our other partners at home here—law enforcement along with Homeland Security.

Senator COONS. Thank you. Thank you for those answers, and I agree with you that in particular in a democracy and facing what is a broadly distributed threat, its origins not completely clear—it is not always attacks from nation states; it is not always attributable to specific foreign actors. Cyber crime and cyber threats come from a very wide range of sources, and they manifest in our country in a very wide range of impacts. And so the ability to complement the defense capabilities with agencies that have broad jurisdiction and with the capabilities to investigate, to deter, to imprison, to seek compensation for victims is a different response than one gets from the Defense Department.

I just wanted to comment, if I could, in my remaining minutes that when it comes to doing comparably broad things that deal with both domestic disorder, natural disaster, or with confronting foreign threats, the National Guard has also a broad range of capabilities. It crosses in its legal authorization, in its actual tactical capabilities, and in its strategic role a fairly broad range of capabilities. And so a number of us Senators—Gillibrand and Vitter, Blunt and I—have introduced the Cyber Warrior Act, which, among other things, would give Governors the capability to order cyber-capable guardsmen to support and train local law enforcement, to leverage the expertise they have from their military training and their civilian careers. My own home State happens to have a very capable network warfare squadron which allows us to tap into the skills and abilities of the fairly sophisticated data centers operated by the advanced elements of the financial services community that are

headquartered in Delaware and have them also in a dual-hatted way through the National Guard serve as adjuncts to the NSA and be helpful.

I think this sort of function in this particular legislative authorization would be helpful for DOJ and FBI as well, because it can help them have more capable, better prepared State and local partners. And I would certainly welcome recommendations or comments from you or from the other witnesses in the next panel. We will be holding a law enforcement caucus event on this particular idea in this bill in June, and I am grateful to Senator Whitehouse for the chance to contribute to this hearing this morning.

Thank you, Senator.

Chairman WHITEHOUSE. Thank you, Senator Coons. We in Rhode Island also have a cyber wing in the Rhode Island Guard, and I look forward to working with you on your legislation. I think it is a very valuable thought. It is, I think, important for the record of this proceeding to reflect that when you move from our local guard and reserve capabilities to our military, and from there to our active-duty military, and from there into our intelligence services, there are increasing restrictions and concerns about taking action within the continental United States, particularly where it involves American companies, systems, and individuals. And so that is, I think, a particular reason why our law enforcement role is so important when we look at this domestically.

We are joined by Senator Klobuchar, a former prosecutor herself, and we are delighted to recognize her.

Senator KLOBUCHAR. Thank you very much, Mr. Chairman. Thank you to both our witnesses. And I was listening to Senator Coons and thinking about back to when I did my job for 8 years, running an office of about 400 people, but two levels of issues with computer crime, cyber crime. One was officers who, despite their best efforts, just did not have the training, so we would have cases where they would go into a room and turn on a computer and then erase everything on it because that is how it was rigged, what it was rigged to do. And it happened a number of times. And the second thing was we are second per capita for Fortune 500 companies, so we have huge companies like Target and Best Buy and companies like 3M and U.S. Bank. So I have firsthand seen how challenging the situation is and how as a local prosecutor we simply did not have the resources or the know-how to handle some of those cases when they would come our way or it would be handled by the U.S. Attorney's Office.

So my first question is on that, to you, Ms. Durkan—thank you for your good work—just how you have coordinated with the local prosecutor's office, how do you think—what is the best model of how we go forward and how we get them trained?

Ms. DURKAN. That is an excellent question, and, again, the partnership with local law enforcement is critical to our successes. Working both with the Secret Service Electronic Crimes Task Force and the FBI's task force, we have great successes in that field. Key to it is training, and we have worked to make sure that we have more not just task force officers but forensic people who can handle this, and also education of the public.

An example of a success where that has worked in my district is we had a very small family restaurant that was hacked by someone who was in Maryland who attacked a number of point-of-sale people. He stole many, many, many credit cards. He sold them to someone who was in Romania, a citizen of another country, who then posted them to a carding site. Then they were purchased by a gang-affiliated group in Los Angeles.

Through our investigation we were able to arrest the person in Maryland, charge and extradite the person in Romania, and get the person in Los Angeles. So we got all three levels of that. We did it, though, working with our local law enforcement, task force officers, the Secret Service, and the FBI all played a part in those and other investigations. So it is a critical part of it.

The training also, if we look at our training for lawyers, we have worked to make sure that not just our CHIP lawyers are trained in cyber activities but other lawyers have experience. We have the National Advocacy Center in South Carolina, and one of the conferences, even in these difficult times, that we made sure went forward was our cyber conference, because we have to make sure our prosecutors are trained, our local law enforcement is trained, and the public is educated.

Senator KLOBUCHAR. Well, and I think that is part of it, especially with small businesses, which you noted are not going to have the resources of a U.S. Bank in Minnesota. So I think more outreach to them would be a good idea through chambers or anything, because I think they are starting to be victims as well and they just do not have the resources.

Ms. DURKAN. That is absolutely right. And if that small business had not come forward in our case, we would not have had that case. And so having that outreach also enables us to do our job.

Senator KLOBUCHAR. Okay. My next question is on the cloud computing area and the fact that our cases are becoming more and more sophisticated. As you know, digital evidence evaporates a lot quicker than a paper trail, making it very difficult for law enforcement to investigate the crime. And another challenge is if the evidence is incriminating information, it is stored in the cloud out of the jurisdiction of the United States. I had a bill on this that is sort of floating out there like a cloud as we try to deal with some of the cyber bills that I think are important.

Could you comment on the challenges of a lifetime of evidence in cybersecurity crimes and the real possibility that the evidence could be outside the jurisdiction of the United States?

Mr. DEMAREST. There is a very good likelihood that it will be outside the jurisdiction of the United States. As you pointed out, Madam Senator, it presents many challenges, and depending on which country that the evidence may lie, our relationship with that country, with the investigative agencies of that country as well. So it does present several challenges on that front.

Senator KLOBUCHAR. And what would be the best way to try to get at it? Would it be agreements with other countries? Is there something we could put in law that would create a structure for those agreements?

Mr. DEMAREST. Well, I think the agreements, and then I will defer to Ms. Durkan as far as what law or what other changes that

we could possibly put in place to better the circumstances in working with our foreign partners.

Ms. DURKAN. I think it is all of the above, Senator, that you have mentioned. You will notice that one of the budget increases we have asked for is to have additional prosecutors overseas. We have seen more and more of these cases arrive on international soil. Our partnerships with foreign nations in Europe particularly have increased, but we need more people there.

We also have the Budapest Convention, which is gaining more and more international partners to make sure we can get the evidence abroad that we need to prosecute people here. But they cannot get the evidence from our country that they need there. So we have to do all of those things.

Mr. DEMAREST. Madam Senator, we have increased our footprint overseas from just three offices to it will be just short of a dozen this coming year in key locations throughout the globe.

Senator KLOBUCHAR. Thank you. I appreciate it.

Chairman WHITEHOUSE. Senator Graham had his time interrupted both by me and the call he had to take, so let me turn to him and give him a fresh start.

Senator GRAHAM. Just very quickly, we are facing a law enforcement threat, people stealing our property, our intellectual property, stealing our money, and anything else of value through cyber crime. But on the Nation state, national security, counterterrorism, after 9/11 the FBI has two missions now, counterterrorism—right?

Mr. DEMAREST. Yes, sir.

Senator GRAHAM. As well as traditional law enforcement. Are there clear rules of engagement that exist today that would allow the FBI, the CIA, the Department of Defense to engage a nation state who has committed a cyber attack under the laws of war?

Mr. DEMAREST. There has been a lot of discussion and a lot of coordination. We mentioned——

Senator GRAHAM. Well, that means no.

Mr. DEMAREST. No, well—I am sorry. The question again, Senator?

Senator GRAHAM. Are there any rules of engagement—I mean, has anybody sat down and said this event would be considered a nation state cyber attack allowing us to respond outside the law enforcement model? Our Chinese friends seem to be hell bent on stealing anything they can get their hands on here in America rather than developing it in their own time and economy. But I am more worried about what they could, or other nation states, not just China, or terrorist organizations could do to our ability to defend ourselves. Do you worry about a cyber 9/11?

Mr. DEMAREST. Well, again, depending on—it is an extremely complex issue, and what actor set you may be referring to or looking at, different motivations by many——

Senator GRAHAM. Is that possible? Is it possible that through cyber technology you could create a 9/11-type event on America?

Mr. DEMAREST. It is possible that they could cause significant damage and destruction through cyber. It is possible.

Senator GRAHAM. What kind of things would be possible?

Mr. DEMAREST. If you look at access to ICS or SCADA systems, if they do get access to, say, oil and energy and the systems that

actually control key networks or critical networks, that could cause significant damage, and whether it be long-lasting or short-term, it could be both.

Senator GRAHAM. Could they disrupt military operations?

Mr. DEMAREST. I am not sure, sir.

Senator GRAHAM. Well, maybe this—would you like to take a crack at that?

Ms. DURKAN. I think, Senator Graham, that if you look at the range of threats——

Senator GRAHAM. Maybe this is better for Senator——

Ms. DURKAN [continuing]. It is what keeps me up at night——

Senator GRAHAM. Or General Alexander, I guess.

Ms. DURKAN. I think part of these questions have to go to General Alexander. But I do think if you look at the range of threats, anything with intelligence can be hacked—everything from one rogue actor to state actors to criminal organizations—and there are people who work to get that done. That is why the Department of Justice is part of the solution, but it is not the whole solution. And, again, private enterprise is developing better security mechanisms and better technology.

Going back to robbing banks, when banks were set up, they did not all have bars, they did not have cameras, they did not have a lot of defenses. And private companies are now determining technology they have to develop to also provide part of that solution.

Senator GRAHAM. Well, both of you focused about the law enforcement model here and how we can go after bad actors. Are you familiar with the counterterrorism threats? Are you familiar, both of you?

Ms. DURKAN. Yes, sir.

Mr. DEMAREST. Yes, sir.

Senator GRAHAM. Okay. How would you rate our infrastructure on the counterterrorism side, the national security side, to protect us against people who just do not want to steal money but want to do more damage?

Mr. DEMAREST. Well, I think based on the tragic losses of 9/11, part of the response to that in New York and also here at headquarters, I think it is a much more developed model that I think the community has in addressing counterterrorism issues.

Senator GRAHAM. So we are further down the road?

Mr. DEMAREST. Well, I think we are further down the road, and for good reason.

Senator GRAHAM. Do you agree with that?

Ms. DURKAN. Absolutely.

Mr. DEMAREST. And I think we will get there, Senator, with cyber as well.

Ms. DURKAN. And if I could just use one example, the National Security Cyber Specialist, while it just sounds like another Government alphabet soup, one thing we realized in the national security setting, if there is a cyber event or we get intelligence that there is going to be, who do we call? Do we call the cyber lawyer who may not have the security clearances? Do we call the antiterrorism lawyers who may not have the cyber experience? We knew we had to marry those two things up, so that is what we are trying to do,

is to make sure that we have the right, appropriate people in every office and the best expertise we can have in here to get to the field.

Chairman WHITEHOUSE. Let me, before I release you guys and call up the next panel, ask you two things. One is, Could you in a supplemental fashion to the testimony that you have provided make a little bit more of a detailed case as to the conclusion you describe in both of your testimonies about how complicated, complex, resource-intensive, et cetera—as much as you can without revealing things that should not be revealed, try to put some tangible facts and real teeth into that discussion, because it will help both Senator Graham and myself in arguing with our colleagues for this if we have more than the conclusory statement that these are complex, difficult, require forensic capabilities or unusual—and really lay out a case study or an example of something that makes that case a little bit further. That would be very helpful to us as we try to proceed.

The second thing is we have had this discussion about resources and structure and budgets, and I look forward to continuing that discussion with the new OMB Director and with your Department and your Bureau. But separate from that, I think we can make some progress on your capabilities and authorities and safeguards in taking out these botnets. And I would ask you for your commitment to work with us in drafting appropriate legislation that will allow you to have more authority and proper safeguards as you go after future Corefloods and future Confickers. Would you do that?

Ms. DURKAN. Absolutely, Senator.

Mr. DEMAREST. Yes, sir.

Chairman WHITEHOUSE. Terrific.

Ms. DURKAN. Thank you.

Chairman WHITEHOUSE. Again, let me close by thanking both of you for your service and for your passion in this area. I am really pleased that people like you are in our Government service. And if you detect a note of impatience from myself and from Senator Graham, it comes with the recognition that you are parts of very, very large bureaucracies that do not always move with great alacrity, and it is sometimes our job to give them a little bit of a shove. But it reflects not at all on either of you or on the folks who are working this problem set. It is being done very impressively.

Thank you very much.

Ms. DURKAN. Thank you, Senator.

Mr. DEMAREST. Thank you.

Chairman WHITEHOUSE. We will take a minute to call up the new panel.

[Pause.]

Chairman WHITEHOUSE. Let me thank our private sector representatives for being here.

Kevin Mandia is the CEO of Mandiant Corporation, which he founded in 2004 to help private organizations detect and respond to and contain computer intrusions. When you find out you have been hacked, "Who are you going to call? Ghostbusters." That is kind of what Mandiant does. He began his career in the U.S. Air Force, in which he served as—Senator Graham is also in the Air Force—a computer security officer and as a cyber crime investigator. He has degrees from Lafayette College and the George

Washington University. He has also taught at both George Washington and Carnegie Mellon Universities.

Let me just stop there, and I will call on Kevin. But let me also—back in our earlier legislative process, Senator Graham and I and Senator Mikulski and others organized a series of classified briefings for Senators to try to bring them more into awareness of what was going on in this field, and you were gracious enough to come and make one of those presentations, and it was a very effective one, and I want to thank you for that.

Let me ask you to proceed with your testimony, and then I will introduce the other witnesses as they are called up.

Mr. Mandia.

STATEMENT OF KEVIN MANDIA, CHIEF EXECUTIVE OFFICER, MANDIANT CORPORATION, ALEXANDRIA, VIRGINIA

Mr. MANDIA. Thank you, Mr. Chairman and Ranking Member Graham.

Today, and into the foreseeable future, American companies are going to be under siege by many different types of attacks—criminal attacks, economic espionage, more than nuisance-based attacks. Today what I am going to talk about is the sophisticated economic espionage attacks. And while many organizations are actively trying to counter these threats, at the end of the day there is a security gap that we need to close. So today what I would like to talk about is three things: why the security gap exists; what the private sector is doing about it; and then how law enforcement can help in regards to that security gap.

First, the reason the security gap exists is that there are Government resources hacking our private sector. It is simply an unfair and imbalanced fight. If our Government was chartered to hack the private sector in other countries, we would be very successful at that. So I always likened it to an ultimate fighting champion mugging my grandmother. It is simply an imbalanced battlefield.

Mandiant pointed that out when we did an APT1 report. In February of this year, we released a report to the public that clearly shows that there are members of the PLA targeting the private sector here in the United States.

The second reason there is a gap in our cybersecurity is that—for the first time in history that I am aware of—it used to be when systems were targeted, nobody knew who used that system. But today the cybersecurity attacks, there are human targets, and we also showed that in our APT1 report in that the PLA is recruiting English-speaking people so that they can send those innocuous-looking emails, but, in fact, those innocuous emails that have fake information in them and purport to be from someone they are not and are compromising systems. So we have human targets, and we have not figure out technically how to patch the human trust.

The third reason is that the government entities that we see compromising the U.S. private sector are actually compromising a lot of the supply chain. So we have the big companies that have a rather mature security program, so if that security program is bolstered and it starts rejecting some of these attacks, what the attackers do is go down the supply chain, hit smaller organizations

that only have hundreds of folks, and potentially no cybersecurity posture, and that is a tough one to defend.

The fourth reason we have a security gap is because there is simply an imbalance. It only takes one attacker, and that one attacker can create work for thousands, if not hundreds of thousands, of defenders. It is just an imbalance in the expertise that is required.

Another reason, there is simply no risk of repercussions to hacking the U.S. infrastructure if you do it from certain safe harbors or safe havens, such as apparently China, potentially Russia, North Korea, Iran. These are countries that could hack our resources with impunity and not really fear any repercussions.

We also have a lack of resources, and I can go on. But, in short, technology and our adoption of it vastly outpaces our ability and willingness to secure it.

So what are companies doing about it? Essentially, I have noticed two things. There are companies that are aware they are compromised, and they are doing some—really they are adopting technologies and hiring the expertise to defend. And, Senator, you had mentioned we are unwilling to oppose China. I would say in my experience most of the private sector takes it very seriously when they have had a breach from China to do everything they can on the technical front to bolster their safeguards. And I think that the fear and unwillingness is more a public admission as to what happens based on the fear of shareholder value repercussions, and at the same timeframe, because simply the economic gains could be so great in China. So it is a very tough issue. But make no mistake, on the cybersecurity side, folks are doing a lot in the private sector when they are aware of the breach and have the resources to do something about it.

Then there are a lot of companies that are pre-aware that they have had a security breach, and they could be making very important intellectual property for our country, but they simply do not have the defenses to safeguard it. Those companies are beholden to standards legislation or regulations to create some kind of security posture, and it has been my experience that if your sole driver for security is some kind of compliance, that compliance usually does not prevent the attacks we see.

So what can we do about it? What can the FBI or law enforcement do to help?

The FBI already conducts outreach to American companies that have been compromised by advanced threat groups. Indeed, about two-thirds of the breaches Mandiant responds to are first detected by a third party. So if we do what we can to have—and the detection could be the DOD, it could be the intel community, but I have seen the communication come from the FBI. If the FBI narrows that gap and notifies quicker, we can eliminate the impacts and consequences of breaches.

And while private industry will not always win the battles being fought in cyberspace, if we share that information in a timely and codified manner, what you will see is we can limit the impact of the breaches, limit the consequences, and we just need to be able to share that information, and I think law enforcement is the arm that can do that.

By establishing a system where law enforcement and the private sector share proactively and use this threat information, America will build a cyber defense that is actually dynamic. No one is getting any smarter from these breaches today.

So with that, I would like to thank you very much for this opportunity to share with you.

[The prepared statement of Kevin Mandia appears as a submission for the record.]

Chairman WHITEHOUSE. Thanks, Mr. Mandia.

Our next witness is Stewart Baker. He is a partner at Steptoe and Johnson here in Washington. From 2005 to 2009, he was the first Assistant Secretary for Policy at then the early stages of the Department of Homeland Security. As an intelligence lawyer, Mr. Baker has also been general counsel to the National Security Agency and general counsel to the commission that investigated weapons of mass destruction intelligence failures that took place prior to the Iraq war.

Mr. Baker, welcome. Thank you.

STATEMENT OF STEWART BAKER, PARTNER, STEPTOE AND JOHNSON, LLC, WASHINGTON, DC

Mr. BAKER. Thank you, Mr. Chairman, Senator Graham. I am going to sound some of the themes that Kevin sounded and then turn to the question of what the role of the FBI and the Justice Department could be, should be. I will not spend too much time. As Kevin demonstrated, we are not likely to defend our way out of this problem. Defenses play an important role. I have been very supportive of the legislation and the Executive order, but it is not enough. It is as though we were trying to solve the street crime problem by telling pedestrians to buy better body armor every year. That is not a complete solution. We have to find the criminals, and we have to deter them. I do not have to preach to either of you about the importance of that.

But in thinking about that, the real question is how can we best reach the threats that are most troubling to Americans today, which is the government-protected attackers. And there it seems to me that both the Justice Department and the FBI suffer from a lack of imagination about authorities and a lack of imagination about resources.

With respect to their authorities, prosecuting the people who are attacking us who are protected by nation states is deeply unlikely, and we need to find additional mechanisms for deterring that activity. The administration is doing some naming and shaming. That is a good thing. But we should be using our visa authorities to say if you participate—if you train hackers in a country, if you hire hackers after they finish their tour of duty as hackers in the government, you are going to have to cooperate in investigations, or you are not going to get visas to come to the United States.

The same thing is true for the Treasury Department which designates nationals with whom we will not do business. We will not do business with people who are bad for human rights in Russia or in Belarus. We will not do business with people who are engaged in conflict diamond transactions. I think we should take at least as much care to protect against people who are abusing human rights

right here by breaking into the computers of dissidents and ordinary citizens. So we should be using those tools as well.

I see that Senator McCain, Senator Levin, Senator Coburn, and Senator Rockefeller have just introduced a bill that goes down this road, looking for tools to deter government-sponsored attacks. Just the names of the cosponsors gives me a lot of hope, and I think that the approach of looking for ways to deter the beneficiaries of this espionage is really worth pursuing.

Let me turn now to the question of resources, which is profound and probably not solvable in our current budget situation. Chairman Whitehouse talked about the JTF that notifies people about attacks on their networks. This is enormously effective because many people do not know they have been exploited for months. But at the end of the day—and I have worked with clients who have had this experience—the FBI's role basically is to figure out that somebody has been compromised and to tell them. And maybe they can give them a little bit of advice, but, frankly, after that it is a little like having somebody tell you your bicycle has been stolen. You are not going to get a lot of help from the police tracking that bicycle down because they do not have enough cops to do it. And the FBI will not be able to help all the companies that they are notifying. In fact, after they have put a few person-days into the investigation and made the notice, the company is largely on its own, and the company goes out and hires somebody like Kevin Mandia or like Symantec, and it begins a process of spending hundreds of thousands of dollars, sometimes millions of dollars, to get the attackers out of its network and to figure out who is attacking it.

We know from the report that Mandiant has done that they gather enormous volumes of information about who is actually attacking their clients. We should be working much more effectively to utilize that information to build it into mechanisms that will deter the attackers by outing them.

The biggest problem that I think we face is that even though private sector resources are enormous and they are well focused on particular attacks, we do not let the individuals who are under attack or the experts whom they have hired go beyond gathering evidence in their network and perhaps a few networks that will cooperate with them voluntarily inside the United States.

I am not calling for vigilantism. I am not calling for lynch mobs. But we need to find a way to give the firms that are doing these investigations authority to look beyond their own network, perhaps under guidance from the Justice Department, and certainly without doing harm to the networks that they are investigating. They need to enter the networks where the hackers are storing all of their stolen data, to retrieve the stolen data, and to gather enough evidence to actually prosecute the attackers.

My deepest disappointment here, and the reason I think that just pouring more money into the Justice Department at this point is a dubious proposition, is the Justice Department's reaction to that idea has been to pour as much cold water on it as they can, to say, "We think that is a bad policy idea, and probably illegal." Justice is deterring companies that want to investigate the people who are attacking them and provide that information back to the

Government. Justice is saying, "Well, you can give the evidence to us, but we might indict you instead of the hacker." That is just the wrong answer.

And so my suggestion would be that we find mechanisms to provide the kind of oversight that is necessary so that we are not just authorizing victims to shoot in the dark, but we are authorizing people who know what they are doing to carry out investigations and pursue attackers back to what they currently think is their safe haven in another country. If we do not do that, we will never get to the bottom of most of these attacks.

Thank you.

[The prepared statement of Stewart A. Baker appears as a submission for the record.]

Chairman WHITEHOUSE. Thank you.

Finally, Ms. McGuire from Symantec. Thank you for being here, and thank you for so much that Symantec has done to be helpful in our process of trying to get to legislation.

STATEMENT OF CHERI F. MCGUIRE, VICE PRESIDENT, GLOBAL GOVERNMENT AFFAIRS AND CYBERSECURITY POLICY, SYMANTEC CORPORATION, WASHINGTON, DC

Ms. MCGUIRE. Thank you. Chairman Whitehouse——

Chairman WHITEHOUSE. I think your microphone may need to be turned on.

Ms. MCGUIRE. Thank you. Chairman Whitehouse, Ranking Member Graham, it is my pleasure to testify here before you today.

My name is Cheri McGuire, and I am the Vice President for Global Government Affairs and Cybersecurity——

Chairman WHITEHOUSE. I should have done a more complete introduction. Ms. McGuire served in various capacities at the Department of Homeland Security, including Acting Director and Deputy Director of the National Cybersecurity Division and the US–CERT. So she comes not only with her experience at Symantec but with considerable Government experience, and I am sorry I omitted that.

Please proceed.

Ms. MCGUIRE. Thank you very much. So Symantec is the global leader in developing security software, and we have over 31 years of experience in developing Internet security and information management technology. Today we have employees in more than 50 countries and more than 21,000 employees with us.

In particular, I would like to mention our Global Intelligence Network, or what we call the GIN, which is comprised of more than 69 million attack sensors in more than 200 countries, where we record thousands of Internet events per second, which gives us incredible insight into the worldwide threat landscape. In addition, every day we process more than 3 billion email messages and more than 1.4 billion Web requests at our 14 global data centers.

As I said, these resources allow us to capture worldwide security intelligence data that gives our analysts a view of the entire Internet threat landscape.

A few key findings from our latest Internet Security Threat Report that I would like to share with you include a 42-percent rise

in targeted attacks in 2012 and 93 million identities exposed through hacking, theft, and simple error.

In addition, we estimate that there were 3.4 million bot or zombie computers worldwide, and one in seven, or 15 percent of these, were actually located in the United States. We also saw a 52-percent rise in the threats to mobile devices.

Another disturbing trend was the expansion of what we refer to as "watering hole attacks." These are efforts by attackers to compromise legitimate Web sites so that every visitor runs the risk of infection. Criminals often use these sites to distribute ransomware, which is a type of malware or type of malicious software that locks a user's computer, displays a fake FBI warning, and attempts to extort money from the user in return for unlocking the computer, which, oh, by the way, usually does not get unlocked even after the user pays the extortion.

Now, Symantec participates in numerous industry organizations as part of our global commitment to fighting cyber crime as well as numerous public-private partnerships in the U.S. and abroad to address these and other cyber threats. Just a few of these successful partnerships include the Norton Cybersecurity Institute, the National Cyber Forensics and Training Alliance, the FBI's Infraguard, the U.S. Secret Service Electronic Crimes Task Force, and Interpol. I have provided more information about each of these in my written testimony, but I do want to highlight a few.

For example, 2 years ago, we established the Norton Cybersecurity Institute to help address the critical shortage of investigators, prosecutors, and judges who are adequately trained to handle complex cyber crime cases. Through the Institute, we coordinate and sponsor technical training for law enforcement globally. We also publish the annual Norton Cyber Crime Report, which is one of the largest global cyber crime studies that interviews more than 20,000 users globally across 24 countries.

Another example that I would like to highlight is the National Cyber Forensics and Training Alliance, which includes more than 80 industry partners and provides members with real-time cyber threat intelligence to help identify threats and their actors and which has been a key player in the fight against some of the financial sector intrusions that have occurred recently.

These partnerships have led to some notable successes, and one example is the takedown earlier this year of the Bamital botnet, which compromised millions of computers being used for criminal activities such as identity theft and click fraud. This takedown was the culmination of a multi-year investigation—many would say that it takes far too long to complete these investigations—and demonstrates what can be done when private industry and law enforcement join forces to go after cyber crime networks. I have also detailed in my written testimony similar successes in Operation Ghost Click as well as Coreflood, which have been mentioned earlier in other testimony today.

Unfortunately, these examples highlight just how much still needs to be done. For a while we have seen some successful prosecutions and takedowns, as, Chairman Whitehouse, you described in your opening statement, there are undoubtedly more and larger criminal rings that are operating today, and the relative dearth of

cases like these is not because the Government does not want to pursue them or because the criminals are not out there. In fact, the investigators and prosecutors, at least we have found, are quite willing and many in the private sector are even eager to help. But, unfortunately, prosecuting cyber crime cases requires a highly technical understanding of how computers and networks operate as well as a deep knowledge of multijurisdictional legal issues.

There are simply not enough investigators, prosecutors, or judges with this technical training to keep up with the cyber criminals. Thus, as you have already heard today, there is a low bar for deterrence.

At Symantec, we are committed to improving online security and securing our most critical infrastructure as well as their data across the globe, and we will continue to work collaboratively with governments and industry on ways to do so.

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

[The prepared statement of Cheri F. McGuire appears as a submission for the record.]

Chairman WHITEHOUSE. Thank you. Let me thank all the witnesses for their very helpful testimony.

I am going to turn immediately to Senator Graham, as his schedule is starting to tug at him, and I am going to be here until the end of the hearing. So, Senator Graham, let me thank you very much again for being the Ranking Member on this and for the intensity of your effort at protecting our Nation in a variety of areas, but particularly in this new cyber area.

Senator GRAHAM. Thank you, Mr. Chairman. Enjoy the easy question period you are about to embark upon, because he will be back.

I really have learned a lot from Senator Whitehouse and the witnesses today, but just to keep this sort of at a 30,000-foot level, Mr. Baker and Kevin, do you both agree that China as a nation state is actively involved in hacking into U.S. databases, banks, stealing intellectual property? Is that a fair statement?

Mr. BAKER. Yes.

Mr. MANDIA. I would agree that is the case.

Senator GRAHAM. Could you give me, both of you, two pages of why you say yes? And I am going to take it to the Chinese Ambassador and ask him to give me a response.

Mr. MANDIA. I will give you about a hundred pages, sir.

Senator GRAHAM. Yes, which will be consolidated to two.

[Laughter.]

Mr. BAKER. Yes, absolutely. Kevin's company has done the most——

Senator GRAHAM. Using very big words.

Mr. BAKER. But other research——

Senator GRAHAM. Russia?

Mr. BAKER. Russia is harder to identify as a country because they are more stealthy.

Senator GRAHAM. Well, let us rank the bad actors here. Would you say China is number one?

Mr. MANDIA. China is the number one reason my company grows. It doubles in size every year. So, yes, they are number one.

Senator GRAHAM. Good news/bad news, I guess.

Mr. MANDIA. Yes.

Mr. BAKER. China by far in terms of volume is the most aggressive and is doing the most——

Senator GRAHAM. Who would be second?

Mr. MANDIA. There is a battle for second.

Senator GRAHAM. Could you give me the top five?

Mr. MANDIA. I think it aligns with safe harbors, so you are going to see Middle Eastern organizations emerging. It goes China first, probably Russia second, but it has been my opinion that the rules of engagement between Russia and America, it is almost like we have worked it out. If we see the Russians—generally their government only hacks our Government. If we see them, they tend to go away. The Chinese are like a tank through a cornfield. They just keep mowing through it. And I think there is an enormous gap between China first, Russia second. But I think second is there is competition there. I think we are starting to see attacks coming out of the Middle East more at this point.

Senator GRAHAM. Okay. Give me the top five, because I am going to get with Senator Whitehouse, and we are going to try to do something about this. We are going to try to put nation states on notice that if you continue to do this, you are going to pay a price. And visa programs are all kinds of tools available to us as politicians up here to put the bad actors on notice, and maybe the immigration bill would be a good opportunity to do that. We have got to think outside the box.

Now, when it comes to cyber 9/11s—and I have got 2 minutes and 20 seconds—could you in 20 or 30 seconds describe what you think a cyber 9/11 could look like? Mr. Baker, then——

Mr. BAKER. Sure. Very briefly, if you can break into a network, you can probably break it, and there are no networks in the United States, as far as I can tell, that have not been broken into. So all of them can be attacked. And in many cases, you can move to the equipment that runs on that and break that. We demonstrated that when I was at DHS with a big generator. Just by sending code to it, we burned it up. And so the real risk here is that an attacker that is determined could break into our industrial control systems and wreck power systems, pipelines, refineries, water, and sewage. You know, New York City, without all of those things, is going to be a very unpleasant place, and if the crisis lasts for a week, it will feel worse than 9/11.

Senator GRAHAM. Do you have anything to add there?

Mr. MANDIA. I think it is complex to determine what will happen when somebody tries to bring down an electric grid. Even from the attacker's perspective, you may get unpredictable results. I remember during the Super Bowl when the lights went out, everybody was, like, "Was that cyber?" But the results would be very unpredictable. I would give you two things.

One, we should see and we might see shots across the bow before it happens. I do not think the first attack, if it is truly remote, will be noticed. The catch is I think that if it does happen, it is going to come from a third grade classroom in Mississippi somewhere. It is going to come from an IP address here in the States or from a

human operator here in the States, and then it will branch out from there.

The second thing is that hopefully we have the controls in place—and this is what is most important—to know who did it, because I think the deterrence for that kind of act is outside of the cyber domain.

Senator GRAHAM. Ms. McGuire, you mentioned about the law enforcement resources and model. How would you rate our legal infrastructure in terms of providing the tools necessary to actively go out and attack cyber theft and create deterrence without all of us having to worry about more body armor? And from a resourcing point of view, how advanced are we? Give a grade from A to F. Legal infrastructure and the resources available to our Government to fight cyber crime.

Ms. MCGUIRE. I think from a standpoint of our actual legal infrastructure, we have a pretty strong legal infrastructure in this country. But being equipped to address cyber crime, as I mentioned in my opening statement, is something that we need to play catch-up with. There is quite a gap there because we just do not have the number of investigators, prosecutors——

Senator GRAHAM. Well, give us kind of a wish list of what you think we would need to get to where we want to be.

Ms. MCGUIRE. Well, I think that we clearly need more investigators, prosecutors, and judges who are equipped and trained with the necessary skills to address these kinds of actions. That is a pretty big gap that we have today. The folks who are out there are doing yeoman's effort. Probably most of them would say they are overworked and they cannot keep up with the volume that they are being presented with every day.

Senator GRAHAM. I do not want to run over, but given the threat and given the focus, is there a big gap there? He mentioned a security gap. Is there sort of a gap between the threat we face as a Nation and the amount of resources we are supplying to the threat, to meet the threat? How big is that gap?

Ms. MCGUIRE. I do not know if I could actually quantify how large that gap is, but I think suffice it to say that there is a gap. It is a significant gap. We are not putting enough resources against this today. What you mentioned earlier about the way that we approach burglaries and robbers, we do not put the same type of emphasis on cyber criminal and cyber crime activity today in this country. We are making progress, but we have got a really long way to go to catch up.

Senator GRAHAM. Thank you, Mr. Chairman.

Chairman WHITEHOUSE. Thank you, Senator Graham.

Let me do a couple of follow-ups. First of all, Mr. Mandia, when you mentioned that a big attack might very well come through a classroom in Mississippi or through somebody's individual computer, you did not mean that it would be originated there. You were referring to an attack starting overseas that would have come through a slaved computer there so that it would look as if that was the source. But clearly that is the level of sophistication that our enemies are operating at, is that they could slave a Mississippi classroom computer to use that to vector attacks into our critical infrastructure. Correct?

Mr. MANDIA. That is absolutely the case. Almost every single attack that we currently respond to, there are hot points in between, but they are all in the United States. These attacks are not coming straight out of China straight into the end victim. They are being routed through vulnerable sites, and the real challenge that we have, sir, is that the protocols—nothing looks bad about the traffic going from a nation state to a third grade classroom in Mississippi. It is going to look like normal access. It looks bad when it goes from a classroom to the real target. So it is going to be very complicated to prevent that.

Chairman WHITEHOUSE. And if you are looking at—you mentioned China and Russia. If you are looking at what we would call, for want of a better word—I do not think it is the best word, but it seems to be the word that has developed—"advanced persistent threats" versus, say, botnets and big criminal siphoning efforts, the Chinese effort is much more in the direction of advanced persistent threats and of attacking our intellectual property and trying to insert potential sabotage, cyber sabotage, into our systems, and not so much engaged in botnets and that kind of activity; whereas, from the Russian side, there is both official and criminal network activity, and that is much more involved in stealing and spamming and botnets. So they are a little bit two different problem sets, depending on the source. Is that correct?

Mr. MANDIA. That is correct, and at the highest level of abstraction, when you think botnet, I would think it is a consumer problem, not necessarily an enterprise problem, but it does cross into companies having to deal with it, and it is a criminal element using it. And then with the targeted attacks, the criminal element uses them, but when you think economic espionage, most of those are targeted attacks, very sophisticated attacks.

Chairman WHITEHOUSE. Now, if I heard you correctly in your testimony, you said that two-thirds of the time when you respond to a company that has said, "We have been hacked," they had no idea that they had been hacked until some Government agency warned them, often the FBI—usually the FBI, sometimes the Department of Homeland Security.

There was a time not too long ago—and I am just using my recollection now—when my recollection is that both your company and the NCIJTF, the FBI operation, indicated that when they went out, 90 percent of the time they were the bearers of bad news to companies that had no idea, a little bit like the U.S. Chamber of Commerce, which, while busily attacking our efforts to get legislation in this place, also had basically the Chinese throughout all their systems right down to the fingernails for months and months and months and months, and had no clue about that until the Government came and told them, "By the way, I think you have been hacked."

Has it shifted from 90 percent to two-thirds? Is my memory failing me or——

Mr. MANDIA. No, no.

Chairman WHITEHOUSE [continuing]. Something that has happened where there is a little bit more awareness in the private sector now?

Mr. MANDIA. I would not even equate it to awareness, sir. We had a misleading figure. Quite frankly, when Mandiant reports that, it is based on the incidents that we respond to. I have been responding to Chinese intruders since 1996. Over time, it is no longer the first time you are learning you have been compromised by these folks. So when you go through your second or third drill of being compromised from Chinese hackers, in general, your security posture gets to a point where you now detect it yourself.

So I think that is just a skew because last year we would have told you over 90 percent, and I have been tracking this since 1998. It has been over 90 percent third-party notification since 1998 for the customers that I have serviced. And this is the first dip, and it is because we are responding for the second or third or fourth time to organizations that have detected it themselves because they have already lived through that first wake-up call from law enforcement.

Chairman WHITEHOUSE. Now, would you describe some of the companies whom you provide services to as operating critical infrastructure in America?

Mr. MANDIA. Yes, I mean, the critical infrastructure demarcation line is harder to find in some industries, but the answer is yes.

Chairman WHITEHOUSE. Do you see any difference among companies that operate critical infrastructure? Are they demonstrably and noticeably better at this? Are they far away from the 90 percent, or are they more or less like any other company?

Mr. MANDIA. It has been my experience that if there is a regulation or a standard imposed, aligned by your industry that your security is, in fact, better in general than organizations that maybe fall through the cracks of all the hodgepodge of standards, legislation, and regulations out there. So if you are in a regulated industry, in general your security is better.

Chairman WHITEHOUSE. So let us talk a little bit about what we can do to increase security for critical infrastructure. Let me ask Ms. McGuire and Mr. Baker. You both have a background at the Department of Homeland Security. It has been the Department of Homeland Security's task for some time to try to develop better defenses in the critical infrastructure sectors. We have also heard I think from both of you that—the word "dynamic" keeps popping up. This is a very dynamic threat. And if we said XYZ strategy or XYZ technology is the mandated defense, then within a week or a month or a year that would be obsolete, and now we would be holding companies back from doing what they needed to do because we would be requiring them to stay with an obsolete technology. That is, if we set the regulatory requirements up in a very stupid and static way.

So what is your recommendation as to how we might go about accomplishing what Mandiant has suggested, which is that standards help and we need to have them and we particularly need them for critical infrastructure, with the same time the dynamic capability that is necessary to meet this evolving threat? Ms. McGuire, then Mr. Baker.

Ms. MCGUIRE. I think the key point here is this is not a simple technology solution issue. You cannot just fix this with technology. It has to be a multi-pronged approach—many of us would use the

term "defense in breadth"—that goes across all areas of a business. And——

Chairman WHITEHOUSE. But, to interrupt, you cannot tell when a company has it and when they do not. So the fact that it is not just a technological solution does not mean that there is not a best practice solution out there, correct?

Ms. MCGUIRE. Absolutely. You have got to have—first and foremost, you have got to have the technology that is properly deployed and up-to-date in order to be your first line of defense. And in most cases, we will catch most of those attack vectors and threats. But to Mr. Mandia's point, we are not going to catch everything. In the face of a sophisticated attacker that is well resourced, that has very deep roots of sponsorship, we will not be able necessarily to address those kinds of APTs and other types of threats.

So what has to happen is really a mesh or a standard risk management approach. You have got to address this through common risk management principles, and that includes the technology, it includes training of personnel, it includes awareness of critical infrastructure owners and operators that this threat is real. I think they are starting to get that now that we are having more high-profile conversations around this with events like Stuxnet in the past as well as the recent Saudi Aramco issue with the bricking of more than 30,000 computer devices, associated with control system devices that operate major pipelines. They are starting to have this awareness about the urgency and the importance of it.

There are a couple of other areas that we also need to address, and that is information sharing, and information sharing is a tool. It is not the be-all, end-all, but it certainly can help with the warning and the preparedness of those critical infrastructure owners and operators. And the common standards question always comes up, and I think again, as you mentioned, they need to be dynamic and flexible enough to allow for the most modern and up-to-date technologies to be implemented. But having the common standards that, for example, are being worked on through the Administration's Executive order right now that hopefully will raise the bar across all industries, I think that will go a long way. It still remains to be seen, but that is a positive step forward.

Chairman WHITEHOUSE. Mr. Baker, same question.

Mr. BAKER. Yes, so not only can we not solve this with technology, the regulation is not the greatest tool here because, as we have seen, the things you should be doing keep changing faster than the regulators can identify the things that need to be done and start imposing sanctions. So if people are not actually willing to pursue security themselves, a pure regulatory solution will not solve the problem.

The good news, I think, is there is a way to think about this——

Chairman WHITEHOUSE. Unless perhaps the regulatory solution measures the pursuit rather than the solution.

Mr. BAKER. That is what I was getting at. You know, when they paint the Golden Gate Bridge, they never stop. They get to the other end, and they go back to where they started and begin painting over again. And that is the security approach that probably is our best. I start with who is attacking me, or who is likely to attack me. What tactics are they using now and likely to use? How

do I stop those tactics? I implement that. And then I say, okay, now that I have implemented those measures, who still wants to attack me and what tools are they going to use now? And I find a solution to that and implement it, and you just—you know, lather, rinse, repeat. That process is probably the only thing you could say for sure we are going to have to require people to do. And measuring that——

Chairman WHITEHOUSE. It strikes me that there is an array of responses among operators of critical infrastructure to this problem. Some of them are very forward in the foxhole. They are throwing everything they can at the problem. And the danger that regulation creates is that you actually interfere with and hold back their efforts. And there is a price to be paid if that is the effect.

At the same time, there are free riders and people who just figure, well, you know, why should I spend the money this quarter when what are the chances if it is really happening now, and, by the way, it is probably such a big catastrophe that the Government is going to come in and save my rear end anyway, and so there are laggards and free riders and cheats on the system, basically. And without a standard, they will continue to be laggards and free riders and cheats. And so there is a significant cost to not having any standard as well.

Where I come down on that is that there needs to be a standard, but it needs to be dynamic, and it needs to measure pursuit rather than any static point.

Mr. BAKER. The one area where I think there has already been a sort of distortion due to regulation and where we should be trying to find a way to use the existing regulatory schemes are some of the data breach notification laws say you do not have to notify if you had encryption. People are spending a lot of their security budget putting encryption on the hard drives of laptops so that if they get lost, they do not have to disclose that they had a breach. That is probably not their biggest threat, but it is the one that hurts the most. And so finding a way to get the FTC and the State Attorneys General to focus more on security as a whole rather than just this one thing is probably useful.

Chairman WHITEHOUSE. Mr. Mandia, any thoughts on the pursuit versus static regulatory problem? You deal with a lot of these companies as well.

Mr. MANDIA. I think when you look at legislation, I think it is a very complicated matter, and I have had these discussions for 15 years on how do you legislate security benchmarks. I think that is very complicated. I think that aligns by industry, and I think the private sector for the most part is doing a lot of that themselves.

I think what I have heard here makes a lot of sense. If you can push for an agile defense mechanism here in the United States that our companies can take threat intelligence being shared with it and have the technology and the means processes to do something with it, I think that is a great next step to cover that security gap.

I think there is already a hodgepodge of standards, legislation, and regulations that are covering the 80 percent of the problem out there, the white noise. But when we want to deal with the nation state, 10 to 20 percent of the problem, I think what needs to be

pushed now is the means for the Government to be able to share intelligence with the private sector, the private sector to get it to the private sector without enormous liabilities in doing so, and just start that information sharing in a codified way where we can make it actionable quicker.

Chairman WHITEHOUSE. But all three of you agree that among the operators of critical infrastructure in this country, you can find companies that are not doing what they should be doing in this area and that are either just not paying the attention that it deserves or have made the economic decision not to invest or are just basically playing the role of the laggard and the free rider and letting other people drive it forward. I see—is that a yes, yes, and yes across the board?

Mr. MANDIA. I have a slightly differing opinion. I can say most of the organizations that we have responded to had breaches that were probably unreasonable to prevent. So we respond to over 30 of the Fortune 100. I do not think they had bad security. I think they were probably all getting a check in the go box for compliance with pretty aggressive standards, yet they were still breached. When it comes to the critical infrastructure, as I sit here today thinking about it, the majority of the organizations we have assisted had security programs that were mature and above compliance, yet they were still breached. But I am giving you an unfair frame of reference because we are responding to the highest end, that 10 to 20 percent of the breaches that are hard to prevent.

Chairman WHITEHOUSE. There are really two problems. One is that even the high performers remain vulnerable to breach by very highly qualified and persistent attackers. And at the same time, there is a considerable set of critical infrastructure operators who make it easy by simply not being up to basic standards.

Mr. MANDIA. Sir, I would just describe in 10 seconds, as if you are a B in security or an F in security, the attackers that Mandiant responds to have the exact same chance of getting in. The only thing that separates the A's in security from the B's is the A's will detect the successful attack themselves, the B's will not. And we are responding to some A's and some B's right now.

Chairman WHITEHOUSE. Back to the point that I have heard many people articulate in this area, and that is that if you are looking at a company, it is in one of two categories: It either has been hacked and knows it, or it has been hacked and does not know it. But that any company of significance has all been hacked, and I think it was also important—Senator Klobuchar and Senator Coons both mentioned the interest in small business. As the attack broadens, small businesses, particularly those that have a specialized process or product or skill that is susceptible of being stolen and then replicated without having to pay license fees and without having to invent it on your own, are becoming more and more the target, particularly if they are in the supply chain to the defense industrial base.

So we get to a point where, if you are a small shop in Rhode Island that is the best place in the world at manufacturing a very specific kind of metals technology, that is what we want you to be doing. We do not want you to have to stop everything and try to bring in best of class cybersecurity in the same way that a

Raytheon or a McDonnell-Douglas or some really major contractor would, and yet they are just as much at risk. I think we all agree.

Well, let me thank all of you. I know you work hard in this area every day and you think in very dynamic ways about this problem, and I look forward to working with all of you as we go forward. I will accept Senator Graham's invitation or suggestion that we try to come up with something on visas, perhaps in the framework of the immigration bill that is now pending. But as I said to the first panel, we are also re-engaging and trying to basically do cyber legislation 2.0 now that the Executive order is in place, and we look forward to talking with all of you about the substance of that legislation and also to having you help us in communicating with our colleagues both the nature and the importance of this problem. So this has been very helpful. I am very grateful to all of you.

The hearing will stay open for a week if anybody wishes to add anything to the record of the hearing. If I have not done it already, then by consent I will add the piece that Lindsey Graham and I wrote into the record of the hearing, and with that, we will stand adjourned.

[Whereupon, at 10:54 a.m., the Subcommittee was adjourned.]

[Additional material submitted for the record follows.]

APPENDIX

ADDITIONAL MATERIAL SUBMITTED FOR THE RECORD

Witness List

Hearing before the
Senate Committee on the Judiciary
Subcommittee on Crime and Terrorism

On

"Cyber Threats: Law Enforcement and Private Sector Responses"

Wednesday, May 8, 2013
Dirksen Senate Office Building, Room 226
9:00 a.m.

Panel I

The Honorable Jenny Durkan
United States Attorney
Western District of Washington
Seattle, WA

Joseph Demarest, Jr.
Assistant Director, Cyber Division
Federal Bureau of Investigation
Washington, DC

Panel II

Kevin Mandia
Chief Executive Officer
Mandiant
Alexandria, VA

Stewart Baker
Partner
Steptoe & Johnson, LLC
Washington, DC

Cheri McGuire
Vice President
Global Government Affairs & Cybersecurity Policy
Symantec Corporation
Washington, DC

PREPARED STATEMENT OF HON. JENNY A. DURKAN

Department of Justice

STATEMENT OF
JENNY A. DURKAN
UNITED STATES ATTORNEY
WESTERN DISTRICT OF WASHINGTON
DEPARTMENT OF JUSTICE

BEFORE THE
SUBCOMMITTEE ON CRIME AND TERRORISM
COMMITTEE ON JUDICIARY
UNITED STATES SENATE

ENTITLED:
"CYBER THREATS: LAW ENFORCEMENT AND PRIVATE SECTOR RESPONSES"

PRESENTED
MAY 8, 2013

Statement of
Jenny A. Durkan
United States Attorney
Western District of Washington
Department of Justice

Before the
Subcommittee on Crime and Terrorism
Committee on Judiciary
United States Senate

At a Hearing Entitled
"Cyber Threats: Law Enforcement and Private Sector Responses"
May 8, 2013

Good afternoon, Chairman Whitehouse, Ranking Member Graham, and Members of the Subcommittee. It is an honor to appear before you to testify about investigating and prosecuting cyber threats to our nation and the resources required to do so. I am pleased to share with the Subcommittee an overview of the Department of Justice's role in the U.S. Government's overall investigative strategy and enforcement efforts as it relates to cyber. The President's 2014 budget also has some funding requests that would enhance our ability to address these threats. I will provide more detail later in my remarks. The Department's approach to 21st Century cyber threats is rooted in three interests: 1) deterring, disrupting, and dismantling the threat; 2) holding bad actors accountable; and 3) protecting our national security, economic interests, and individual privacy.

As United States Attorney, I see the full range of threats our communities and nation face. Few things are as sobering as the daily cyber threat briefing I receive. Cyberspace is the new frontier. We have witnessed the rapid creation of incredible businesses, lifesaving technologies, and new ways to connect society. Unfortunately, the "good guys" are not the only innovators. We have seen a significant growth in the number and nature of bad actors exploiting new technology. As Attorney General Holder has noted, "[f]rom criminal syndicates, to terrorist organizations, to foreign intelligence groups, to disgruntled employees and other malicious intruders, the range of entities that stand ready to execute and exploit cyber attacks has never been greater." Threats to the nation's computer networks and cyber systems continue to evolve, as the nature and capabilities of those responsible for the threats evolve. Over the last several years, investigators and prosecutors have seen significant increases in the skills of threat actors and the complexity of their organizations. These actors have a variety of aims and motivations. For instance:

- Financially motivated groups working closely and easily across national boundaries have stolen large quantities of personal data. These criminals coalesce in forums where they barter individual skills to create ad hoc criminal networks with a power and reach sometimes approaching that of traditional transnational organized crime networks.

- Criminal groups have also developed tools and techniques for disrupting and sometimes damaging computer systems. Motivations run from profit to politics, but their motivations do not change the damage incurred by users and our economy.

- State actors and organized criminal groups have demonstrated the desire and the capability to steal sensitive data, trade secrets, and intellectual property for military and competitive advantage. Whether through remote attacks or insider threats, such thefts pose significant risk to our national security and economic interests.

- Malicious actors are now seeking to exploit the computer networks that control our critical infrastructure.

Responding to these threats requires a multi-faceted approach, including diplomacy and public-private partnerships. The Department, acting with its law enforcement components and in partnership with other agencies, plays a critical role by identifying the offenders, seizing their hardware and assets, and deterring their conduct through, among other things, indictment, arrest, prosecution, and appropriate punishment. In doing so, the Department works closely with other agencies and private sector entities to reduce vulnerabilities. Stated another way, we need to develop better locks, but when those locks are broken—as they inevitably will be—the Department responds to bring the offenders to justice.

Our reliance on technology requires that we take action to protect not only the information infrastructure itself, but the data it carries and activity that it supports. The Administration is committed to integrating and organizing the government's cybersecurity efforts to better ensure that we have a comprehensive framework in place that will allow us to bring all of our collective tools to bear in the fight against cyber criminals, terrorists, and other adversaries. The Department of Justice plays a key role in that fight.

Nature of the Threat

Ten years ago, many of the threats to the burgeoning Internet came from solo hackers, writing viruses like "I love you" or "Melissa," or crafting denial of service attacks on fledgling Internet companies. As bothersome as those attacks were, the threats today are much more significant. We face the challenges of organized crime, botnets (i.e., a collection of compromised computers under the remote command and control of a criminal or foreign adversary), identity theft, and carding, to name just a few. Many of these threats originate overseas.

However, we face significant challenges in attributing the origin of these threats. The tools used to commit serious cyber theft and damage are not only wielded by those with large-scale development resources. Instead, using widely available tools, individuals or small groups can steal huge quantities of sensitive data, damage key computer systems, or silence those who

disagree. Financial gains from these crimes can, in turn, be used to build larger networks and buy protection from foreign government officials. As a result, U.S. investigators working to determine the source and nature of a cyber threat often do not know at the outset whether an attack was mounted by an individual acting alone, an organized criminal or terrorist group, or a hostile nation.

Every day, criminals hunt for our personal and financial data so that they can use it to commit fraud or sell it to other criminals. The technology revolution has facilitated these activities, making available a wide array of new methods that identity thieves can use to access and exploit the personal information of others. Skilled criminal hackers are now able to perpetrate large-scale data breaches that leave hundreds of thousands—and in many cases, tens of millions—of individuals at risk of identity theft. Today's criminals can remotely access the computer systems of universities, merchants, financial institutions, credit card companies, and data processors to steal large volumes of personal information—including financial information. As I explain below, we are working hard to address these threats to personal information.

The most significant threats are continuing to evolve, and now increasingly include threats to corporate data. A 2011 report from McAfee and Science Applications International Corporation confirms this trend in cybercrime. According to this report, which was based on a survey of more than 1,000 senior IT decision makers in several countries, "high-end" cyber criminals have shifted from targeting credit cards and other personal data to the intellectual capital of large corporations. This includes extremely valuable trade secrets and product-planning documents.

These threats come both from outside criminal hackers as well as insiders who gain access to critical information from within companies and government agencies. Trusted insiders pose particular risks. Those inside U.S. corporations and agencies may exploit their access to funnel information to criminals, competitors or foreign nation states. And once the enemy is inside the gates, external defense can only provide limited protection. The Justice Department has successfully prosecuted corporate insiders and others who have obtained trade secrets or technical data from major U.S. companies and routed them to other nations via cyberspace.

The massive proceeds from these online crimes create another troubling issue. It is too soon to say where that money ends up, but the risk that it is being used to influence foreign governments, distort foreign justice systems, and fund terrorists cannot be ignored.

The national security cyber threat picture has similarly undergone a dramatic evolution in recent years. Although we have not yet experienced a devastating cyber attack against our critical infrastructure, we have been victim to a range of cyber activities that have siphoned off our valuable economic assets or had other effects on our infrastructure, threatening our nation's security.

These threats are as varied as the actors who carry them out. While details about most of the state-sponsored intrusions remain classified, the Intelligence Community has publicly noted that "entities within China and Russia are responsible for extensive illicit intrusions into US computer networks and theft of US intellectual property." Indeed, "Chinese actors are,"

according to a 2011 public report of our top counterintelligence officials, "the world's most active and persistent perpetrators of economic espionage." The Secretary of Defense has stated that "Iran has also undertaken a concerted effort to use cyberspace to its advantage."

Likewise, the threat of cyber-enabled terrorism looms large. While terrorists have not yet used the Internet to launch a full-scale cyber attack against the United States, they already use cyberspace for more than merely spreading propaganda and recruiting followers – they have used cyberspace to facilitate operations. The individuals who planned the attempted Times Square bombing in May 2010, for instance, used public web cameras for reconnaissance, file sharing sites to share operational details, and remote conferencing software to communicate. In addition, they have exhorted their followers to engage in cyber attacks on America. Last year, an al-Qaeda video released publicly by the Senate Homeland Security Committee encouraged al-Qaeda followers to engage in "electronic jihad" by carrying out cyber attacks against the West.

The national security cyber threats posed by state-sponsored actors and terrorists are growing, and although to date they have resembled in some ways the crimes perpetrated by financially-motivated criminals, their emergence and evolution make the threat of cyber-generated physical attacks, like those that might disrupt the power grid, appear no longer to be the stuff of science fiction. Leaders in our national security community have predicted that the cyber threat "will pose the number one threat to our country" in "the not too distant future." Accordingly, just as the Department realigned its counterterrorism efforts after 9/11, we are realigning our cyber efforts to meet this challenge.

Addressing these complex threats requires a unified approach, one that incorporates criminal investigative and prosecutorial tools, civil and national security authorities, diplomatic tools, public-private partnerships, and international cooperation. Criminal prosecution, whether in the United States or a partner country, plays a central and critical role in this collaborative effort. While prosecution is not the appropriate approach for every threat that affects the United States, identifying and understanding the threat will very often involve the use of criminal investigative tools and methods.

Role of the Department of Justice

A key part of the nation's overall cybersecurity effort is the investigation and prosecution of cyber criminals – be they financially motivated actors, criminal hackers, terrorists, or state actors. Our goal is to stop or deter these actors before they can complete an attack on our networks, or to punish and deter similar acts in the future if a successful intrusion has already occurred. Many Department of Justice components—including the Criminal and National Security Divisions and United States Attorneys' offices across the country—are actively working to counter these threats.

These cases can be complex to investigate and prosecute. We need to ensure we have the investigative expertise and forensic capabilities needed to meet the challenge. We appreciate the support this committee has given in this regard. Almost every federal case prosecuted now

involves an increasing volume of digital evidence, sometime scattered over numerous devices and multiple online services. For example, in one recent case in our District, the target carried as many as 15 cell phones. Gathering, sifting, and analyzing digital evidence is an increasing challenge. Bad actors know how to hide their cyber tracks: evidence can disappear with a few key strokes, or through malicious code set as a booby trap. Moreover, large cyber cases frequently involve multiple players in multiple states and countries. One significant case can require multiple agents and several years to investigate. Obtaining evidence from foreign countries – even those that are strong allies – can take time, delay, and require translating voluminous foreign language evidence.

To meet these challenges, the Department has organized itself to ensure that we are in a position to aggressively investigate and prosecute cybercrime wherever it occurs. The Criminal Division's Computer Crime and Intellectual Property Section (CCIPS) and a nationwide network of Assistant United States Attorneys (AUSAs), including nearly 300 AUSAs designated as Computer Hacking and Intellectual Property (CHIP) prosecutors lead our efforts to investigate and prosecute cybercrime offenses. These prosecutors, as well as other Assistant United States Attorneys (AUSAs) working cybercrime cases throughout the country, work closely with our law enforcement partners, including the FBI, the Secret Service, and the U.S. Postal Inspection Service. In addition, we have a strong partnership with the FBI's National Cyber Investigative Joint Task Force (NCIJTF), which brings together law enforcement, intelligence, and defense agencies to focus on high-priority cyber threats.

Other sections of the Criminal Division also play important roles in cybersecurity. The Fraud Section focuses on large-scale fraud cases involving identity theft. The Office of International Affairs (OIA) supports and enhances international cooperation efforts by expediting the sharing of critical electronic evidence with foreign law enforcement partners and by marshaling efforts to secure the extradition of international fugitives. Increasingly, large scale cyber cases involve actors from any number of foreign countries. OIA not only secures evidence and international fugitives from abroad, it also plays a central role in cultivating law enforcement cooperation with foreign partners by complying with the United States' reciprocal obligations to provide U.S.-based evidence to foreign authorities for their investigations. International cooperation is critical and the work of OIA a key component of our success.

The Department's National Security Division (NSD) pursues national security cyber threats through a variety of means, including through counterespionage and counterterrorism investigations and prosecutions. The Counterespionage Section (CES) prosecutes, among other offenses, misappropriation of intellectual property to benefit a foreign government, as provided by the Economic Espionage Act of 1996 (18 U.S.C. § 1831), and obtaining national defense, foreign relations, or restricted data by accessing a computer without authorization, as provided by the Computer Fraud and Abuse Act (18 U.S.C. § 1030). The Counterterrorism Section (CTS)—leveraging the capabilities and expertise of CCIPS, the Anti-Terrorism Advisory Council, Joint Terrorism Task Forces, and others—would play a pivotal role in addressing any potential cybersecurity attack by terrorists or associated groups or individuals. NSD also

provides the FBI, and the intelligence community in general, with extensive legal support on cyber issues.

Recognizing the diversity of national security cyber threats and the need for a coordinated approach to them, the Department also established last year a nationwide network of National Security Cyber Specialists (referred to as the "NSCS network"). The network brings together the Department's full range of expertise on national security-related cyber matters, drawing on experts from NSD, the U.S. Attorney's Offices, CCIPS, and other DOJ components. This network seeks to build on the successes of existing initiatives, including the CHIP network and the Anti-Terrorism Advisory Council. Each U.S. Attorney's office around the country has designated a point of contact for the National Security Cyber Specialists network. Last year, approximately 120 Assistant U.S. Attorneys and presenters convened in Washington, D.C. for a cyber training program to kick off the NSCS program.

The NSCS network now serves as a centralized resource for prosecutors and agents around the country. The network has focused the Department nationwide on opening more national security cyber investigations with an eye toward criminal prosecution. Through this network, we are bringing our best resources to bear against the problem—to enhance information sharing, ensure coordination, and leverage the Department's expertise in legal authorities and advice relating to national security cyber threats. Finally, we are using this network to do more outreach to the private sector and to enhance our joint work with the NCIJTF.

In addition to these efforts, the Department works closely with our partners throughout the government—including law enforcement agencies, the Intelligence Community, the Department of Homeland Security (DHS), Department of Commerce, and the Department of Defense—to provide legal support to cybersecurity efforts and inform policy discussions. The intersection between laws and technology can require complicated analysis and multidisciplinary training. That is why the Department has lawyers in US Attorneys offices, and the Criminal and National Security Divisions, who are specially trained to handle cyber issues, ranging from the use of existing legal tools and authorities, the legality of cybersecurity programs like the EINSTEIN program, and the ways in which we can vigorously protect privacy, confidentiality, and civil liberties while still achieving our goal of securing the Nation's networks. Partnering with the National Science Foundation (NSF), through NSF's CyberCorps Scholarship for Service (SFS) program - which seeks to increase the number of qualified students entering the fields of information assurance and computer security and to increase the capacity of the U.S. higher education enterprise to continue to produce professionals in these fields to meet the needs of our increasingly technological society – the Department currently employs more than 40 SFS CyberCorps graduates, including 17 working for the Federal Bureau of Investigation.

For example, the Department is currently providing legal and policy advice to the Department of Homeland Security in support of its cybersecurity mission and to the National Security Agency in support of its information assurance efforts. We are participating in government-wide planning and preparedness efforts, such as the development of the National Cyber Incident Response Plan and the associated Cyber Unified Coordination Group, which assists the Secretary of DHS in coordinating responsive measures to significant cyber incidents. We also participate

in cyber exercises, such as 2012's National Level Exercise, and, along with other governmental partners, in reviewing the national security implications and vulnerabilities of certain foreign acquisitions of U.S. companies, including those with cyber-related capabilities.

Our work does not stop at our shores. Due to the global nature of the Internet, many of our cases involve computers and electronic evidence located in other countries. Many times the offenders are located in another country. Even U.S. criminals will use computers located in another country to hide their tracks. Often it is impossible to identify, arrest, and prosecute offenders without the assistance of foreign governments.

To assist us in preserving and obtaining evidence from other nations, the Department, with funding support from the Department of State Bureau for International Narcotics and Law Enforcement Affairs, has engaged in numerous efforts to enhance the ability of foreign governments to fight cybercrime, including:

- promoting the Council of Europe Convention on Cybercrime (2001);
- providing technical expertise to countries developing their legal frameworks relating to computer crime and electronic evidence;
- providing U.S.-based evidence through mutual legal assistance treaties to aid foreign investigations;
- providing capacity building assistance for foreign law enforcement agencies; and
- promoting the 24/7 High-Tech Crimes Network of the G8, which is a network of points of contact designed to facilitate rapid law enforcement coordination across borders.

The profusion and diversity of cyber threats, and the challenges inherent in identifying and addressing them, highlight the need for a whole-of-government approach—an all-tools approach—to combating cyber threats. As Director Mueller has said, "We must be willing to use whatever legal means are available and appropriate—civil, criminal, or other means—to disrupt a particular threat—whether it be a terrorist threat or a cyber threat."[1] Just as law enforcement and other legal tools have been critical in our efforts to combat organized crime, terrorist threats, and espionage, so too will they be critical to the deterrence and disruption of cyber threats.

Operational Successes

The relationships between the Department's prosecuting components and the federal investigative agencies, such as the U.S. Secret Service and the Federal Bureau of Investigation, and the robust cooperation and information sharing that they support, have led to a number of

[1]Address at RSA Cyber Security Conference, San Francisco, CA (February 28, 2013) http://www.fbi.gov/news/speeches/working-together-to-defeat-cyber-threats.

enforcement successes. In FY 2012, computer intrusion investigations resulted in 138 convictions and pre-trial diversions. I would like to highlight a few here.

International, Multi-state Carding Ring – In my District, we prosecuted participants at all levels of an international credit card skimming ring from a Secret Service investigation. Christopher A. Schroebel, 21, of Keedysville, Maryland, obtained credit card information by hacking into vulnerable point of sale computers in small business operations across the country, including one in the Seattle area. Tens of thousands of people were victimized, and the investigation indicated that over 100,000 credit cards were compromised. David Benjamin Schrooten, 22, a Dutch citizen living in Romania sold the card numbers for a profit by advertising them on "carding websites." Charles Tony Williamson, 33, of Torrance, California, has also been charged with buying the card numbers for his criminal group to use in multiple frauds. Schroebel was sentenced to seven years in prison, Schrooten received a twelve year sentence, and Williamson is awaiting trial.

Prolific Identity Thief and Hacker Sentenced. Following a complex Secret Service investigation, on July 18, 2012, a court in the Eastern District of New York sentenced Aleksandr Suvorov to seven years in prison following his 2009 plea to conspiracy to commit wire fraud and his 2011 plea to trafficking in unauthorized access devices. Suvorov, an Estonian, was extradited from Germany in 2009. Along with Albert Gonzalez and Maksym Yastremskiy, he participated in a massive hacking scheme involving retail merchants. The May 2009 pleas, for example, involved a hack into the Dave & Buster's restaurant chain in which the group stole names and account numbers for approximately 110,000 credit card accounts. Gonzalez, arguably the most prolific identity thief in American history, had already pled guilty and was sentenced in March 2010 to 20 years in prison. Yastremskiy earlier received a 30-year prison term in Turkey for identity theft and related crimes.

Coreflood Botnet Takedown. In April 2011, the government filed a civil complaint against 13 "John Doe" defendants, alleging that they ran the Coreflood Botnet in order to engage in wire fraud, bank fraud, and illegal interception of electronic communications. At its peak, the group had control over several million computers infected with the Coreflood malware. Search warrants were obtained for computer servers throughout the country, and a seizure warrant was obtained for 29 domain names. The government also obtained a temporary restraining order (later followed by a preliminary and permanent injunction), authorizing the government to respond to signals sent from infected computers in the U.S. in order to stop the Coreflood software from running, thereby preventing further harm to hundreds of thousands of unsuspecting users of infected computers in the United States. Over the next month, the Coreflood Botnet was effectively eliminated.

Charges Brought Against Six Leaders of Anonymous and Related Criminal Hacking Collectives. In March 2012, the Southern District of New York (SDNY) unsealed charges against five criminal computer hackers in the United States and abroad

who identified themselves as aligned with the online group "Anonymous" and/or related offshoot groups including "Internet Feds," "LulzSec," and "AntiSec." SDNY unsealed one indictment that charged Ryan Ackroyd, aka "kayla"; Jake Davis, aka "topiary,"; Darren Martyn, aka "pwnsauce,"; and Donncha O'Cearrbhail, aka "palladium," with computer hacking conspiracy involving the hacks of Fox Broadcasting Company, Sony Pictures Entertainment, and the Public Broadcasting Service (PBS), among others. In addition, SDNY unsealed the guilty plea of Hector Xavier Monsegur, aka "Sabu," the former head of Anonymous and LulzSec who had been cooperating with the FBI since his arrest in the Southern District of New York in June 2011. Monsegur pleaded guilty not only to charges in SDNY, but also to substantive hacking charges filed by four other U.S. Attorney's Offices -- Eastern District of California (hacks of HBGary, Inc. and HBGary Federal LLC), Central District of California (hacks of Sony Pictures Entertainment and Fox Broadcasting Company) , Northern District of Georgia (hack of Infraguard Members Alliance), and Eastern District of Virginia (hack of PBS). Finally, the FBI arrested Jeremy Hammond, aka "Anarchaos," who identified himself as a member of "AntiSec," on a complaint in SDNY that charged him in connection with the hack of Stratfor, a global intelligence firm based in Austin, Texas.

Notorious Criminal Hacker and Identity Thief Surrendered by France to the U.S. On April 5, 2013, Vladislav Anatolievich Horohorin, a/k/a "BadB" was sentenced to 88 months in prison by Judge Huvelle in the District Court for the District of Columbia. Horohorin, a citizen of Russia, Ukraine, and Israel, was a major vendor of stolen credit and debit cards who possessed more than 2.5 million stolen account numbers at the time of his arrest. Horohorin also participated in the intrusion at Atlanta-based RBS Worldpay in 2008, in which an international criminal group that completed more than 15,000 fraudulent transactions at over 2,100 ATMs in at least 280 cities worldwide in a 12-hour period in November 2008, causing more than $9.4 million in losses. Horohorin was extradited to the United States from France, where he was arrested on August 8, 2010 at the request of U.S. authorities.

Romanian "Point-of-Sales" Criminal Hackers Extradited to U.S. Following an extensive Secret Service investigation, on May 4, 2011, a federal grand jury in Concord, New Hampshire, returned an indictment charging Adrian-Tiberiu Oprea, Cezar Iulian Butu, Iulian Dolan, and Florin Radu, all residents of Romania, with conspiracy to commit computer intrusions, wire fraud, and access device fraud. The defendants were part of a group that, beginning in 2008, remotely hacked into Subways' and other merchants' "checkout" or "point-of-sales" computer systems; surreptitiously installed "keystroke logging" software, which in turn recorded and stored customers' credit, debit, and gift card data; electronically transferred the stolen card data to several U.S.-based computer servers ("dump sites") and from there to a server in Cyprus, for temporary storage; and then made unauthorized charges on the compromised accounts and sold stolen card data to other co-conspirators. Members of the conspiracy have compromised over 146,000 accounts and have made unauthorized charges in excess of $10,000,000 on these compromised accounts. Dolan and Butu, were arrested upon their entry to the United

States in August 2011, have pled guilty, and remain in United States custody awaiting sentencing. Adrian-Tiberiu Oprea, 28, of Constanta, Romania, was extradited from Romania to the United States and appeared in federal court in New Hampshire on May 29, 2012. Radu is currently at large.

Operator of Worldwide Spam Botnet Convicted. On February 27, 2013, Oleg Nikolaenko, 25, a citizen of Russia who entered the United States on a tourist visa, was sentenced to time served (just over 27 months) in the Eastern District of Wisconsin following an earlier guilty plea. According to court documents, Nikolaenko operated and controlled the Mega-D botnet, which was at one time the world's largest spam botnet, accounting for approximately 32% of all spam worldwide. A network security company estimates that approximately 509,000 computers worldwide were infected with Mega-D botnet malware.

Operation Trident Tribunal Takes Down International Crime Rings Distributing Scareware. Operation Trident Tribunal is a coordinated international enforcement action targeting a cybercrime ring that caused over $71 million in losses to more than one million computer users by operating a "scareware" scheme. Scareware is malicious software that cybercriminals plant on victim computers through a variety of computer exploits including the use of botnets, "drive-by" downloads, and criminal search engine manipulation. The scheme uses a variety of ruses, including web pages featuring fake computer scans, to trick consumers into purchasing fake anti-virus software products at a cost of up to $129. In June 2011, DOJ coordinated the efforts of law enforcement in over a dozen countries to seize dozens of servers that were being used to orchestrate this scheme. Two Latvian nationals, four Ukrainian nationals, and a Swedish national were indicted in connection with the scheme, and five foreign bank accounts were frozen.

On January 19, 2012, defendant Mikael Patrick Sallnert, a citizen of Sweden, was arrested in Denmark and extradited to the United States. Sallnert was a trusted payments processor for the scareware ring, responsible for processing funds fraudulently obtained from U.S. victims. Sallnert pleaded guilty to one count of conspiracy to commit wire fraud and one count of accessing a protected computer in furtherance of fraud on August 17, 2012, and was sentenced to 48 months in prison on December 14, 2012 by Judge Pechman in the Western District of Washington.

These cases illustrate the broad scope of the Department's efforts to pursue cyber criminals. While the Department is proud of these cases and all of our efforts to tackle the growing and evolving cybersecurity problem, we recognize that there is much more to be done, and we will continue to work with our law enforcement and private sector partners to meet that challenge. Because of the global nature of the Internet and the related crimes it can facilitate, continued close coordination and cooperation with foreign law enforcement is critical to our collective success. And because our prosecutors understand the severe damage that computer crimes can have upon a victim, we continue to pursue appropriate cases, both large and small.

Legislation to Enhance the Department's Ability to Combat Cyber Threats

As the threat increases and evolves, so must our legal tools to combat the threat. In May 2011, as part of the Administration's Cybersecurity Proposal, the Department proposed some needed, moderate updates to the computer crime laws.2 We continue to believe that many of these proposals would enhance our ability to combat cyber threats, including:

- A proposal to update the Racketeering Influenced and Corrupt Organizations Act ("RICO") to make the Computer Fraud and Abuse Act ("CFAA") offenses subject to RICO. The CFAA is the primary statute used to prosecute hacking crimes. Computer technology has become a key tool of organized crime. Indeed, criminal organizations are operating today around the world to: hack into public and private computer systems, including systems key to national security and defense; hijack computers for the purpose of stealing identity and financial information; extort lawful businesses with threats to disrupt computers; and commit a range of other cybercrimes. Many of these criminal organizations are similarly tied to traditional Asian and Eastern European organized crime organizations.

- A proposal to clarify and update the forfeiture provision of the CFAA. This proposal would allow for civil forfeiture and clarify the rules governing criminal forfeiture under the statute.

- A proposal to update the CFAA's sentencing provisions. The goal of these changes is to eliminate overly complex, confusing provisions; simplify the sentencing scheme; and enhance penalties in certain areas where the statutory maximums no longer reflect the severity of these crimes.

Resources to Enhance the Department's Ability to Combat Cyber Threats

Because of the very serious nature of cyber threats, and the pressing need to respond to them, the Administration is asking for an enhancement to the Department's budget to target this critical problem. These additional resources will help us to keep pace with the increased numbers and ever evolving sophistication of our adversaries. The Department's FY 2014 Budget proposal therefore provides a total of $668 million in cyber resources to address computer intrusions and cybercrimes and to defend the security of the Department's critical information networks. This request includes an increase of $92.6 million for the FBI, NSD, and the Criminal Division.

For the FBI, the budget includes an increase of $86.6 million and 152 positions (60 agents) to support the FBI's Next Generation Cyber Initiative, which will more strategically focus the FBI's efforts on the greatest cyber threat—intrusions into government and industry computer networks. The Next Generation Cyber Initiative combines national security and criminal

---

[2] *See* http://www.whitehouse.gov/sites/default/files/omb/legislative/letters/law-enforcement-provisions-related-to-computer-security.pdf.

investigative resources to more holistically approach multi-dimensional cybercrimes and to better leverage the full range of FBI authorities. The requested funding will add 50 special agents and 50 computer scientists to increase cyber investigative capabilities and victim notification, enhance the capabilities and expertise of FBI investigative personnel, and improve the collection and analysis of electronic evidence. It will also extend centralized analytical capabilities to the field by deploying cyber workstations to serve as portals for communicating intrusion-related data bureau-wide.

Like the FBI, the Department's National Security Division seeks to improve its capability to respond to cyber-based threats to the national security and the capability to respond. Cyber-based threats to the national security are, according to the intelligence community "increasing in scope and scale," and cyber-espionage in particular "is almost certainly allowing our adversaries to close the technological gap between our respective militaries, slowly neutralizing one of our key advantages in the international arena." NSD is involved in the full range of U.S. cyber and cyber security efforts, including cyber threat prevention, detection, disruption, investigation and prosecution, as well as oversight, vulnerability management, and cyber policy development. As I mentioned above, last year NSD created the National Security Cyber Specialists Network to facilitate a threat-based approach, rather than a statute- or tool-based approach, to the national security cyber challenge. To this end, NSD is establishing "threat focus" cells of cyber specialists to focus on particular high-priority cyber targets. The subject-matter experts who comprise such teams will serve as Departmental focal points for information about—and strategies designed to defeat—these identified cyber threats. One such cell has already been created, and has successfully begun work on a significant threat actor.

As NSD positions itself to better accomplish its cyber mission, and as it continues its work leading, expanding, and developing the NSCS Network, our first priority is ensuring that we have a well-equipped cyber workforce. To achieve this goal, NSD must hire, equip, and train both new and existing personnel. These additional resources are critical to ensuring that the Division's redoubled cyber efforts do not detract from ongoing, and critical, counterterrorism, counterespionage, and intelligence-related matters. As a result, NSD has requested $3.5 million and 26 positions (16 attorneys) for FY14. This increase will enable NSD to strengthen its investigative, prosecutorial, intelligence collection, and oversight abilities to support the Intelligence Community in identifying and disrupting cyber threats to national security.

Similarly, the Criminal Division has seen a growth in cyber threats perpetrated by actors other than foreign nation states and terrorist organizations. And as I mentioned before, criminal prosecution, whether in the United States or a partner country, plays a central and critical role in eliminating these threats. In addition, while prosecution is not the appropriate approach for every threat that affects the United States, identifying and understanding the threat will very often involve the use of criminal investigative tools and methods. Just as the threats to our nation's invaluable proprietary and personal information are increasing, so must our innovation and our efforts to deter, disrupt, and prosecute those threat actors. Studies have shown that the number of intrusions continues to increase, and the cost of cybercrime to American businesses and citizens likewise continues to mount. The Division's Computer Crime and Intellectual

Property Section (CCIPS) has experienced a 42% increase in pending investigations and an 11% increase in pending prosecutions between FY 2010 and FY 2011. The requested additional resources will help the Division keep pace with the growing cyber caseload and should be viewed in tandem with the increase in FBI investigative resources for FY 2014.

A reality of cyber investigations is that it is nearly impossible to forecast where they will begin or end. Consequently, the Division, through CCIPS, provides nation-wide support to investigations, prosecutions, and disruption efforts, helping to ensure that its law enforcement partners receive consistent, quality support whether the investigation's trail leads to Silicon Valley, rural America, or overseas. As a result, Criminal Division prosecutors have led, or partnered in, some of the country's most significant data breach and computer intrusion cases, the success of which has required a comprehensive grasp of computer network technology and electronic evidence law and a subtle understanding of the often loosely organized worldwide groups that work together to plan and execute these attacks.

CCIPS prosecutors work in direct cooperation with the CHIP network and investigative agencies to identify and address threat actors. CCIPS houses prosecutors with a deep understanding of data breaches and computer misuse cases and prosecutors who understand the complexity of intellectual property cases to comprise a leading resource for deterring, investigating, and punishing the theft of sensitive electronic information. Consequently, every additional prosecutor in CCIPS becomes a force multiplier for the Department, leveraging its expertise wherever it is needed to the benefit of all USAOs and the achievement of the Department's cyber crime goals.

The Criminal Division is therefore requesting an increase of 25 positions (9 attorneys), 14 FTE, and $2,580,000. This enhancement will increase the Division's capability in four key areas: cybercrime investigations and prosecutions; advice to the field regarding legal tools and authorities; international cooperation and outreach; and forensic support. This increased capacity will allow the Division to successfully deter, investigate, and punish the theft of sensitive electronic information and other cybercrime.

Moreover, a critical part of the Department's efforts to combat cyber threats is international engagement. As I have just described, criminals residing outside of our borders are a major component of the overall threat, and even criminals inside the U.S. commonly use computers overseas to store their tools, hide stolen data, and conceal their identities. Thus, a critical part of addressing the cyber threat is to improve our ability to work with law enforcement agencies in foreign governments to collect electronic evidence on our behalf and arrest and either extradite or prosecute cyber criminals.

The Criminal Division has long had a robust program for encouraging the development by foreign governments of laws, investigation and prosecution capacity, and appropriate infrastructure to address emerging cybercrime threats and capabilities. From the development and maintenance of a 24/7 response capability in more than 50 countries aimed at preserving critical evidence before it is deleted, to its leading role in negotiating the first multilateral convention on cybercrime, to its regular engagement on training, policy, and operational issues

with law enforcement partners around the world, the Division and its partners in the US Attorneys offices have led the fight against transnational cybercrime.

Despite significant advances in law enforcement cooperation and understanding, criminals continue to use gaps and inefficiencies in international law enforcement capabilities to evade detection, attribution, and punishment. Foreign authorities apply data protection regulations in ways that can frustrate investigations. Delays in evidence collection can stop investigations almost at their inception. And some of the myriad entities involved in providing Internet connectivity and domain registration have permitted the growth of "data havens" where criminal and other threat actors can commit crimes with relative impunity.

Despite these challenges, the Criminal Division has attempted to perform effective international outreach on cyber issues. Using a balanced approach of frank policy discussions with countries that have similar capabilities, combined with multilateral training initiatives aimed at countries whose legal or technical infrastructure to address cyber threats is at an earlier developmental stage, the Division has continued to improve capacity to address cybercrime around the world. CCIPS attorneys lead efforts to build capacity and law enforcement relationships in Africa, Eastern Europe, and Latin America, including through multi-lateral organizations such as the Organization of American States and the Asia-Pacific Economic Cooperation. As computer infrastructures expand in developing countries, and offenders who victimize Americans inevitably follow, the need for this sort of international engagement continues to grow.

Having prosecutors stationed in foreign hotspots will contribute immeasurably to these efforts. Consequently, the Criminal Division also requests an enhancement of 11 positions (including 7 attorneys), 6 FTE, and $3,500,000 to place four DOJ Attachés overseas. These DOJ Attachés will serve as regional International Computer Hacking and Intellectual Property coordinators (ICHIPs). This program will build on the existing Intellectual Property Law Enforcement Coordinator Program (IPLEC) that has proven to be very effective in enhancing the Department's goals in fighting international intellectual property crime. Since 2006, the IPLEC Program has deployed experienced federal prosecutors overseas to take the lead on our intellectual property protection efforts in key regions including Asia and, until March 2011 (when State Department funding expired), Eastern Europe. Through the IPLEC program, the Department has seen a substantial increase in foreign enforcement and cooperative casework where U.S. law enforcement has had a visible and ongoing presence in the most active countries or regions. This enhancement request would allow for the expansion of the program to additional critical regions.

* * *

The Department of Justice stands ready to work with the Committee as it examines these important issues. We appreciate the opportunity to testify today, and we look forward to continuing to work with you.

This concludes my remarks. I would be pleased to answer your questions.

PREPARED STATEMENT OF JOSEPH M. DEMAREST, JR.

Department of Justice

STATEMENT OF
JOSEPH M. DEMAREST, JR.
ASSISTANT DIRECTOR
CYBER DIVISION
FEDERAL BUREAU OF INVESTIGATION

BEFORE THE
SUBCOMMITTEE ON CRIME AND TERRORISM
COMMITTEE ON JUDICIARY
UNITED STATES SENATE

ENTITLED:
"CYBER THREATS: LAW ENFORCEMENT AND PRIVATE SECTOR RESPONSES"

PRESENTED
MAY 8, 2013

Statement of
Joseph M. Demarest, Jr.
Assistant Director
Cyber Division
Federal Bureau of Investigation

Before the
Subcommittee on Crime and Terrorism
Committee on the Judiciary
United States Senate

At a Hearing entitled
"Law Enforcement and Private Sector Responses"

May 8, 2013

Chairman Whitehouse, Senator Graham, and distinguished members of the Committee, I am pleased to appear before you today to discuss the cyber threat, how the FBI has responded to it, and how we are marshaling our resources and strengthening our partnerships to more effectively combat the increasingly sophisticated adversaries we face in cyberspace.

The Cyber Threat

The 21st century brings with it entirely new challenges, in which criminal and national security threats strike from afar through computer networks, with potentially devastating consequences. These intrusions into our corporate networks, personal computers, and government systems are occurring every single day by the thousands. Such attacks pose an urgent threat to the nation's security and economy. The threat has reached the point that given enough time, motivation, and funding, a determined adversary will likely be able to penetrate any system accessible from the Internet.

We see four primary malicious actors in the cyber world: foreign intelligence services, terrorist groups, organized criminal enterprises, and hacktivists.

Dozens of countries have sophisticated cyber espionage capabilities, and these foreign cyber spies have become increasingly adept at exploiting weaknesses in our computer networks. Once inside, they can exfiltrate government and military secrets, as well as valuable intellectual property—information that can improve the competitive advantage of state-owned entities and foreign companies.

Terrorist groups would like nothing better than to digitally sabotage our power grid or water supply. Although most such groups currently lack the capability to conduct sabotage operations over the Internet themselves, the tools and expertise to perpetrate a cyber attack with physical effects are readily available for purchase or hire.

Organized criminal groups, meanwhile, are increasingly migrating their traditional criminal activity from the physical world to the online world. They no longer need guns to rob a bank; they use a computer to breach corporate and financial institution networks to steal credentials, account numbers, and personal information they can use to make money.

These criminal syndicates, often made up of individuals living in disparate places around the world, have stolen billions of dollars from the financial services sector and its customers. Their crimes increase the cost of doing business, put companies at a competitive disadvantage, and create a significant drain on our economy.

Hacktivist groups are pioneering their own forms of digital anarchy, posing novel cybersecurity threats by repeatedly, illegally accessing computers or networks for a variety of reasons including politically or socially motivated goals.

With these diverse actors, we face significant challenges in our efforts to address and investigate cyber threats. While the FBI has already made great strides in developing its capability to address the cyber threat, we are currently prioritizing our immediate and long-term areas for strategic development in order to best position ourselves for the future.

FBI Response

The FBI recognized the significance of the cyber threat more than a decade ago and created the Cyber Division in 2002 to combat cyber-based terrorism, hostile foreign intelligence operations conducted over the Internet, and cyber crime, by applying the highest level of technical capability and investigative expertise. Since then, the FBI elevated the cyber threat to its number three national priority – after only counterterrorism and counterintelligence – and significantly increased the hiring of technically trained agents, analysts, and forensic specialists.

The FBI has also seen the value of its trusted partnerships and worked tirelessly to support and improve them. Securing our networks demands cooperation, and cyber vulnerabilities are magnified when you consider the ever-connected, interdependent ecosystem of the cyber world.

To that end, we have expanded our partnerships with law enforcement, private industry, and academia, through initiatives like InfraGard—a public-private coalition of 55,000 members to protect critical infrastructure—and the National Cyber-Forensics and Training Alliance, a proven model for sharing private sector intelligence in collaboration with law enforcement.

The FBI has made significant progress in recent years. Ten years ago, if you were an agent conducting a cyber investigation and the Internet Protocol (IP) address tracked back to a foreign country, that was effectively the end of your investigation.

Since then, the FBI has placed cyber specialists in key European locations to effectively facilitate the investigation of cyber crimes affecting the United States. This, along with improvements in our ability to track IP addresses back to their source, has led to a recognition in the underground economy that there are fewer safe hiding places around the globe. Building on the success of our

international outreach, we are currently expanding our Cyber Assistant Legal Attaché program to additional countries.

A prime example of how our investigations have progressed in the 10 years since the Cyber Division was created is the 2011 takedown of Rove Digital, a company founded by a ring of Estonian and Russian hackers to commit a massive Internet fraud scheme.

The scheme infected more than four million computers in more than 100 countries with malware. The malware secretly altered the settings on infected computers, enabling the hackers to digitally hijack Internet searches using rogue servers for Domain Name System (DNS) routers and re-routing computers to certain websites and ads. The company received fees each time these web sites or ads were clicked on or viewed by users. This scheme generated $14 million in illegitimate income for the operators of Rove Digital.

Because Estonia has improved its domestic laws, we were able to work with our law enforcement counterparts and our private industry partners to execute a takedown of this criminal organization. Following the arrest of several co-conspirators in Estonia, teams of FBI agents, linguists, and forensic examiners assisted Estonian authorities in retrieving and analyzing data that linked the co-conspirators to the Internet fraud scheme. At the same time, we obtained a court order in the United States to replace the rogue DNS servers with specified clean servers.

In this case, we not only took down the criminal organization, but worked with our partners in DHS and other agencies to mitigate the damage. Seven individuals have been indicted in the Southern District of New York in this case: six were located in Estonia and one was in Russia. The United States has sought extradition of all six Estonian subjects. To date, two of them have been remanded to U.S. custody. One pleaded guilty on February 1, 2013.

We are also employing novel ways of combating the threat. In Operation Coreflood, the FBI worked with our private sector and law enforcement partners to disable a botnet that infected an estimated two million computers with malicious software.

The malware on this Coreflood botnet allowed infected computers to be controlled remotely by criminals to steal private personal and financial information from unsuspecting users. In an unprecedented move, the FBI obtained a court order to seize domain names, re-route the botnet to FBI-controlled servers, and respond to commands sent from infected computers in the United States, telling the zombies to stop the Coreflood software from running. The success of this innovative operation will help pave the way for future cyber mitigation efforts and the development of new "outside the box" techniques.

While we're pleased to report on our progress against the threat, we recognize that we must be pro-active in order to respond more rapidly and prevent attacks.

Next Generation Cyber

The need to prevent attacks is a key reason we have redoubled our efforts to strengthen our cyber capabilities while protecting privacy, confidentiality, and civil liberties. The FBI's Next

Generation Cyber Initiative, which we launched in 2012, is an FBI-wide initiative to enhance our ability to address the full range of cybersecurity threats to the nation. In just the last year, this initiative has enhanced the FBI's ability to collect, coordinate, integrate, share, and act on information related to cyber intrusion investigations at headquarters, throughout its 56 domestic field offices, and with its partners overseas.

Implementation of this initiative is focused in four areas: strengthening the National Cyber Investigative Joint Task Force (NCIJTF); expanding the Cyber Task Forces focused on intrusions in each of our 56 Field Offices; advancing the capability of the cyber workforce and supporting enterprise infrastructure; and enhancing information sharing and operational collaboration with the private sector.

A key part of the intergovernmental effort is the FBI-operated National Cyber Investigative Joint Task Force (NCIJTF), which serves as the deconfliction center on cyber investigations among 19 federal agencies. The FBI aims to strengthen and solidify the NCIJTF as the cybersecurity center for coordinating cyber threat investigations and disruption options. In the last year, the NCIJTF has made significant progress in developing its supporting capabilities and operational coordination, as well as expanding its interagency leadership. The NCIJTF now involves senior personnel from key agencies, including Deputy Directors from the National Security Agency, the Department of Homeland Security, the Central Intelligence Agency, the U.S. Secret Service, and U.S. Cyber Command.

In the future, the FBI must continue to strengthen the NCIJTF, which will include expediting analysis of interagency holdings and perfecting the coordination model on incident response and threat disruption operations.

Another critical element of the FBI's success is the restructuring and expansions of the FBI's network of field office Cyber Task Forces (CTFs), which emulate the successful Joint Terrorism Task Force (JTTF) model, such that each office has a robust multi-disciplinary, cross-program, and multi-agency domestic ground team to conduct cyber threat investigations and respond to significant cyber incidents.

In just the last year, the FBI has formally established a CTF in each field office, staffed by cyber-specialized agents, analysts, and other agency participants. The CTF is now established as a national brand, under which all field office efforts addressing cyber intrusion matters are addressed. The FBI offers a robust curriculum of FBI-developed and industry certification courses to its CTF members. In the future, each CTF will continue to grow its capabilities, leveraging nationally developed systems and investigative efforts. The FBI will also increase the participation of state and local law enforcement officers and expand the cadre of agents, analysts, and computer scientists on each CTF to ensure a high baseline capability.

The FBI is committed to advancing the capability of its cyber workforce and the supporting enterprise infrastructure. We have leveraged and developed our human capital by establishing core cyber competencies and further supported the workforce by extending enterprise capabilities. The FBI established its High-Technology Environment Training (HiTET) initiative to enhance the technical proficiency of Special Agents, Intelligence Analysts, Professional Staff,

and Task Force Officers (TFOs) who are directly involved in operations. HiTET training consists of numerous web-based courses, case studies and/or practical demonstrations, job-aids, legal fact sheets, technology articles and other related reference materials. HiTET training is developed in bundles to provide context and applicability to law enforcement and domestic intelligence missions requiring technical skills.

The current results of this effort are increased efficiencies and improved information analysis. Since the roll-out of the Next Generation Cyber initiative, the FBI has expanded visibility into the source of cyber threat activities and dramatically increased its cyber intelligence reporting. While we have seen success, the threat continues to grow and advance; in the future, the FBI must continue to expand the capability of its cyber workforce and its supporting technical infrastructure.

Last but not least, the FBI is working to strengthen both local and national information sharing and collaboration to support success in network defense, intelligence operations, and disruption operations. The private sector is an essential partner if we are to succeed in defeating the cyber threat. A critical piece of the relationship with private industry and individuals is assisting them in protecting themselves and their systems from the threat posed by terrorists, nation-states, and criminal groups conducting computer network operations against the U.S. To support this, the FBI has created an organizational unit focused on leveraging FBI operational information and intelligence to provide victims of cyber attacks more timely and valuable information regarding cyber attacks targeting them.

To maximize our efficiency, we adopted and enhanced the successful Counterterrorism Division Guardian terrorist threat tracking and collaboration system called eGuardian and enhanced it to accept cyber incidents from the fusion centers and state and local law enforcement. Further, we are deploying a platform called iGuardian to enable trusted private industry partners to also report cyber incidents in a secure and efficient manner to the FBI, and we are leveraging intelligence from the NCIJTF to effectively identify and notify cyber attack victims. We coordinate these efforts closely with the cybersecurity centers and our cybersecurity partners.

Conclusion

In conclusion, Mr. Chairman, in order to counter the growing cyber threats, we are focusing our resources, expanding our presence both at the local and national levels, and engaging in an unprecedented level of intergovernmental collaboration and cooperation with the private sector.

As the Committee knows, we face significant challenges in our efforts to combat cyber crime. We are optimistic that by identifying and prioritizing strategic areas for change, the FBI will continue to succeed in identifying and neutralizing cyber criminals, thereby protecting U.S. businesses and critical infrastructure from harm.

We look forward to working with the Committee and Congress as a whole to determine a successful course forward to ensure our defense. Thank you again for the opportunity to appear before you today. I would be happy to answer any questions you may have.

PREPARED STATEMENT OF KEVIN MANDIA

WRITTEN TESTIMONY OF

KEVIN MANDIA
CHIEF EXECUTIVE OFFICER
MANDIANT CORPORATION

BEFORE THE

SUBCOMMITTEE ON CRIME AND TERRORISM
JUDICIARY COMMITTEE
UNITED STATES SENATE

May 8, 2013

Introduction

Thank you Mr. Chairman, Ranking Member Graham, and Members of the Subcommittee, for this opportunity to share my observations and experience with you. As requested I am going to discuss three things: 1) the nature of the cyber threats facing American businesses; 2) the measures being taken by organizations to counter these threats; and 3) what law enforcement can do to help organizations protect themselves and their corporate secrets.

Today, and into the foreseeable future, American companies will face a motivated, technically sophisticated, and well-resourced adversary intent on depriving businesses of their wealth and intellectual property. While many organizations are actively trying to counter these threats, there currently exists a sizeable gap between what their safeguards can prevent and the ability of motivated attackers to circumvent those safeguards.

Narrowing this security gap is where law enforcement can best assist American businesses. The FBI and other agencies can provide an early warning system, informing businesses when they have been compromised by these motivated adversaries. Law enforcement and other agencies can also share actionable intelligence about cyber-threats that can help companies prevent or detect compromises on their own. While these actions cannot stop each and every cyber security breach, they are essential to suppressing the impact and consequences of the security breaches that will occur.

Background

Following several years as a Computer Security Specialist and an agent in the Air Force Office of Special Investigations, I founded Mandiant in 2004 to offer private sector companies the ability to respond effectively to emerging cyber threats. In addition to running Mandiant, I have had the honor of training FBI agents in cybersecurity investigations in an ongoing capacity for nearly 15 years. As I testify here today, Mandiant employees are on the front lines of the cyber battle, responding to active computer intrusions at dozens of the largest American companies and other organizations important to our nation, including attacks at the *New York Times* and the *Washington Post*.

Mandiant has responded to incidents at hundreds of companies. We have investigated millions of systems, and we receive calls almost every single day from companies that have suffered a cyber-security breach. These cyber intrusions continue to impact virtually every industry, including law firms, financial services, blue chip American manufacturers, retailers, the defense industrial base, telecommunications, space and satellite and imagery, cryptography and communications, government, mining, software and many others. I have witnessed the unique

threats facing each of these sectors, and continue to help companies respond to these advanced cyber threats.

What are the Threats?

Cybersecurity professionals are aware that criminals and government operators are using the Internet to compromise American businesses. These intruders are able to steal both wealth and the means of generating wealth by exfiltrating the intellectual property and strategic business information that will drive commerce into the future. As General Keith Alexander noted last year, the loss of information and intellectual property through cybercrime and espionage constitutes the "greatest transfer of wealth in history."

In accessing these networks, our adversaries have the ability not to just steal our wealth, ideas and information, but they could also have a physical impact on our lives. Deleting valuable information, manipulating industrial control systems or introducing false data into a system could result in death or the destruction of property felt far beyond the loss of a bank account, patent application or corporate secrets.

Through my experience in combating cyber threats, I have seen firsthand the methods attackers use as they seek to undermine and exploit our nation's infrastructure. Simply put, these sophisticated threats have evolved faster than our ability or willingness to reliably safeguard our assets.

Most American organizations can secure their networks from "consumer-grade" threats by adhering to industry standards and best practices. From a technical perspective, these attacks are conducted using exploits and techniques that are relatively well known and preventable. These attacks are usually not advanced enough to exploit the gap in our security.

Today, I focus instead on the advanced threats that we are not preventing or detecting. It is reasonable to assume that, if an advanced attacker targets your company, a breach is inevitable. That surprises many people, but it is the undeniable truth, and a direct result of the gap between our ability to defend ourselves and our adversaries' ability to circumvent those defenses. There are at least six reasons why attackers continue to successfully exploit this gap in security:

First, the sophisticated, cutting-edge attacks that were previously reserved solely for government targets have spread to the private sector. Advanced threat actors have shifted the application of their sophisticated tools, tactics and procedures from U.S. government targets to corporate America. Many American companies, even if they are compliant with cyber-security regulations and best practices, are not prepared for these advanced threats.

An example of an advanced threat actor targeting American businesses is a group Mandiant refers to as APT1. Mandiant has identified APT1 as Unit 61398, or the 2nd Bureau of China's People's Liberation Army General Staff Department's 3rd Department. Unit 61398 has targeted thousands of English speaking businesses from various sectors of the economy around the world -- the majority right here in the United States.

The second reason attackers are able to successful exploit the security gap is that they are targeting people, not computer systems. While previous generations of attacks targeted technology and exploited vulnerabilities in software, attackers have now evolved to target human inadequacies and weaknesses. As Americans increasingly rely on the Internet, invest more in their online identities and continue to pour their personal details into online blogs and sites such as Facebook, Google+, LinkedIn and Twitter, attackers are able to target their attacks at individuals using the detailed, personal information they themselves make available. These personalized attacks are difficult to detect and prevent because they exploit two things that are difficult to secure: human vulnerabilities and human trust.

Mandiant documented this tactic in its recent report on APT1. In that report, Mandiant demonstrated that APT1's operatives were recruited for their proficiency in English in order to target English-speaking personnel at target companies. APT1 initiate attacks by researching specific individuals online in order to send a seemingly legitimate email, but the fake or spoofed email would contain malware embedded in attachment that appeared innocuous. When opened, the attachment launches the malware that creates a foothold for APT1 operatives to leverage access to the entire network.

Third, more attacks are coming from the "inside." Advanced attackers consistently leverage the pre-existing infrastructure of compromised networks in the United States to target and attack new companies. We frequently see attackers compromise smaller companies with fewer security resources, and then "upgrade" their access from those trusted, smaller companies to the main target. This is also a problem where large businesses "acquire" the infected networks through a corporate merger or acquisition of these smaller enterprises.

The fourth reason attacks continue to be successful involves the imbalanced nature of cyber-attacks and the number of defenders in the U.S. A single attacker can generate work for hundreds, if not thousands of defenders. Also, while a single attacker need only breach his target's defenses once to accomplish his goals, the victim company's entire cyber security staff must attempt to prevent 100% of the threats. This imbalance is compounded by the critical shortage of skilled security professionals here in the U.S.

Fifth, many advanced attackers reside in nations that not only refuse to hold attackers accountable for their crimes, but provide resources and direction to the attackers. As long as state-sponsored criminals can infiltrate American networks and steal American intellectual property without risks or repercussions, these attacks will continue unabated. As if to prove that point, APT1 continues to operate even after being exposed in Mandiant's recent report.

Finally, one of the most valuable resources in detecting and responding to cyber-attacks – accurate and timely threat information – is often unavailable to many defenders. The U.S. needs an effective framework for sharing information among commercial entities, and between corporate America and the government. Too often attackers are finding success using resources and methods that are known by some, but have not been shared with potential victims because of a lack of authority and mechanisms to accomplish the communication.

What are Organizations Doing about the Threat?

As a result of the above six factors, corporate America continues to be routinely compromised by the advanced adversaries. Although it sounds dramatic, it is generally true that there are two sorts of businesses: those that know they have been compromised, and those that have been compromised but just do not know it yet.

Most of those organizations that are aware of the threats are taking the challenge seriously. They are buying technologies that are effective against the consumer-grade threats, especially if appropriately configured and operated by trained and conscientious professionals. The majority of the products available today, however, are less effective against the more sophisticated threats, and are significantly less effective if not operated by professionals trained to identify and appropriately scope the inevitable breaches.

Many organizations that do not yet understand the threat facing businesses today still attempt to implement some level of security through a compliance program. Though having compliance standards that align industry efforts provides important guidance, it often results in organizations concluding that compliance is "good enough," or that their efforts will eliminate the security gap. That is simply not the case.

Companies that are the most effective in dealing with advanced threat actors are those that employ appropriate technology correctly, and bolster that technology with skilled experts trained in identifying network compromises, tracking the adversary, and containing their activity.

What can the FBI do to Assist?

It is the law enforcement's job to protect Americans, be they individuals, businesses or government agencies. The FBI already conducts outreach to American companies who have been compromised by advanced threat groups. Indeed, about two-thirds of the breaches Mandiant responds to are first detected by a third party – usually the FBI or another law enforcement agency – not the victim companies. That means that a majority of the companies we assist had no idea they had been compromised until law enforcement or a business partner notified them.

The significance of that number cannot be overstated. With virtually every other crime, the victim is the first to know that they have been violated. Here, however, we have the government in the unique position of informing victims that they are, in fact, victims. Actionable information, if shared quickly and consistently, could be used to prevent or mitigate the impact of these breaches instead of merely notifying victims long after their intellectual property has been stolen.

Speed is critical to the effective mitigation of a compromise by an advanced threat actor. Once a foothold has been established, the infiltrator must conduct network reconnaissance in order to either upgrade his credentials or find data valuable enough to steal. This reconnaissance takes time, and, if appropriate action is taken during this time, the adversary can be thwarted with minimal impact to the victim. Increased speed of notification to victims provides them a chance at mitigation as opposed to just evaluating the impact of the compromise and the value lost to the adversary. Although we cannot eliminate every security breach, speed allows us to suppress the impact and consequences of the breach.

The FBI is uniquely positioned to be an early warning system for compromised organizations. Due to its tremendous top-down visibility into domestic networks, the FBI could increase the scale and speed at which it notifies victim companies. While speed of notification is critical, any additional actionable information shared with the victim makes containing the adversary faster and easier. A simple dossier including observed IP addresses and tactics used by the adversary allows the victim to quickly observe and orient on the malicious activity and appropriately contain the damage. Machine-readable intelligence, in a format such as Mandiant's OpenIOC, would be even more actionable.

The sharing of actionable threat information will narrow the security gap facing businesses today. Government, including law enforcement, and some companies have this actionable intelligence. We need to create a way in which they can share this information in a standard, codified, machine-readable way that does not betray or diminish the effectiveness of our national security or law enforcement missions, or significantly impact our privacy and civil rights. If we

do it right, sharing threat information will promote an aggressive, dynamic "learning system" of cyber-security for the nation. Effective information sharing:

1 – Acts as an early warning system giving potential victims advance notice of significant threats;
2 – Promotes technologies that facilitate the effective use of threat information;
3 – Empowers the private sector to defend itself more effectively; and
4 – Significantly reduces the duration and impact of breaches, should they occur.

The private sector cannot do this alone. While many industry players have extremely capable security programs, the majority of threat information is currently in the hands of the government.

Conclusion

While private industry will not always win the battles being fought in cyberspace, we can drastically narrow the security gap by sharing actionable intelligence and enabling law enforcement to act as an early warning system. By establishing a system where law enforcement and the private sector share and proactively use accurate and timely threat information, America will build a dynamic cyber-defense system that grows smarter and more capable by the day.

Thank you very much, Mr. Chairman.

PREPARED STATEMENT OF STEWART A. BAKER

The Attribution Revolution:
Raising the Costs for Hackers and Their Customers

Statement of Stewart A. Baker

Partner, Steptoe & Johnson LLP

Before the Judiciary Committee's Subcommittee on Crime and Terrorism
United States Senate

May 8, 2013

Mr. Chairman, Ranking Member Graham, members of the subcommittee, it is an honor to testify before you on such a vitally important topic. I have been concerned with cybersecurity for two decades, both in my private practice and in my public service career, as general counsel to the National Security Agency and to the Robb-Silberman commission that assessed U.S. intelligence capabilities on weapons of mass destruction, and, more recently, as assistant secretary for policy at the Department of Homeland Security. In those two decades, hacking of computer networks has evolved from occasionally annoying pranks into a full-fledged counterintelligence crisis.

Today, network insecurity is not just an intelligence or law enforcement concern. It could easily cause the United States to lose its next serious military confrontation.

I have been broadly supportive of recent efforts to improve the security of our networks, and I still am. But let's not kid ourselves. Today, even our most secure systems are being compromised. Security professionals don't expect to keep hackers out of their networks; all they can hope to do is – perhaps – isolate and protect some really sensitive data. And, to tell the truth, after multiple demonstrations that hackers can reach completely isolated networks, no one is offering any guarantees that they can do that, either.

Our network security, in short, is toast. We've been living in a dream world, thinking that if we could just fix all the security holes that hackers have been exploiting, then our networks would at last be secure. But if that dream were ever achievable, it looks hopeless today. The resources that hackers are putting into finding holes are growing steadily, as the modest risks and great rewards of exploiting networks continues to attract everyone from nation states to organized crime.

In short, we can't defend our way out of this fix, any more than we could solve the problem of street crime by firing our police and making pedestrians buy better body armor every year.

The ineffectiveness of our current strategy is clear. As it is, the great majority of companies that get hacked only discover the intrusion when they are told by a third party, like the FBI. And by the time companies learn of the intrusion, on average, the bad guys have been in their computers for months if not years. We need to find another paradigm for improving our security.

Attribution 101

That is why I will focus my remarks today on what is shaping up to be an "attribution revolution." The theory is simple. The same human flaws that have left our networks ever more exposed to attack are undermining our attackers' anonymity. This is what I like to call Baker's Law: "Our security may be toast. But so is theirs."

As numerous recent reports show, attackers are only human. They make mistakes when they're in a hurry or overconfident. They leave bits of code behind on abandoned command-and-control computers. They reuse passwords and email addresses and computers. Their remote access tools are full of vulnerabilities. These are openings that private researchers – from Mandiant and Trend Micro to SecDev and the Citizen Lab – have exploited; they've traced cyberattacks to the command and control computers used to carry them out, then to homes and offices of the hackers that perpetrate them. These reports have identified individuals and institutions closely associated with hacking US companies and agencies. They've found the universities where the hackers trained. They've found the hackers' names and instant message addresses . Using these clues, researchers have even tracked the hackers down and called them up for comment. They've found the companies that employ the hackers today. In at least one case, hacking victims in the Republic of Georgia have turned the tables and used their attackers' malware to take an attacker's picture with his own desktop camera.

The attribution revolution has truly begun.

From Attribution to Deterrence

But attribution is only half of the formula if we want to deter cyberespionage. The other half is retribution. Once we identify our attackers, we need to persuade them to choose another line of work.

That does not necessarily mean that we should rely exclusively or even primarily on the Department of Justice or the Federal Bureau of Investigation. We must look beyond traditional criminal prosecutions to deter cyberespionage. Once we do, we will find plenty of tools at our disposal:

1. Expose and Isolate Nations

Naming and shaming is a commonly used method of deterring bad conduct by other nations. The U.S. may be reticent about releasing hard-won intelligence about the activities of foreign governments. But some of the most explosive – and convincing – recent allegations against foreign governments have in fact been made by private entities. The report released earlier this year by Mandiant offered extensive evidence of the People's Liberation Army's role in hacking into U.S. companies over a number of years. The report placed an embarrassing spotlight on state sponsored hacking in China and sparked bitter but vague denials from the Chinese government.

Of course, it's not clear that embarrassment alone will stop countries like China or Iran or North Korea from supporting cyberattacks against our companies and our government. But it's a start. It raises the cost of what has been a relatively low-risk, asymmetric strategy. It strips them of a sense that they are protected by a veil of ambiguity about the origin of attacks on our networks. And it sets the stage for further action in the future.

2. Sanctions for Spies – And Their Enablers

The Justice Department and the FBI may not be able to reach hackers located on the other side of the world. And even if we could catch them, we might not want to risk compromising intelligence sources and methods by taking them to court. But that does not mean we cannot punish them. We already use classified information to identify terrorist supporters and drug kingpins as "specially designated nationals" and to impose sanctions on them – seizing their bank accounts and assets, for example, and prohibiting U.S. citizens from doing business with them. We even have such programs for sanctioning Belarusian kleptocrats and those who traffic in conflict diamonds. Maybe it makes sense for the American government to use sanctions to punish misdeeds in Belarus or West Africa, but it surely makes a lot more sense to use these measures to punish people who are invading homes and offices across the United States?

To tell the truth, I don't know why the President hasn't done this already. He's got all the authority he needs to impose sanctions on cyberspies and their enablers. Under the International Emergency Economic Powers Act, the President could determine that cyberspying poses "an unusual and extraordinary threat" to the United States and declare a "national emergency." He could then publish a list of hackers who would be subject to sanctions. In keeping with past practice, he could rely heavily on classified data to make the designations – without disclosing any of it.

3. Visas

One of the things that Mandiant disclosed was how much some of our adversaries hate their jobs. They found a blog maintained by one notorious hacker, and all he could talk about was his dream of making a "prison break" from his 9-to-5 job stealing secrets.

Maybe we should help him out. The Justice Department is authorized to issue a couple of hundred "S" visas each year to foreign nationals "in possession of critical reliable information concerning a criminal organization or enterprise." The visa allows family members to enter as well, and it becomes a permanent residency if the witness's "information has substantially contributed to the success of an authorized criminal investigation."

Systematically hacking US companies and agencies surely constitutes a criminal enterprise under US law, and I note that an investigation can apparently be deemed a success without leading to a criminal conviction. If a witness's cooperation helps us to thwart other countries' cyberspying campaigns, that surely counts as a success.

On the flip side, the U.S. government also has the power to deny visas and other perks to entities that act as enablers to hackers.

For example, late last year Trend Micro released a report that unmasked "Luckycat," a Chinese hacker who had attacked the Dalai Lama, aerospace firms, and other targets. His real name, according to the report, was Gu Kaiyuan, formerly a student at Sichuan University's Information Security Institute and at least at the time an employee at a major Chinese Internet company, Tencent.

Now we can't reach Mr. Gu in China, but why haven't the officials investigating those intrusions gone to his employer and his alma mater and asked them to cooperate in the investigation? Unlike Mr. Gu, these institutions benefit mightily from good relations with the United States government. Sooner or later, every Chinese university wants its students and faculty to get visas to work and study in the United States. And every Chinese company that does business here is subject to our investigative authority. They have many reasons to cooperate, particularly to rebut any evidence that they condoned or enabled cyberspying. At a minimum, taking a hard look at these institutions will make them think twice before they support or turn a blind eye to hackers in their midst.

4. Criminal and Civil Suits for Final Customers

But punishing individual hackers is only part of the story. What if we applied all of these measures not just to the hackers themselves but to companies that benefit from the data they filch from U.S. networks? There's not much difference in criminal responsibility between a thief and the guy he's stealing for. But there could be all the difference in the world between hackers who do their work from the safe environs of a protective government agency and the hackers' customers, who can't be truly successful in today's world if they aren't part of the global marketplace. And going global means exposing their companies, executives, and assets to the legal systems of the United States, Europe, and a host of other countries that are pretty much sick of wholesale espionage aimed at their companies. If a few big companies find that having a cozy relationship with their government's hackers means criminal prosecutions and asset seizures, they're a lot more likely to say "Thanks, but no thanks" to offers of stolen data.

Of course, to bring those cases, we'll have to have those companies dead to rights, and so far we don't. US security researchers have done a great job of tracking the thieves back home. But they've had trouble identifying the companies who ultimately benefit from cyberspying.

That too is an attribution problem – the next one we have to solve if we want to really discourage commercial cyberespionage. It will be difficult, but no harder than the first attribution problem looked five years ago. Nailing the customers for stolen data is going to take a major intelligence campaign, but in the end I think we can identify with certainty both the cyberspies and their spymasters.

What Role for Private Companies?

This brings me, finally, to the role that private companies should play. I'll be blunt. We can't rely exclusively on the Federal Bureau of Investigation. Sure, when combined with our intelligence assets, the FBI has resources and authorities that exceed those of any single

company. But in aggregate, it's the private sector that is spending the most to counter cyberspies. When the FBI discovers that a company has been compromised, it tells the victim, but it rarely offers technical advice about how to identify or thwart the attacker. Instead, the victim hires a company like Mandiant to deal with the attack. These private investigators know their adversary. They can often tell who the attackers are by the tools and tactics they use. They can often gain access to the command and control machine used for the exploit, where they find the clues that help them confirm their attribution of the attack. This is all information gathered by private investigators. To be frank, it is information that the FBI would never gather on its own. The Bureau doesn't have the manpower and it doesn't have the technical capacity to investigate all of these intrusions in such detail. And, given the current budget climate, it never will. Only in the private sector are we likely to see a continued rise in expenditures to fight network attacks and cyberespionage.

So, if we want to take full advantage of the attribution revolution, we can't simply leave this to the Bureau and the prosecutors. We need better ways to draw on the resources of the private sector and their investigators.

Right now, however, the Justice Department is doing more to hurt than to help companies that want to respond aggressively to the theft of their secrets and their intellectual property.

Let me give you one example. Suppose that a private investigator finds that data is being exfiltrated from his client to a particular command and control server. If the server is in the United States, the investigator may be able to persuade the owner, who is probably himself a hacking victim, to grant access to the server. This happens a lot, and it has great value, especially for attribution. The investigator may be able to identify the attackers and even recapture some of the stolen data.

But what if the hackers get wise and move the server to another location that they actually own? Can the investigator follow them to that other server and use what he knows about the gang's passwords to get access to the evidence and the stolen data stored there?

Not according the United States Department of Justice, which has begun actively and publicly discouraging any investigations that do not rely on the consent of the network owner, even when the network owner is the hacker himself. Recently, an anonymous Justice Department spokesman told Bloomberg BNA that intruding on an attacker's network would be both bad policy and "likely a violation" of the Computer Fraud and Abuse Act.

This is unfortunate in so many ways that I can understand why the spokesman insisted on anonymity.

Remember that the FBI is not itself gathering such information from foreign command and control servers – or doing much else to stop individual attacks. And, as we've seen, the FBI simply can't be expected to keep up with the current wave of attacks. Companies suffering massive cyberespionage losses are getting about as much attention as an Adams-Morgan resident whose bicycle has been stolen from the lamppost outside his home.

So when it says that private investigations into other networks are "likely a violation" of federal law, the Justice Department is really saying, "We may not be able to protect you from hackers, but we sure can stop you from protecting yourself."

This view has particularly hampered efforts to track attackers back to their headquarters. In many cases, private investigators know exactly where those headquarters are located and have a pretty good idea what passwords would get them into the network. But those networks are certainly owned by their attackers, and the prospect of being prosecuted means that only the bravest and most outraged victim is likely to take the risk of following his attackers home – and even if he did, it isn't clear what he could do with the evidence he gathered, since the Justice Department might decide he's easier to indict than the hacker

The problem is a lack of imagination–in particular, a belief that the only choices are wise, temperate, and ineffectual rule by government prosecutors on the one hand and a pitchfork-wielding mob of vigilantes on the other.

But in the real world, we have many more choices than that. If someone stops making payments on a car loan but keeps the car, the lender doesn't call the police. He hires a repo man. In the real world, if your child is kidnapped and the police aren't making the investigation enough of a priority, you hire a private investigator. And, if I remember correctly the westerns I watched growing up, if a gang robs the town bank and the sheriff finds himself outnumbered, he deputizes a posse of citizens to help him track the robbers down.

That's where we are now. Things a lot more valuable than a car have been stolen; the police aren't able to help; they barely have the resources to protect themselves; and they're definitely outnumbered.

Private investigators and deputized citizens and repo men aren't the same as vigilantes or a lynch mob. They are institutions that allow the victim of a crime to supplement law enforcement – while also providing social control and oversight of the victim's actions. The time has come to experiment with the same kind of institutions for cybercrime. The Justice Department and the Bureau should be required to let responsible private investigators work as adjuncts to government and to use carefully supervised portions of government authority as they gather evidence to identify hackers.

If we can do that much, we will go a long way toward gathering the attribution evidence we need to truly deter these attacks. This is not simply speculation. A recent cybersecurity report from two Luxembourg entities, a private computer incident response team and iTrust Consulting illustrates the potential for such an approach. The researchers that prepared this report, led by Paul Rascagnères, were able to break into and map the command and control infrastructure of a notorious Chinese hacking unit. In fact, he did to them what they have been doing to us – breaking in, logging the attackers' keystrokes and stealing their passwords, and then while they were searching for the intruder on their network, packing up their tools and stolen data and exfiltrating everything out from under their noses.

That kind of thing shouldn't be done without government oversight. And it cannot be done without the help of security professionals working for the victim. It's time to find a new way forward.

A Strategy For Exploiting the Attribution Revolution

Government agencies do many things well, but finding a new policy direction isn't usually one of them. This committee can play a valuable role in making clear that the government needs a new strategy for the cybersecurity crisis.

Some of the recommendations I made earlier could be incorporated into a new strategy. For example, Congress could adopt legislation imposing sanctions on foreign hackers and their customers. Congress has done this on numerous occasions to punish human rights violations abroad, as with the recent Magnitsky Act. Why not impose sanctions this time on those who have violated the human rights of Americans right here in the United States?

Similarly, Congress could supplement the "S" visa to make it more effective in combating cyberespionage. This could include increasing the number of "S" visas or allowing agencies other than the Justice Department to issue such visas. Congress could also authorize DHS and the State Department to deny visas to institutions that enable hacking activities.

Finally, Congress can do more to enable retribution against large companies that benefit from information stolen by hackers. At the outset, this should include providing sufficient authorities, resources, and encouragement to the Intelligence Community so it has the capacity to track down stolen data. Congress may also wish to consider laws that make it easier for victims to sue these companies, for example by encouraging them to piggyback on successful prosecutions.

Conclusion: Our Best Hope is a Change in Strategy

In closing, let me return to my main theme. We face a crisis. Cybersecurity is bad and getting worse. Civilian lives, our economic future, and our ability to win the next war, depend on solving our security problems. We need to find ways to turn the tables on hackers by putting the pressure on them and the entities that sponsor and enable them. To do this, we need to shift to a more active defense posture—one that relies on attribution and retribution.

In my view, this shift would be best achieved if we find ways to allow victims to use their own resources, under government oversight, to identify the people who are stealing their secrets and the institutions that are benefiting from the theft.

The first step in the shift is to acknowledge how bad things are, and how seriously our current institutions have failed. The next step is to chart a new course.

The good news is that we have taken the first step.

The next step is up to you.

PREPARED STATEMENT OF CHERI F. MCGUIRE

Prepared Testimony and
Statement for the Record of

Cheri F. McGuire
Vice President, Global Government Affairs & Cybersecurity Policy
Symantec Corporation

Hearing on

"Cyber Threats: Law Enforcement and Private Sector Responses"

Before the

United States Senate
Committee on the Judiciary
Subcommittee on Crime and Terrorism

May 8, 2013

226 Dirksen Senate Office Building

Chairman Whitehouse, Ranking Member Graham, and distinguished members of the Subcommittee, thank you for the opportunity to testify today on behalf of Symantec Corporation.

My name is Cheri McGuire and I am the Vice President for Global Government Affairs and Cybersecurity Policy at Symantec. I am responsible for Symantec's global public policy agenda, including cybersecurity, data integrity, critical infrastructure protection (CIP), and privacy. In this capacity, I work extensively with industry and government organizations, including serving from 2010 to 2012 as Chair of the Information Technology Sector Coordinating Council (IT SCC) – one of 16 critical sectors identified by the President and the US Department of Homeland Security (DHS) to partner with the government on CIP and cybersecurity. I also serve as a board member of the Information Technology Industry Council, the TechAmerica Commercial Policy Board, and the US Information Technology Office (USITO) in China, and am a past board member of the IT Information Sharing and Analysis Center (IT-ISAC). Previously, I served in numerous positions at DHS, including as Acting Director and Deputy Director of the National Cyber Security Division and US Computer Emergency Readiness Team (US-CERT).

Symantec is the largest security software company in the world, with over 31 years of experience in developing Internet security technology. We provide security, storage and systems management solutions to help consumers and organizations secure and manage their information and identities. Our Global Intelligence Network (GIN) is comprised of more than 69 million attack sensors in over 200 countries, and records thousands of events per second. In addition, every day we process more than three billion e-mail messages and more than 1.4 billion web requests across our 14 global data centers.

These resources allow us to capture worldwide security intelligence data that gives our analysts a view of the entire Internet threat landscape, including emerging cyber attack trends, malicious code activity, phishing and spam. We welcome the opportunity to provide comments as the Subommittee continues its important efforts to bolster the state of cybersecurity in the US and abroad. In my testimony today, I will provide the Subcommittee with:

- our latest analysis of the threat landscape as detailed in the just-released Symantec Internet Security Threat Report (ISTR), Volume 18;
- a summary of our cooperative engagements with law enforcement, both domestically and abroad; and
- some thoughts on how you can bolster the law enforcement community's important work in this area.

Today's Threat Landscape

We rely on technology for virtually every aspect of our lives, from driving to and from work, to mobile banking, to securing our most critical systems. As the use of technology increases so do the volume and sophistication of the threats. Criminals are constantly looking to exploit new vulnerabilities to steal money, intellectual property, and identities. At Symantec, it is our goal to ensure that we are thinking ahead of the attackers. Looking at the current threat landscape is not enough – we must also keep our eyes on the horizon for evolving trends and attack patterns.

In the latest Symantec ISTR, we identified the current trends in cybercrime and detailed how we see the landscape changing in 2013. Last year, we saw a significant increase in targeted attacks – up 42 percent

from 2011,[1] and it is almost certain that this trend will continue in the coming years. Large scale data breaches continued to be an issue, and last year approximately 93 million identities were exposed through hacking, theft, and simple error. That is 93 million people whose personal information is now potentially for sale on the black market – 93 million people who are at risk for credit card fraud, identity theft, and other illegal schemes.

Another trend in 2012 was the expansion of what we refer to as "watering hole attacks" – efforts by attackers to compromise legitimate websites so that every visitor to those websites runs the risk of infection. Criminals target sites that they believe their victims will frequent, and are often quite sophisticated in evading detection. In some cases, they insert malicious code onto the site only at key times of the day to evade security scans.

Once the criminals take over sites, they often use them to distribute so-called "ransomware," a type of malicious software that locks a user's computer and displays a screen purporting to be from a law enforcement agency. In the US, ransomware typically puts up a fake Federal Bureau of Investigation (FBI) notice that (1) informs the user that illegal content was found on his or her computer, and (2) offers to provide a code to unlock it if the user pays a "fine." *See* Figure 1. Unfortunately, payment of the "fine" usually does not unlock the computer.

Fig. 1 – Actual image used by common "Ransomware" to extort money from a victim. Note that in an effort to frighten the victim as much as possible, the ransomware accuses the victim of crimes involving child pornography and child abuse.

[1] *Symantec Internet Security Threat Report* XVIII, April 2013. http://www.symantec.com/security_response/publications/threatreport.jsp

Networks of compromised, zombie computers that are controlled by criminal enterprises – also known as "botnets" – continue to be a problem. Botnets range in size from just dozens to millions. A computer becomes a "bot" when an attacker surreptitiously installs malware on the system that allows the criminal to remotely control it. Bots can be used to send spam, to try to infect other computers, or as pawns in massive denial of service attacks. We estimate that there were 3.4 million bot zombies in 2012, up from 3.1 million in 2011. Last year, one in seven (or 15 percent) of global bot-infected computers resided in the US.

We also saw a sharp rise in the threats to mobile devices. Last year, mobile malware increased by 58 percent, and 32 percent of all mobile threats attempted to steal personal information, such as e-mail addresses and phone numbers. Attacks on mobile devices will almost certainly continue to rise as we become ever more reliant on these devices to perform our daily activities, including working, banking, shopping, and social networking.

Another alarming finding was the rise of attacks on small and medium size businesses. In 2012, 50 percent of all targeted attacks were aimed at businesses with fewer than 2,500 employees, and the largest growth area for targeted attacks was aimed at businesses with fewer than 250 employees. Thirty-one percent of all attacks targeted them, up from 18 percent the year before. This likely stems from the fact that unlike large enterprises, smaller businesses often do not have the resources to establish adequate security protocols, making them an easier target for attackers. Yet many of these small companies subcontract or work for larger companies – and thus hold intellectual property and trade secrets coveted by attackers. As one of our security engineers likes to say, while every subcontractor may sign a strict non-disclosure agreement, the attacker who is sitting on that small company's system is not bound by it.

In sum, whether they are attacking our computers, mobile phones or social networks, cyber-criminals are looking to profit by spying on us or stealing our information. Our best defense is strong security, education and awareness, and good computer hygiene.

Engagement with Law Enforcement

At Symantec, we partner with all levels of government, both here in the US and abroad. When requested, we work with law enforcement through traditional means, such as responding to subpoenas and warrants. In addition, we share high-level cybercrime and cyber threat trends and information on a voluntary basis through a number of different fora to help protect our customers and their networks. Of course, all of this work is done in keeping with both our strict privacy policies, and all applicable national and international privacy laws.

Symantec has a long and successful history of participation and leadership in various industry organizations, as well as public-private partnerships in the US and globally. Among these are the National Cyber-Forensics & Training Alliance (NCFTA), InfraGard, and INTERPOL. Effective sharing of actionable information among the public and private sectors on cyber threats, vulnerabilities, and incidents is an essential component of improving cybersecurity and combatting cybercrime.

The NCFTA is a good example of how private industry and law enforcement partnerships can yield real world success. The NCTFA is a Pittsburgh-based organization that includes more than 80 industry partners – from financial services and telecommunications to manufacturing and others – working with federal and international partners to provide real-time cyber threat intelligence to an actionable level in order to identify threats and actors, and provide intelligence to domestic and international law

enforcement to neutralize those threats. Through this partnership, hundreds of criminal investigations have been launched, which otherwise would not have been addressed, with successful prosecutions of more than 300 cyber criminals worldwide. In further support of these initiatives, the NCFTA has produced more than 400 cyber threat intelligence reports over the past three years alone. Through the NCFTA, Symantec is able to share crucial cyber threat information across a wide-ranging group of private industry and law enforcement entities at home and abroad.

InfraGard, of which Symantec serves on the National Board of Advisors, is another example of how law enforcement can partner with both private industry and individuals to share information on cyber threats. This successful partnership between the FBI and members of the private sector is focused on intrusions and vulnerabilities affecting 16 critical infrastructures. Comprised of a coalition of more than 55,000 private and public sector members, InfraGard promotes ongoing dialogue and timely communication between its members and the FBI. InfraGard members gain access to threat information that enables them to better protect their cyber and physical assets, as well as an avenue to share information with the government to help prevent terrorism and other crimes.

Cyberspace is a domain without borders, where crimes are often committed at a great distance. In effect, every computer in the US is a potential border entry point, making investigation and prosecution of cybercrimes a difficult task. This reality makes international engagement on cybersecurity essential. For this reason, Symantec works to maintain effective relationships and open communication lines with international law enforcement entities including INTERPOL, EUROPOL and individual national police forces, by making them aware of the latest technological trends, the evolution of the threat landscape and identifying some of the techniques that cybercriminals use to attack our customers. We also participated last fall in the first ever Industry Expert Meeting with the G8 High-Tech Crime Subgroup. The meeting was comprised of representatives of law enforcement, justice departments, and other governmental bodies of the G8 countries and private industry.

Unfortunately, both here in the US and around the world, there is a critical shortage of investigators, prosecutors, and judges who are adequately trained to handle complex cybercrime cases.

Recognizing this need, Symantec established the Norton Cybersecurity Institute (NCI) two years ago to help provide law enforcement with the skills to level the playing field with cybercriminals. Through the NCI, we have a number of initiatives whereby we work with law enforcement organizations and non-profit safety groups to provide training and technical expertise, and to help facilitate global cooperation. For example, through our partnership with the National Center for Justice and the Rule of Law (NCRLJ) and the US National Association of Attorneys General, Symantec has aided in training prosecutors in trying cybercrime cases as well as judges who adjudicate those cases.

This training can – and should – start when young lawyers are still in school. In March 2013, we sponsored a successful cyber moot court competition at UCLA School of Law. The competition helped the students develop their legal skills and introduced them to many of the difficult legal concepts surrounding cybercrime. Eleven law schools sent teams to compete – but more needs to be done.

It is important to remember that cybercrime is not victimless, and we do what we can to help the victims of cybercrime. We have partnered with the National White Collar Crime Center (NWC3) to develop an online assistance program that helps cybercrime victims better understand the investigation process and help prevent future attacks. We also make tools available to the public – for example, we offer free software that allows victims of ransomware and botnets to clean their systems.

Internationally, Symantec partners with various non-profit organizations, including the Canada-based Society for the Policing of Cyberspace (POLCYB), to provide training workshops to law enforcement officials and policymakers around the globe. Later this month, through our partnership with POLCYB, we are supporting a cybercrime workshop in Kiev, Ukraine to train law enforcement officials in the region. This is just one of several trainings offered annually to enhance public-private collaboration to identify and address gaps in cybercrime investigations and prosecutions. To date, we have partnered with POLCYB to train law enforcement officials and policy makers in more than 35 countries around the world.

Industry to industry partnerships also work. One example is the model that helped to bring down the Bamital botnet, a major takedown that happened earlier this year. This effort was the culmination of a multi-year investigation, in partnership with Microsoft and law enforcement, to dismantle the botnet. The Bamital botnet had taken over millions of computers for criminal activities such as identity theft and click fraud, threatening the $12.7 billion online advertising industry. This successful takedown demonstrates what can be done when private industry and law enforcement join forces to go after cybercriminal networks.

Current and Future Law Enforcement Efforts

Investigating and prosecuting cybercrime poses no less a challenge than does defending against cyber attacks. It is technically challenging, and requires a level of expertise and training that many police agencies and prosecutors are 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 often count on it.

In the face of these obstacles, the amount of progress that has been made is impressive. Not too long ago, numerous cultural and organizational barriers prevented federal agencies from coordinating on the investigation and prosecution of international cyber criminals. Those barriers have come down, and today we see that kind of cross-agency coordination on a regular basis. John Boles, the Deputy Assistant Director of the FBI's Cyber Division, had it right when he told a House Subcommittee this past March that federal agencies "are coordinating at an unprecedented level."

The disruption of an Estonian cyber gang using the "DNSChanger" malware is an excellent example of the kind of real-world results that can come from this coordination. Dubbed "Operation Ghost Click," the criminals surreptitiously installed malware that changed the settings on a computer that control how it routes to websites, essentially hijacking a victim's searches and directing web browsers to ads that generated revenue for the criminals from phantom "clicks." The malware also prevented the victims from finding resources that might alert them to the infection. Working with the Estonian authorities, in 2011 the FBI arrested six members of the gang and shut down their operations.

But the effort did not stop with the arrests. Because simply shutting down the criminals' command servers would have effectively disconnected millions of unknowing victims from the Internet, the FBI worked with the DHS, the Courts, and the private sector to put in place infrastructure so that victims could still access the Internet safely and clean their machines of the infection. This type of effort was unprecedented: not only was a major criminal ring interrupted, but the government worked across agency lines and with the private sector to minimize the impact on the victims.

Operation Coreflood is another example of how effective legal tools can be when they are employed creatively. Coreflood was a piece of malware that infected and took over as many as two million

computers, creating a massive botnet. In this case, the FBI worked with private sector partners and obtained a court order that allowed them to commandeer the command and control servers, identify the infected computers, and send a command to each of them telling the malware to shut down.

Unfortunately, these examples highlight just how much still needs to be done. For while Ghost Click and Coreflood were successes for law enforcement, there are undoubtedly more – and larger – criminal rings operating today. This should not be taken as a criticism, however; the relative dearth of cases like these is not because the government does not want to pursue them, or because the criminals are not out there. The investigators and prosecutors are willing, and the private sector is eager to help. But unfortunately, cybercrime cases require a highly technical understanding of how computers and the Internet work. They are also time intensive – the Ghost Click investigation took more than two years, and the effort to disinfect affected computers took almost another year. There are simply not enough investigators, prosecutors, or judges who can handle them well, and the FBI, the Secret Service, and state and local law enforcement agencies need more personnel dedicated to fighting cybercrime.

And while the Courts proved helpful in those two cases, there is no doubt that law governing cybercrime needs to be modernized. In the US, we need to look at laws such as the Electronic Communications Privacy Act, which was written before most Americans had heard of email or the Internet and when cell phones were the size of bricks. This is no less true overseas. While Estonia had modern laws that allowed the US Government to work with them on Operation Ghost Click, most countries laws are playing catch up with the state of modern technology.

CONCLUSION

The threat landscape is constantly changing, and cyber criminals will not stop seeking new victims and new ways to compromise computers and networks. There is still much work to be done, but in one important way we have made progress: at all levels, government recognizes the imperative for collaboration to fight cybercrime and is working to fill the gaps in our law enforcement system.

At Symantec, we are committed to improving online security across the globe, and will continue to work collaboratively with governments on ways to do so. Thank you again for the opportunity to testify, and I will be happy to answer any questions you may have.

REUTERS

PROVIDENCE Journal | Providence Journal eEdition

Protecting against cyber-attacks

By Senators Lindsey Graham and Sheldon Whitehouse
April 9, 2013

Last year, Congress failed to forge a workable framework for cybersecurity to protect the United States against a fast-growing national security and economic threat. Our cyber-networks remain dangerously vulnerable to outside attack and are the repeated targets of foreign governments intent on stealing the fruits of our intellectual and business efforts. Congress must address this crucial issue.

The threat to our critical infrastructure, national security and economic prosperity was laid out in a February report by Mandiant, a respected U.S. computer security firm. An elite unit of Chinese hackers affiliated with China's People Liberation Army, the report concluded, is likely behind a wave of attacks on U.S. government and business computer systems.

Since 2006, according to the report, the Chinese unit has stolen data – including blueprints, test results, business plans and emails – from at least 115 U.S. companies across a wide spectrum of major industries.

Almost every facet of American life is threatened when intruders exploit our cyber-vulnerabilities. And the risk is not from China alone. Foreign governments like Iran and terrorist organizations such as al Qaeda seek to worm into critical national infrastructure and threaten catastrophe here at home. Foreign agents raid our companies, stealing plans, formulas and designs. Foreign criminal networks take money out of our banks, defraud consumers with scams and sell illicit goods and products, cheating U.S. manufacturers. It may be the greatest illicit transfer of wealth in human history.

If you're a business owner, listen to our top cyber-experts, who say there are only two kinds of businesses: those that have been hacked, and those that don't know they've been hacked. If you're a consumer, know there's a third group: those who know they've been hacked and won't admit it.

Following Congress' failure to act, President Barack Obama has issued an executive order to address some of our nation's vulnerabilities. But an executive order can't accomplish everything that needs to be done.

We both worked hard last year to forge a bipartisan legislative compromise, and still believe it can be reached. To get this right, a bipartisan solution must include the following elements:

First, there must be far more disclosure of cyber-threats. Americans should not be in the dark about the risks we face. The government should do more public reporting, and companies should be candid with shareholders and customers about the problems.

Second, companies that operate critical U.S. infrastructure should meet some basic standard to protect their customers and our way of life. We have discussed ways for government to work with industry to set these standards while allowing private-sector initiative to determine the specific manner of companies' compliance. The model may work for other sectors, as a more nimble, smarter alternative to overly prescriptive administrative regulation.

Third, government agencies and private industries, particularly the communications companies that run the Web's infrastructure, need to share more information about the threats they see on their networks. This will require removing existing legal barriers – while protecting classified information and privacy.

Fourth, prosecutors should have the resources to pursue international cyber-criminals. These cases are technically and legally complex; involve difficult intelligence and diplomatic and foreign law challenges, and require massive forensic capability. Rather than complain about cyber-robbers overseas, we'd like to see them indicted and prosecuted.

Fifth, we need to make sure that training is available to bring Americans into the cybersecurity field, and maintain our technical leadership in this crucial area. Cyber-danger is not going away. More and more of our business and personal lives will take place in cyberspace. Cyber-threats will expand and evolve. America must be prepared.

In all this, we must safeguard the privacy of U.S. citizens. We can keep the United States secure without infringing dearly held liberties. Well-crafted legislation can achieve this.

We must do this, because we never want to see a nightmare scenario become reality.

Imagine waking up one morning to find the power out at home, and no signal on the phone or computer to tell you what's going on. You drive into town and find dozens of people in front of the banks, wondering why the ATMs aren't working. There are lines at gas stations and supermarkets because businesses can't process sales on credit or debit cards.

The failures all around you – no heat or air conditioning, no banking, no Internet or phone, and cash-only sales in the stores that are open – have no end in sight. There may even be smoke on the horizon from a plant on the outskirts of town, aflame because of compromised equipment.

A cyber-attack could cause all this. We need to work together to ensure America never has to face that day.

Senator Lindsey Graham (R-S.C.) is ranking member of the Subcommittee on Crime and Terrorism of the Senate Judiciary Committee and also serves on the Armed Services and Budget Committees. Senator Sheldon Whitehouse (D-R.I.) serves on the Senate Judiciary Committee and is the chairmen of its Subcommittee on Crime and Terrorism. In 2010 he served as co-chairman of the Select Committee on Intelligence's Cyber Task Force.

ANNUAL REPORT TO CONGRESS

Military and Security Developments Involving the People's Republic of China 2013

Office of the Secretary of Defense

Preparation of this report cost the Department of Defense a total of approximately $95,000 in Fiscal Years 2012-2013.

missiles with ranges of 1,000km and speeds of 2,800m/s. China's domestic CSA-9 long-range SAM system is expected to have a limited capability to provide point defense against tactical ballistic missiles with ranges up to 500km. China is proceeding with the research and development of a missile defense umbrella consisting of kinetic energy intercept at exo-atmospheric altitudes (>80km), as well as intercepts of ballistic missiles and other aerospace vehicles within the upper atmosphere. In January 2010, and again in January 2013, China successfully intercepted a ballistic missile at mid-course, using a ground-based missile.

Cyber Activities Directed Against the Department of Defense. In 2012, numerous computer systems around the world, including those owned by the U.S. government, continued to be targeted for intrusions, some of which appear to be attributable directly to the Chinese government and military. These intrusions were focused on exfiltrating information. China is using its computer network exploitation (CNE) capability to support intelligence collection against the U.S. diplomatic, economic, and defense industrial base sectors that support U.S. national defense programs. The information targeted could potentially be used to benefit China's defense industry, high technology industries, policymaker interest in US leadership thinking on key China issues, and military planners building a picture of U.S. network defense networks, logistics, and related military capabilities that could be exploited during a crisis. Although this alone is a serious concern, the accesses and skills required for these intrusions are similar to those necessary to conduct computer network attacks. China's 2010 Defense White Paper notes China's own concern over foreign cyberwarfare efforts and highlighted the importance of cyber-security in China's national defense.

Cyberwarfare in China's Military. Cyberwarfare capabilities could serve Chinese military operations in three key areas. First and foremost, they allow data collection for intelligence and computer network attack purposes. Second, they can be employed to constrain an adversary's actions or slow response time by targeting network-based logistics, communications, and commercial activities. Third, they can serve as a force multiplier when coupled with kinetic attacks during times of crisis or conflict.

Developing cyber capabilities for warfare is consistent with authoritative PLA military writings. Two military doctrinal writings, *Science of Strategy,* and *Science of Campaigns* identify information warfare (IW) as integral to achieving information superiority and an effective means for countering a stronger foe. Although neither document identifies the specific criteria for employing computer network attack against an adversary, both advocate developing capabilities to compete in this medium.

The *Science of Strategy* and *Science of Campaigns* detail the effectiveness of IW and CNO in conflicts and advocate targeting adversary C2 and logistics networks to affect their ability to operate during the early stages of conflict. As *Science of Strategy* explains, "In the information war, the command and control system is the heart of information collection, control, and application on the battlefield. It is also the nerve center of the entire battlefield."

In parallel with its military preparations, China has increased diplomatic engagement and advocacy in multilateral and international forums where cyber issues are discussed and debated. Beijing's agenda is frequently in line with Russia's efforts to promote more international control over cyber activities. China and Russia continue to promote an Information Security Code of Conduct that would have governments exercise sovereign authority over the flow of information and control of content in cyberspace. Both governments also continue to play a disruptive role in multilateral efforts to establish transparency and confidence-building measures in international fora such as the Organization for Security and Cooperation in Europe (OSCE), ASEAN Regional Forum, and the UN Group of Governmental Experts. Although China has not yet agreed with the U.S. position that existing mechanisms, such as international humanitarian law, apply in cyberspace, Beijing's thinking continues to evolve.

Role of Electronic Warfare (EW) in Future Conflict

An integral component of warfare, the PLA identifies EW as a way to reduce or eliminate U.S. technological advantages. Chinese EW doctrine emphasizes using electromagnetic spectrum weapons to suppress or deceive enemy electronic equipment. PLA EW strategy focuses on radio, radar, optical, infrared, and microwave frequencies, in addition to adversarial computer and information systems.

Chinese EW strategy stresses that it is a vital fourth dimension to combat and should be considered equally with traditional ground, sea, and air forces. Effective EW is seen as a decisive aid during military operations and consequently the key to determining the outcome of war. The Chinese see EW as an important force multiplier and would likely employ it in support of all combat arms and services during a conflict.

PLA EW units have conducted jamming and anti-jamming operations testing the military's understanding of EW weapons, equipment, and performance, which helped improve their confidence in conducting force-on-force, real-equipment confrontation operations in simulated electronic warfare environments. The advances in research and deployment of electronic warfare weapons are being tested in these exercises and have proven effective. These EW weapons include jamming equipment against multiple communication and radar systems and GPS satellite systems. EW systems are also being deployed with other sea and air-based platforms intended for both offensive and defensive operations.