RPTS MCKENZIE

DCMN SECKMAN

CYBERSECURITY: NETWORK THREATS AND POLICY CHALLENGES

FRIDAY, MAY 1, 2009

House of Representatives,

Subcommittee on Communications, Technology,

and the Internet,

Committee on Energy and Commerce,

Washington, D.C.

The subcommittee met, pursuant to notice, at 1:04 p.m., in Room 2123, Rayburn House Office Building, Hon. Anthony D. Weiner presiding.

Present: Representative Weiner.

Staff Present: Amy Levine, Senior Counsel; Greg Guice, Counsel; Sarah Fisher, Special Assistant; Amy Bender, Minority Counsel; Neil Fried, Minority Senior Counsel; and Sam Costello, Minority Assistant.

Mr. Weiner. Welcome to the hearing of the Energy and Commerce Subcommittee on Communications, Technology, and the Internet.

I welcome the witnesses.

Since April 17th, President Obama has had on his desk recommendations of a panel that has been studying cybersecurity policies and structures of our government. Already we have heard a push and pull going on behind the scenes and increasingly in public about some of the thorniest questions that that panel will consider.

Today we will offer some advice.

This committee will have the jurisdiction to implement the policies that are recommended by the President, and notwithstanding the activities in some other committees, which we welcome, the jurisdiction for these matters will be here in the Telecommunications Subcommittee and in the Energy and Commerce Committee.

We will hear from a brilliant set of witnesses, but we will not hear from someone from the administration for some reasons obvious and some reasons not so. The obvious is I don't think they know what their policies will be. So asking them to testify on them might be premature. But also we wanted to, by design, to have a conversation here among interested parties in the community that would allow us to inform our reactions to the

administration's proposals that will be forthcoming.

In fact, cybersecurity is not a singular problem. It is at least three. There are, of course, the issues of personal security, issues of spam and nuisance, but also identity theft and the like. This is also an issue of critical infrastructure and protecting it, the economic security of our country and, frankly, the increasingly interconnected economies of all of the countries of the world.

And of course, this is a national security issue. An issue that has been seemingly increasingly brought to the public's attention with stories that fill up the newspapers on everything from fighter jet plans being stolen to Chinese-based spying on Tibet and some of the other countries. We have heard just about a story a day.

We will endeavor to ask and answer some of the big questions that the President is going to be wrestling with. How do we respond to or mitigate or work around or generally respond to the inherent paradox that is the Internet? Its openness, its openness to innovation, its openness to democratization; but also its openness to mischief and mischief makers and often things worse than mischief.

For the most part, Congress has been wise in resisting the temptation for heavy-handed intervention, and that has served the Internet well and has served our country well.

We also have to ask the question that has been dominating the

discussions at the White House. Who should be in charge of combating the mischief maker, the con artists or the terrorists; not only what agency of government but whether or not it should be government at all, and if so, what relationship between government and the private sector? With government, of course, you often get the inevitable heavy-handedness and secrecy, but you do get strong centralized action when it is needed. With the private sector you get entrepreneurship, creativity but you also get silos of self-interest that don't always make for vigorous system-wide defense.

One thing is sure. This cancer can't be exorcised with a rusty axe; we need to use a scalpel.

Third, we have to ask the questions, are we destined to constantly fight the last war when it comes to cybersecurity? Is the cycle of discovery, warning, insulation inevitable?

Conficker gave us an interesting and good example of this. Tiffany and my staff put together a timeline of the Conficker virus, and here is what she wrote.

On December 29, 2008 Conficker.B is first detected; Conficker.A updates itself to Conficker.B.

February 20, 2009, Conficker.C is discovered; Conficker.B updates itself to Conficker.C.

March 4th, Conficker.D is discovered; Conficker.C updates itself to Conficker.D.

April 7, 2009, Conficker.E is discovered; Conficker.D updates

itself to Conficker.E.

Conficker.E downloads scareware and spyware onto computers. It deletes automatic updates of computer systems and prompts a fake need to update one's computer. And when individuals buy the software protection Conficker.E offers, the computer downloads spyware onto the computer. This is a dynamic that clearly does not lend itself very well to discovering the problem, addressing the problem, moving on to the next problem.

Maybe cat and mouse is our only option. Maybe, though, we don't need a military-type approach but more an approach that we in government use at say NIH or the Food and Drug Administration, where government helps to augment creative solutions, help with some of the R&D, and then let the private sector go off and implement them.

And then, of course, there are the more provocative questions that we might not have time to touch on today, such as John Markoff in the New York Times asking the question, do we need a new Internet all together? Or the provocative title of Jonathan Zittrain's great book, "The Future of the Internet and How to Stop It."

The witnesses we have before us will offer us an opportunity to answer some but not all of these questions. This is a conversation that inevitably has to take place not only here in Congress but in the businesses around the Internet and in the coffee shops and parlors of people's personal experiences and, of

course, over at the White House.

Now it is my honor to introduce the witnesses we have before us today.

STATEMENTS OF DAN KAMINSKY, DIRECTOR OF PENETRATION TESTING, IOACTIVE; GREG NOJEIM, SENIOR COUNSEL, CENTER FOR DEMOCRACY AND TECHNOLOGY; LARRY CLINTON, PRESIDENT AND CEO, INTERNET SECURITY ALLIANCE; AND RODNEY L. JOFFE, SENIOR VICE PRESIDENT AND SENIOR TECHNOLOGIST, NEUSTAR.

Mr. Weiner. Dan Kaminsky is the director of penetration testing at IOActive, where he focuses on design capabilities and vulnerabilities of network protocols. He is probably most famous for having discovered a fundamental flaw in the Domain Name System or DNS that would allow him to reassign Web addresses, take over banking sites, or disrupt the flow of data over the Internet. Thankfully, he was a good hacker and brought this flaw to the attention of those entities that were in a position to fix it.

Dan Kaminsky, you are our first witness.

You are recognized for 5 minutes. I know you have presented some testimony already, so feel free to summarize as you see as appropriate.

STATEMENT OF DAN KAMINSKY

Mr. Kaminsky. Thank you very much. Hello, everyone. Members of the subcommittee, please allow me to express my appreciation for offering me this opportunity to testify today.

I am, as said, the director of penetration testing at IOActive. I spent the last 10 years of my career working for Fortune 500 companies, including Cisco, Avaya, and Microsoft to help secure their systems.

It was an interesting experience fixing DNS, working with all the people that needed to be in a position to actually get the fix out, get the fix deployed and ultimately protect the ecosystem. It was an example of a public-private partnership. We worked with USCERT in order to get communication out to the Federal agencies that themselves had to get software out. And it was a remarkable, remarkable experience for all parties. It was a highlight of 2008; 2008 was not, however, an easy year.

Verizon business actually every year puts out a report called the Data Breach Investigation Report. In an industry that always struggles to have good data to work with, Verizon actually did a wonderful thing and has for the last few years in summarizing what they see in their limited sample of their customers base. And what they saw was astonishing. Over 285 million records were

compromised last year, just from their customer base. According to Verizon, this is more than every other year they had seen combined. Worse, over 91 percent of those compromised records, most of which were payment card information, over 91 percent of those were traced going back to organized crime.

We have worldwide problems, and we live in a much more dangerous world than when I first started doing computer security years ago. The reality is, hacking is no longer about kids. It is about people with kids who would like to feed them. Attackers have had years to figure out the absolute best ways that they can monetize their access. Recently, they actually managed to coordinate a widespread attack against the ATM infrastructure in which, in 49 cities, $9 million was extracted from ATMs using purloined ATM data.

Beyond that, extortion, something we have almost no information on, is rumored to be becoming an extraordinary problem not merely hitting the sides or gambling or pornography aspects of the economy but actually standard businesses.

As you mentioned, Conficker. Conficker, it turns out, was a remarkable success. If Conficker had come out in 2003, pretty much every single computer on the Internet, at least every Windows machine, would have been compromised. Since 2003, Windows has become a much, much more secure platform. The actual result of the work from 2003 was probably over 99 percent of the machines that otherwise would have been affected, infected by Conficker

never had a problem. That is what happened when we -- that is the result of our scans and our monitoring of the situation.

That being said, a percentage of a large number is still a large number, and we have had to deal with millions and millions of machines infected. What was most scary about Conficker is, thus far, we still have no idea what the authors of it want.

So where do most of these compromises come from? How is this happening? A lot of problems are in software. This is true. There is a lot of buggy software out there. But according to the Verizon business report, over 60 percent of actual penetrations that led to loss of data did not come from buggy code; they came from our simple inability to strongly authenticate other nodes on the Internet, default passwords, lack of passwords, lack of insufficiently strong passwords. It turns out authentication is in huge amounts of trouble on the Internet today, and the data suggests it is leading directly to compromises of personal information.

Now people may say, why are we still using passwords? Why is this problem still there? It turns out it is because it is the only way to reasonably make things work at all. It turns out, if something doesn't work, people won't use it, even if it is theoretically more secure.

This is ultimately why I become a supporter of the technology known as DNSSEC. DNSSEC on its face is a method to fix DNS, but it is not just that. DNSSEC ultimately allows us to use DNS's

power for allowing communication across organizational lines, ultimately trust across organizational lines, and allows us to apply cryptographic strength to that trust so it can be used not just for existing systems or not just for locating systems but for actually authenticating them and ultimately authenticating the people on the other side. It will take some work. It will take a lot of work, but I see it as the key towards making a new security authenticating ecosystem.

Thank you.

[The prepared statement of Mr. Kaminsky follows:]

******** INSERT 1-1 ********

Mr. Weiner. Thank you.

Our next witness is Rodney Joffe. He is the senior vice president and senior technologist for NeuStar. He is a renowned expert on security flaws in the Internet. He also participated in the Department of Homeland Security's Cyber Storm II, a multinational cybersecurity exercise that examines security preparedness and response capabilities across a variety of infrastructures.

Mr. Joffe, you are recognized for 5 minutes.

STATEMENT OF RODNEY L. JOFFE

Mr. Joffe. Good afternoon, Chairman Weiner.

I am, as you say, the senior vice president, senior technologist for NeuStar.

NeuStar provides innovative services that enable trusted communication across networks, applications, enterprises around the world. A major portion of that is involvement with directories. I joined NeuStar in 2006 when UltraDNS, which is a company I founded, was acquired by NeuStar.

DNS is the core directory that really routes traffic on the Internet. Every one of us uses it all the time. Any computing machine makes use of DNS. The technology itself basically deals with the fact that, as humans, we recognize and we are able to use

words. Computers understand numbers, in this particular case, IP addresses, and they require the IP addresses to be able to move traffic or to be able to get you from one site to another. The DNS, simply put, is the directory that converts names to numbers and vice versa.

So, for example, if I want to go to www.house.gov, I put that into an Internet browser, and the DNS would convert that to the IP address, 204.141.87.18, and the computing device is then able to get you to the House server, and the screen appears on your computer.

So NeuStar also provides the core directory service for the .biz and the .us top level domains, as well as 17 other top level domains, including a number of other country codes. So, for example, we provide the service for Canada, .ca; for the United Kingdom; and for Japan. We also provide the directory service for anyone attempting to reach many of the Fortune 500 or the e2000 sites. So, in all, we serve about 4,000 corporations and government departments around the world and about 15 million domain names.

I really appreciate you inviting me to speak about the particular threats, and I appreciate the fact that the committee has actually taken an interest.

Probably the oldest reason for Internet attacks is that of ego bragging. There are three real reasons. The perpetrators behind those kinds of attacks are generally young and immature,

and they are intent on showing their prowess with computer programming with little or no regard for the damage that they cause in their attacks.

The second and most common category is for financial gain. In this case, the attacks are committed by individuals as well as by organized gangs of criminals. They include large spam e-mail that you have mentioned; the interception and illegal use of computer data, which you have also mentioned, most commonly bank data and credit card data, extortion schemes, which have been around for quite a while; and Distributed Denial of Service attacks. In DDOS or Distributed Denial of Service Attacks, botnets, which are large groups of thousands, hundreds of thousands, sometimes millions of machines all working together, that have been previously infected, will be used and rented by criminals in the underground. Not only for themselves, but they rent them out. It is a business. The criminal then commands the botnet to try and reach a specific site. The result is that a Web site, for example, is hit by millions of hackers at the same time in an attempt to overwhelm the site and take it down. Frequently, it is successful.

An important thing to note here is that it would require fewer than 10,000 strategically located compromised machines with some reasonable knowledge to disable a sizable portion of the U.S. Internet. It doesn't take many machines.

Generally though the botnets involve hundreds of thousands

because the people who build these botnets have no real cost. They are using our resources, and botnets are built almost automatically. We have seen notes where kids go off to school, come back, and take a look at how many bots they have added to their botnet while they have been at school. We have actually seen discussion in the underground about that.

Another lesson on the very dangerous kind of malicious behavior that exists in cyberspace which is known as DNS cache poisoning. This is something that Dan has discovered as you know, last year. Thanks to Dan, we are a lot safer than we were.

But effectively what happens with DNS cash poisoning is that your ISP's caching service are poisoned. The DNS is pointed to a fake site. When you go to your bank, you end up at a Web site that looks just like your bank, but actually isn't. It belongs to criminals. And what they do is they ask you for your password, ask for your user ID, and then they go ahead and make use of that to make transfers and to empty your account.

The third category we talk about is cyberterrorism, which really relates to generally nation-state issues. Over the last 2 years, there have been at least three public attacks reportedly on nation-states. We know that one of them probably is, countries we all recognize Estonia, Georgia and Kyrgyzstan. Additionally, The Wall Street Journal reported on April 8th of this year, as you mentioned, critical infrastructure facilities had been compromised.

It is really important to note over here that, while most people are unaware of the attacks, these attacks are going on all the time, and our industry is reasonably successful in being able to actually stop some of those attacks before they become public. But the attacks are occurring all of the time.

On April 12th, talking about banking, most of this is theoretical, on April 12th, the DNS servers of a major Brazilian ISP, Virtua were compromised. Their cache was poisoned for the entry of one of the largest banks in Brazil, Bradesco, making use of the kinds of things that Dan had talked about. Users of that bank were redirected to a fake Web site, and it took about 5 hours before the bank and the ISP were able to realize that, in fact, the recent entry had been poisoned. The bank was reasonably open in their statement when they said, approximately 1 percent of our customers were affected by this. But that represents almost 150,000 individuals who could possibly have had their accounts compromised during one event. And this is an event in one country over the course of 5 hours.

The other event is one that you have touched on already, and with indulgence, I will perhaps expand a bit more, which is on the Conficker botnet, the Conficker worm.

We have an industry group called the Conficker Working Group, an unofficial group that came together in the private sector to deal with a real threat, an immediate threat of Conficker. They have been working around the clock to dismantle the botnet with no

real success. On the 8th of April, as you said, it took the first steps with version E. You had mentioned earlier that it had upgraded from version D to version E. It wasn't just an upgrade. It was also the first time we got some insight into how the botnet was actually going to be used. It was used to sell fake antivirus. If you have seen those pop-ups on your computer screen, where it may say that you are infected, you normally expect that to show from your antivirus software. In fact, if you were infected with Conficker, there were no messages from your antivirus software. It was actually from the criminal group behind it. They then advertise some software that you could purchase online there and then, enter your credit card, your personal information and download their software. Of course, their software doesn't disable the virus. It installs more malicious software, and the job is now even more difficult.

As a sobering side note on this, last month, in collaboration with one of the other members of the Conficker Working Group from Georgia Tech, we identified at least 300 critical medical devices from a single manufacturer. We stumbled on it. It is not that easy to tell what it is. There were at least 300 medical devices that were infected with Conficker. The hospitals had no idea. The manufacturer had no idea. When we called them, they were obviously shocked. These devices are used in hospitals to allow doctors to view high-intensity scans, MRI for example, CT scans. And they are often found in ICU facilities. They are connected to

local area networks. They should never, ever have been connected to the Internet, and according to the manufacturers, they weren't. However, they were connected at some stage to the Internet because they were infected, and they were checking in with us.

The way we know they are infected is that we run systems that those devices will connect to. Worse, after we had notified the manufacturer and the hospitals involved, and we are obviously doing our best for hospitals around the world, we were told that, because of FDA rules that they referred to as 510(k) regulations, 90 days notice was required before the systems could be modified to remove the infections and the vulnerabilities. In some cases, clearly, there can be a disconnect between government rules which are meant to protect consumers and today's cyber threats which sometimes result in delaying and hindering the ability to fix problems as in the medical system.

So based on my long experience in operating large networks connected to the Internet, I think one of the most important areas for Congress to concentrate on is improving the communication both between the public and the private sectors and across those sectors. The Department of Homeland Security operates USCERT, which is part of its mission to act as a liaison between public and private sectors. It is a start, in my view, but it is woefully understaffed, and it is woefully underfunded for the enormous task that is put before it. Ideally, I would like to see much more focussed collaboration, as that Dan had mentioned and I

assume that you have heard before.

In summary, we face enormous escalating threats from all parts of cyberspace both to the economy and to the safety and well-being of many citizens. So, beyond the normal perennial call for additional resources, we need to concentrate on improving the collaboration between industry and government; between different government departments; and between the U.S. and foreign governments.

Mr. Chairman, thank you for the opportunity to address you and the rest of the committee, and I am happy to answer any questions.

[The prepared statement of Mr. Joffe follows:]

******** INSERT 1-2 ********

Mr. Weiner. Thank you, Mr. Joffe.

Our next witness is Larry Clinton. He is the president and CEO of the Internet Security Alliance, an organization that represents corporate security interest and provides a forum for information sharing on information-security issues. Mr. Clinton is also a member of the GAO's expert panel which will make recommendations to the Obama administration on cybersecurity.

Mr. Clinton, welcome. You are recognized for 5 minutes.

STATEMENT OF LARRY CLINTON

Mr. Clinton. Thank you, Mr. Chairman, and thank you for inviting us to have this hearing, and we are delighted to participate.

Mr. Chairman, virtually our entire economy, our defense system, our culture, now depend on electronic communication systems that are extremely vulnerable and under constant attack. The vast majority of these systems are owned and operated by the private sector.

Unfortunately, virtually all the economic incentives regarding cybersecurity favor the attackers. Attacks are relatively cheap. The area to defend is virtually limitless. Defense residing in separate although connected systems is difficult to coordinate and expensive compared to the return on

investment.

The good news is that we know a great deal about how to prevent and stop these attacks. The bad news is, we are just not doing it. The PricewaterhouseCooper's Global Information Security Study of over 1,000 companies found that those that followed the industry best practices could prevent, almost entirely mitigate the attacks against them. The 2008 Data Breach Investigations Report previously referred to studied more than 500 forensic engagements over a 4-year period and concluded that 87 percent of the breaches could have been avoided if reasonable and identifiable security practices had been followed. Robert Bigman, chief of information assurance for the CIA, has stated publicly that most of the attacks that he sees are not that sophisticated, and 80 to 90 percent of them could be prevented with due diligence.

However, we cannot solve cybersecurity problems by attempting to adapt 19th Century models to a 21st Century problem. A common theme from some policymakers who are relatively new to the cybersecurity problem tend to say, well if industry won't do this on their own, we will just have to regulate them. The Internet Security Alliance believes that such an approach is short-sighted and does not reflect the necessary understanding of the new breed of technologies created by the Internet to begin with. Federal regulatory mandates are best designed to combat corporate malfeasance, and that is not the problem we are facing with

Internet security.

Even if Congress would enact an enlightened statute, it would only have reach to our national borders, and this is an international problem. A set of U.S. regulations would place U.S. industry at a competitive disadvantage in the global marketplace at the time when we can least afford it.

Specific regulations would likely be too static to the technology, and the threat vectors constantly change; while flexible or conceptual regulations may be too general to have any real effect. Regulations are often subject to political pressure, making minimum standards de facto ceilings, something like what we have with campaign finance.

We need a better system, a 21st Century system. Fortunately, there are signs that the Obama administration understands the need for a modern approach to cybersecurity that appreciates the economic issues as much as the technical ones. President Obama assigned Melissa Hathaway of the National Security Council to conduct a review of our Nation's cybersecurity status. Although the report has not been made fully public, Ms. Hathaway did provide a preview a week ago in Silicon Valley.

Among the specifics from the report she did share was acceptance of the principle that, quote, previous attempts to deal with cybersecurity in isolation have failed in no small part because cybersecurity only succeeds in the context of broader economic progress. In particular, Ms. Hathaway specifically cited

the need for government to work with the private sector to, quote, improve market incentives. This is a significant departure from the previous administration's view, which was that the market would emerge spontaneously to address these problems. That did not happen.

Ms. Hathaway is correct. We need to improve market incentives. Consistent with this view, the Internet Security Alliance asks Congress to consider enacting what we call the Cyber Safety Act. The Cyber Safety Act is an affirmative and contemporary approach to dealing with the 21st Century problems of cybersecurity. In brief, we suggest that government's role is not to prescribe mandatory regulation but rather provide market incentives for the private sector entities to adopt the security practices and standards and technologies that have already been empirically demonstrated to work. There are a wide range of incentives which have already been used in various sectors of the economy, such as insurance, liability protections, procurement awards programs, SBA loans, et cetera. All these achieve government goals. What we are suggesting is that these should now be applied to cybersecurity.

Government ought to designate a range of public and private sector entities which can serve as a qualifying set for standards and practices. Government ought to then fund research used to evaluate the standards, practices and technologies developed on an ongoing basis with the sole criteria being their effectiveness.

Private sector entities that can demonstrate compliance with the standards and practices would be deemed effective and would qualify for the incentives. What we are attempting to do here through the Cyber Safety Act is to change the economics of cybersecurity by constructing a market that makes private organizations want to continually invest in cybersecurity in their own economic self-interest. Only then can we create the sort of sustainable and evolving system of cybersecurity that we need.

The purpose of this system is to defend the national security's interest, and thus it is worth the relatively modest investment that the government would have to make in order to provide the incentives. The present research and the expert testimony shows that by motivating the widespread adoption of the practices that have already been demonstrated to work, the vast majority of the problem we are experiencing can be quickly addressed.

However, there is a small but critical 10 to 15 percent of attacks that will not be addressed in this fashion. My written statement goes into some detail on a number of these problems, including the supply chain, the incongruity with laws that were written in the 1980s to current technology, the need to change the basis for security from protecting the instruments like the computers to protecting the data itself. All of these will require a lot more work than what we are proposing with the Cyber Safety Act.

We look forward to working with the committee both to address the 90 percent of the problem that is basically low-hanging fruit as well as the 10 percent of the problem that is going to require substantially more work.

Thank you, Mr. Chairman.

[The prepared statement of Mr. Clinton follows:]

******** INSERT 1-3 ********

Mr. Weiner. Thank you, Mr. Clinton.

Our final panelist before we begin questions is Gregory Nojeim. He is the senior counsel and director of the Project on Freedom, Security and Technology at the Center for Democracy and Technology. He has been integral in bringing together broad coalitions from across the political spectrum to limit the threats to privacy and civil liberties posed by government monitoring of the Internet and other communications.

Mr. Nojeim, you are recognized for 5 minutes.

STATEMENT OF GREG NOJEIM

Mr. Nojeim. Thank you, Chairman Weiner.

It is really a pleasure to testify today on behalf of CDT. Our organization is a nonprofit organization, and we are dedicated to keeping the Internet open, innovative and free.

So it won't surprise you that most of my comments today will focus on the communications infrastructure as opposed to other infrastructure systems and, in particular, on the Internet.

Cybersecurity policies should distinguish between government systems and systems that are owned and operated by the private sector. Policy toward government systems can be much more proscriptive. It can be much more top-down than policy toward private systems.

Congress should also distinguish between the elements of the critical infrastructure operated by the private sector that primarily support free speech and those that do not. As an example, measures that might be appropriate for securing the control systems of a pipeline, they might not be right for securing the Internet. It might be wise, for example, to require a particular kind of authentication of a user of an information system that controls a pipeline. But it might not be wise to require that same kind of authentication for a computer user in the privacy of their own home while they are surfing the Internet.

The characteristics that have made the Internet successful, openness, decentralization, user control, things that you mentioned in your opening statement, Mr. Chairman; these things can be put at risk if heavy-handed cybersecurity policies are applied to all critical infrastructure. This subcommittee should make protection of these attributes an essential part of its cybersecurity mission.

It is also important to ensure that cybersecurity measures do not result in a governmental entity monitoring private communications networks for intrusions. Monitoring these systems is the job of private sector communications providers, and they already do this.

The government can help them do a better job. It can help them develop tools that allow communications providers to monitor for intrusions in the least intrusive way. But it should not be

in the business of monitoring private networks itself. Nor should the government be in the business of shutting down Internet traffic to compromised critical infrastructure information systems in the private sector.

While some have proposed giving the President this extraordinary power over all critical infrastructures, we believe it should extend only to governmental systems. Such authority applied to private systems would empower a President to coerce unwise, even illegal activity. To our knowledge, no circumstance has yet arisen that would justify a Presidential Order to cut off Internet traffic to a private critical infrastructure system when the operators of that system think it should not be cut off.

We also urge you to carefully address two overarching recurring cybersecurity policy problems. The first is excessive secrecy. The subcommittee should work to improve the transparency of the cybersecurity program. Transparency builds trust with the private sector, and that is essential to foster its cooperation. It also enhances public understanding of the nature and justification for any impact on users of cybersecurity measures. Transparency also promotes essential accountability.

The second overarching problem is improving information sharing between the private sector and the government. Starting with the right questions about information sharing will help in settling on the right answers.

Exactly what information held by the private sector has not

been shared with the government when it was specifically requested? What reasons were given for the decision not to share? Why aren't existing information-sharing structures -- I am sorry. Why are existing information-sharing structures like USCERT falling short? And what additional market incentives would encourage the private sector to share threat and information solutions? Generally, as you approach these and other cybersecurity problems, we urge you to favor market-based measures over mandates. And we ask that you consider carefully the impact on the Internet of measures proposed for securing all critical infrastructure systems. Thank you.

[The prepared statement of Mr. Nojeim follows:]

******** INSERT 1-4 ********

Mr. Weiner. Thank you very much.

I would like to begin the conversation looking at, first, in some, as much as we can do in English, some of how the big stories of the day have emerged. When we read in The Wall Street Journal and elsewhere that computer spies have breached a fighter jet project; when The New York Times reports that a vast spy system lutes computers in 103 countries, walk me through a little bit about, and while you can't answer with certitude, a little bit of how we suspect these things have happened and why it is that the cat is a few steps behind the mouse on these things.

Mr. Kaminsky, you can start. You can choose either one of these. Walk me through about why this is more complicated than simply saying, let's just read some code, close some back doors and solve this problem.

Mr. Kaminsky. I would say there tend to be two main ways that attackers seem to be getting in. There are more, but I will go with two. The first way is that the software that is exposed on the Web for remote access, remote management, remote just data collection, while operating systems themselves have gotten significantly more secure over the last few years, the actual software that is exposed that drives Web sites tends to be homegrown and very poorly audited.

So a very common technique that attackers use is what is known as sequel injection, where they actually communicate with

the Web front end and messages are sent to the database back end. And the messages, unfortunately, are insufficiently sanitized or cleaned, and the database is caused to run arbitrary attacker software. That is the most common implementation flaw.

The other method is what I referred to earlier in my talk where I was talking about authentication techniques. According to the Verizon business report, 4 out of 10 of the times when they saw an actual compromise occur, they actually found that there was remote management -- remote management there specifically for third parties, for third-party vendors, using passwords that were either known or could be easily guessed. So we don't have the exact details, or at least I certainly do not have the exact details on how the joint strike fighter data was lost. But in terms of what was lost from server side, you will see either compromises on the Web site or compromises on remote management through default passwords.

One third case which should be brought up is that we do have issues with actual desktops and browsers themselves, where an individual desktop inside of an organization will be compromised through the Web browser through what is called a drive-by download, and that drive-by download will cause that individual host to be a jumping-off point for an attacker to then attack other assets within the organization.

Mr. Weiner. So that then leads us to Mr. Clinton's testimony that if you know these things, and these things thankfully keep

you in business, Mr. Kaminsky, does the panel agree -- maybe Mr. Kaminsky, you want to expand upon this -- but if an overwhelming number of the attacks happen in a certain prescribed way and that if there are certain steps you can take to protect yourself, and I think Mr. Clinton's testimony was 80 to 90 percent if you follow certain protocols; is this a problem people have, people being sloppy and what we are looking at is we figuring out ways to make them less sloppy?

Mr. Clinton, is that a fair summary of at least that portion of your testimony?

Mr. Clinton. Thank you, Mr. Chairman.

In part. I wouldn't say that it is necessarily people being sloppy, but there is some sloppiness involved. I would go up a level.

First of all, I would never dream of getting into a technical discussion with my colleague on the right. I will just accept everything he says as true.

I would operate at a different level. He can tell you in great detail why a particular attack happened. But once we have plugged that hole, the attackers are going to move to another hole. So while we can, you know, patch various holes in the Internet, they are going to continue to find new holes.

What we have to do, in our opinion, is change the system. We have to change the economics of it. The reason we don't have all of these things patched in the first place is because users don't

like security. It makes it harder to use, costs money; businesses the don't like it. What we have to do is change the system, so that instead of people trying to view cybersecurity as a cost center or a bother, they have got to view it as something they want to do so that we can change the economic dynamics of it. And that is what we are arguing for.

So it is certainly true that if we had the right incentives, people could fairly, quickly, and easily, according to the research and the CIA, could reasonably mitigate enormous percentages. I am not sure if it really is 90 percent, but that is what several studies say. If it was 80 percent, it would be an enormous advantage. And we would have to do this on a continuing basis. Once we put up a system of -- once we implemented all the best practices that the Verizon study suggests and we were able to stop this 80 percent, we would have to continue to work on that system because the attackers are going to say, okay, they have plugged all those holes; we are going to go after some others. So we have to do this on an ongoing basis, so the system has to continually grow because the system continually grows and changes.

Mr. Weiner. Doesn't this face the conflict, then, that it is in Google's interest to patch things that attack Google. It is in Verizon's interest, notwithstanding this industry-wide report, to attack things that attack Verizon?

Mr. Clinton. Right.

Mr. Weiner. Where does the system-added conversation happen?

Mr. Nojeim raises concerns about we the government entering into that field, but where should that conversation happen where someone is thinking about the system-wide protection? What is the recommendation of the witnesses on that?

Mr. Kaminsky.

Mr. Kaminsky. Too much of this discussion happens in the context of, how can we apply more pressure to people? How can we push them? How can we force them, or at least in the nicest way, how can we incentivize them? I don't think enough of the discussion happens around, how can we reduce the cost of delivering a secure solution? Users don't like security because security is too expensive and too difficult to deploy. Some of the most expensive failed information-technology projects in the world, we are talking in the $100 million scale and up, have been in systems that have attempted to do cryptographically asserted authentication.

A major role that government can play here is in giving all companies, giving Google, giving Verizon, giving Microsoft, giving us all one shared base that we can start building trust on. The Department of Commerce is doing an enormous amount of painful and thankless work to get DNSSEC to be something that can actually work with a central root of trust. The advantage to this is not just that we fix DNS. It is that we take so much of security technology, which has been a lot of promise and not as much user-opting-in as we might like, to make this stuff inexpensive

enough so that it is actually something that can be deployed. People want security, but they want their systems to work after, and they don't want their costs to explode. DNSSEC can help that.

Mr. Clinton. If I could just quickly, Mr. Chairman. And I would agree with what he said, but to get to your broader issue of, how do we get everybody to do this, it is because everybody has got to see some sort of benefit to doing it. I mean, the problem that we have is, this is a joint system, and the vulnerability is distributed. And they may be trying to get to -- China, for example, may be trying to get to the Pentagon. They don't attack the Pentagon directly. They don't even attack Raytheon, that is linked to the Pentagon. They attack Raytheon's subcontractor, and by getting to Raytheon's subcontractor, they get to Raytheon, and through that they get to -- so we have to get out to that subcontractor. And the subcontractor in the current system says, well -- the Pentagon says, we will give a contract to Raytheon, and they will enhance their security, which they do. They have very good security. And we will tell them to enforce it on the subcontractor. So Raytheon attempts to do that. So the subcontractor says, I am sorry, it is just not worth it for me. I don't want the business. I mean, this is like 5 percent of my business. I am not going to change over my entire information security system. They walk away from the business, which is bad from everybody's point of view. What we are advocating is, we need to have an incentive in place, a small business loan, an

insurance benefit, something -- there are lots of them -- so that the subcontractor now wants to keep his or her security completely up to date. So that we have an incentive for Raytheon that is a procurement contract; we have an incentive for the subcontractor, maybe you know, the ability to get an SBA loan or a lower insurance rate, and so that everybody has -- we need a system-wide set of incentives, and the incentives are going to be different for different people. This is not a one-size-fits-all world. We have to stop thinking of it that way. We need a network of incentives to address a network security issue.

Mr. Weiner. It is puzzling, though, it is puzzling though that we need to offer incentives for a government contractor of Raytheon to do what is intuitive, which is to not share terabytes of information on the Internet with hackers. I am not quite sure that the -- I mean, it strikes me that this gets back to the question and answer; how do you make sure that the silos of security extend -- I mean are systematic?

Mr. Joffe.

Mr. Joffe. Thank you, Mr. Chairman.

There are a couple of fundamental things to think about here. We talk about incentives. There are some fundamental issues. When it comes to incentives, one of the key things that I find when I talk to large corporations that have issues is, they say, well, what is in it for me? And that is really the thing that should drive the incentives. The incentives will be different,

but as long as you can show someone what is in it for them.

One of the problems we have now is that there are -- the issues could affect so many parts of the world and so many parts of the commercial world that people say, why would I step up and fix my part of the problem if other people aren't fixing their part of the problem? Someone else will do it. It seems to be a driving theme in most of the meetings I end up having.

And until I can point out how it affects someone specifically, they really say, not our problem. People don't think about it as being their problem.

The second thing is that the bad guys are as good as we are. One of the problems that we are facing and doesn't seem to be sort of dealt with much is that the people behind most of these attacks are as good as we are if not better. For some other reason, it almost seems like the bad guys are us. The level of sophistication, the things that we see, for example, in Conficker using, you know, certainly state-of-the-art and best-of-breed techniques.

If I was a university professor, grading something like Conficker.E, it would have a very, very high grade. They have done everything right. We don't seem to be able to do it. Maybe it is because you go to the typical large government contractor, and there are 50,000 or 60,000 people who are involved with software development in some way. It seems to be very difficult for us to be able to control that, and there doesn't seem to be

enough of an incentive overall for the companies to take a holistic approach until you see the front page of the Wall Street Journal. Then, all of a sudden, everyone wakes up.

Finally, there are two different ways that this happens. One of the ways -- and I don't know -- obviously, I know nothing about the Joint Strike Fighter issue. But in many cases, this is determined breaches by humans where someone works away at finding the problem. They have all the time in the world. They have a lot of patience, and they work their way through breaking into a system, including using social engineering. A lot of things that have been found have been as a result of social engineering. The issue with USB drives, for example, which not only was an issue for the Federal Government but is an issue with Conficker. One of the major reinfection vectors we see now is people cleaning their machines off, but before they do that, they copy their key documents onto a USB dongle. Clean the system, rebuild it, go through all the effort and plug the dongle back in, in order to copy their key documents across, and they are getting reinfected. That is what we are seeing with Conficker.

The first way is human breach. The second way is, a lot of the attacks aren't as a result of conscious attacks. You get something like Conficker or Torpig or one of the large botnets. They go out there and become like vacuum cleaners. They do their work in an automated process. We don't even know in many cases how systems got infected because they theoretically aren't

connected to the Internet. The mystery behind the botnet, what they are able to do is sit and look at the net result of the vacuum cleaner.

If you think about this, there are over 4 million machines currently infected, we think, with Conficker. We don't know where many of them are. We see a lot of them checking but not all of them. If someone behind that botnet wanted to, all they would have to do is perhaps use it as a giant search engine, basically say, show me any document or give me anything that has somewhere on the hard drive the word "nuclear," the word "blueprint," the word "trigger"; come back and find it for me. And all they have to do is sit back and wait. And over the course of a short period of time, those 4 million machines will look at their local drives and because, as we now know, many of them are actually sitting behind corporate firewalls, they will then examine all of the shared drives.

They are basically no different than the human sitting behind the computer that is infected. They will look at all the shared drives and examine all of the documents looking for that word. Very little work. Somewhere or other, out of maybe a token Congress IP address that maybe is even connected to a home modem, they will find the right set of documents, absorb those, send them back to the miscreant. And before we know it, you have the front page of the Wall Street Journal.

Mr. Weiner. Mr. Nojeim.

Mr. Nojeim. Just a couple of thoughts on this. One is that the bad guys in the fighter jet incident didn't get the best information. They didn't get the most sensitive information. That was on a separate system. And maybe one answer is that, at the time of procurement, the government better describes what has to be on a separate system that is not connected to the Internet. Procurement can be a very powerful tool in your war chest, if you will, for dealing with this problem.

Another thing to think about is that Raytheon is probably protecting its systems in the way that it thinks is most appropriate. It has got people whose job is to do that, and they are acting in the way they think is best. If the government believes that they should be acting in a different way, that additional security measures should be in place, then it should be up to the government to pay for those additional measures and the compensation could be through credits, could be through tax credits, or it could also be through a procurement provision so that you get extra money if you take extra steps.

Raytheon may not have protected that subsidiary in the same way that it protected other more sensitive systems. If that subsidiary needs to be protected, then maybe Raytheon doesn't get the contract. And if it does get the contract, maybe the contract also pays for such protections.

Mr. Weiner. Well, let me use that as a jumping-off point to some of the other threats; that some have been realized, some have

been unrealized. Can you talk a little bit about the danger of expanding the use of smart metering on our electric grid and the vulnerability that it extends to the notion that our electric grid might be vulnerable. Some of our colleagues on the Energy and Commerce Committee talk about empowering FERC to regulate these things further. Let's think about, not the challenges of the past, but let's think about some of the things that we might be vulnerable to.

The electric grid, as I understand it, by and large is not susceptible to a wide-scale attack because it is by and large not attached to the Internet in a large measure. Is it a source of concern to any members of the panel that our energy infrastructure might be susceptible to attack?

Mr. Kaminsky.

Mr. Kaminsky. There is an old joke from the NSA which is that all networks are connected; it is just a matter of how fast.

The energy industry is, on the one hand, completely different than the rest of technology and, on the other hand, no different at all. The 1990s saw a tremendous increase in our use of personal computing technologies and information technologies to, quite frankly, make work more efficient. The energy industry has not been immune from that.

One of the technologies that we have seen spreading, at least in recent design, has been an ability for the actual power meters to communicate with one another, for them to create a peer-to-peer

mesh as one meter speaks to another meter speaks to another meter. This technology is being done by people who, frankly, have not had to deal with the last 10 years of attacks. And on analysis, we have seen these meters actually able to be compromised remotely.

Where we are today with the energy industry, which is there are a lot of information systems, there is a lot of communication going on, there is a lot of gear that has trouble dealing with attackers today, and the only thing preventing pretty widespread attack is a lack of connectivity. With connectivity growing more and more, that is a temporary solve. The future, the future of widespread meter-to-meter communication based on the evidence that I have seen thus far does have me concerned. I would like to see more security for those meters.

Mr. Weiner. And are there steps that can be taken? Or is the technology of the smart grid too new to have best practices in this field?

Mr. Kaminsky. I think we know how to make secure devices. I don't think that that is the problem. I think the problem is that the devices, as they have been made, have not been made with that knowledge. So this would be the sort of thing that certification and independent evaluation would improve. We know how to do it. It is just the devices that have been built thus far, when we actually test them, they tend to fall over.

Mr. Weiner. Mr. Joffe.

Mr. Joffe. Thank you, Mr. Chairman.

One of the biggest problems that we face is that the Internet was never designed to do the things that it is doing today. There are control systems. There are systems that were never designed to be on the open Internet. But the open Internet, one of the great values is the fact that it allows you to communicate fairly cheaply and fairly easily with other computing devices.

Traditionally we used point-to-point connections. There are home-monitoring devices for people who have medical conditions that traditionally made use of a dial-up line and a dial-up modem to communicate that to a doctor's office or a hospital. And people realized very rapidly that if you made use of the Internet, the existing cable connection or DSL connection, you could have much faster, much more reliable connectivity. So the devices were moved on to the open Internet without understanding from a design point of view that, at that point, the security requirements were different.

The same thing is happening in the power industry. The power industry devices are being developed by not necessarily people who are in the power industry but people who are in the computing industry. So they develop devices and the device is then used by the power industry who are used to a closed network. But by its very nature, those home devices, the smart meters are going to have to rely on the open Internet. If they made use of the technology that the power industry was used to, which was point-to-point secured connections, or in fact the same techniques

that existed in the phone industry, there wouldn't be an issue. But there is a disconnect between them. Perhaps it is an educational issue where you have the wrong groups of people getting the right training.

As Dan had mentioned over there, we certainly know that security is an issue. But the people that build the devices, when they first design them, don't think about security first; they think about functionality first. And security is an afterthought, and it really shouldn't be. It should be embedded in the system.

RPTS DOTZLER

DCMN HERZFELD

[2:05 p.m.]

Mr. Weiner. Mr. Clinton.

Mr. Clinton. I agree with Mr. Kaminsky and Mr. Joffe both with regard to the fact that we can build more secure devices, they will be more expensive. But the point I want to add is we also have to operate these systems better.

The single biggest vulnerability that we have is not technical at all, it is the insider threat. Depending on which study you read, a third to half of the problems that we have are from people on the inside. These are people with keys to the technology. You can have the best technology in the world and the best security in the world, but if you just fired your IT guy, and he has put in a back door and he wants to come into your system, he will do it. That is 30 to 50 percent of the problems.

So we not only need to have good technology, we need to have incentives for people to use the technology. Again, this is a systemwide problem. It involves technology and human resources. It involves the economy and legal compliance. It involves a variety of things. It is not going to be fixed when somebody comes up with a new device.

Mr. Weiner. I want to talk about a couple more emerging threats, but before we do, I think we should touch on Conficker and what the state of play today is. It is exactly 1 month from

April 1st, the day Conficker was supposed to bite. There have been some things that have happened since then.

Who would be best to tell us what is the state of play with Conficker right now, whether it is still something people should be concerned about; and more troubling to a layman like myself, why is it that we literally have the code right there in front of us and it is such a vexing issue? What does it say? What is it doing? It seems to me there has to be at least someone who can read it, who is at least as smart as the guy who wrote it and say this thing is going to turn all microwaves on.

Mr. Kaminsky, can you give us as best you can in English language, and I know how difficult it is when you are dealing with these technical matters, where does it stand? Are we going to get up to Conficker.P? Tell us whether we are learning anything. Just give us a an update on where we are with that.

Mr. Kaminsky. Not a problem.

So it used to be that if someone wrote malicious software, they wrote it, it was out there. You could analyze it and tear it apart and figure out exactly what it is and what it is going to do. That is how things used to be.

The new generation of attacks are not about it does what it does, and it can't do anything more. The new generation of attacks, as Mr. Joffe said, are all very much about go back to the attacker and find out what would you like? Would you like me to search for documents? Would you like me to search for updates?

Would you like me to do anything you can possibly imagine?

That is what has made things difficult. Conficker is quite possibly the single most analyzed piece of software in the last 10 years; but we can't tell you everything it is going to do because we don't know because the attackers have not issued the commands or have not released the actual software in a general sense. It always goes and retrieves updates.

What made Conficker special, and what continues to make it special, is that it is actively being maintained and actively defending against the security community's effort. That does not mean that the security community has been lost and unable to do anything about it. We have had entire months of restricting Conficker's ability to update itself and manage itself. Through the public-private partnership of the Conficker Working Group, Conficker.B's entire update strategy was pretty tightly constrained. That is what ended up leading to their need to do an April 1 date. On April 1 they moved from the defenses that were successful in February and March to what we were unable to defend against in April. Technical terms: They moved from using 250 domain names a day, which we could register, to 50,000 domain names a day, which would be too difficult to block.

The state of play as it is today is we have very, very good tools for quickly scanning networks, identifying where Conficker is so that it can be quickly cleaned.

In order to actually get rid of Conficker, it was never, at

least in my perspective, about how do we pressure people into doing it, because pressure will only go so far. It was how do we make it less expensive, less difficult, less time-intensive to actually find this on networks.

Since a little bit before April 1, we have had fantastic tools for sweeping networks to find this. Now it just is a matter of people running those tools and cleaning it off their networks. There are still a few million nodes, but it is going down every day.

Mr. Weiner. You said that Conficker had the ability to go from 250 to 50,000 with an order. Can it keep ahead of you, or are you closing more doors than it is opening as it goes day by day?

Mr. Kaminsky. I will yield time to Mr. Joffe in a second, but I will say that I don't think that we will be able to stop the Conficker authors from sending updates. I do, however, think we will always be able to detect the Conficker-infected hosts. The Conficker authors are doing a lot to try to defend themselves from being found and caught.

The place where I think we have a sustainable advantage is it appears no matter what they do, we can always find them so we can determine we need to clear them.

Mr. Weiner. Let me ask you this: This being the new state of the art in these things, are other hackers and other troublemakers able to look at the Conficker virus and say, huh,

that is a cool way or a vexing way or a troublesome way for us to do our business in the future? Is there now out in the world this new model which is going to mean that the cat and mouse game is going to extend to other hackers who are going to use the same device?

Mr. Kaminsky. Honestly, I think that is a fair statement of the situation. One person has gone ahead and taken a lot of the worst practices, as opposed to best practices. Someone has actually demonstrated the worst practices for how you make something that doesn't just compromise a network today, but has a sustainable advantage, an update advantage. So I do thing that we will see more things of that type.

Mr. Joffe. Mr. Chairman, there is an interesting thing to note about Conficker and April 1. Most of the press saw April 1 as the day when Conficker would suddenly erupt. It was going to be like Y2K.

We knew already that we had been able to disassemble a fair amount of the software. We knew that April 1 represented one thing only, which was a change in the mechanism that Conficker was going to make use of.

Up until then, as Mr. Kaminsky mentioned, we had been able to control, or we thought we had been able to control, the spread of it. They changed the mechanism on April 1. But on April 7 and April 8, as you pointed out, it went to Conficker.E. Conficker.E did two things. The first thing it did was it updated Conficker.D

to a new mechanism for both spreading and communicating.

The second thing that it did was it enabled the download of another piece of software called Waledac, which is another form of malicious software. It enabled the downloading and installation of that, with some very interesting pieces to it. We don't know if the authors of Waledac are the same as the authors of Conficker, but it is very clear these are businessmen.

What Conficker seems to have done is downloaded Waledac, but done it for 2 weeks only. It is a very interesting process. It is almost as if the authors of Conficker rented the use of Conficker to the authors of Waledac to download Waledac, and after 2 weeks to delete it.

What we have been able to see from disassembling some of it, I think it is on May 3 or May 5, any installations of Waledac done by Conficker will be deleted. These people are very, very smart.

One of the things you asked: Don't we know who is behind it? Can't we interrupt it? The cryptography that is used in authenticating between the controller and these machines is so sophisticated; in fact, it didn't exist in the public. The particular thing that they are using, which is something called MD6, was actually submitted for the NIST competition for the new cryptography that will be sort of authorized for the government networks in 2013. They had used this 5 weeks after the submission from Ron Rivest. They had this in place and were using it. It uses a level of cryptography that, as far as we know in the

private world, there aren't enough computing cycles to be able to crack that in any way. It is being used to authenticate the updates.

So we can see the software, and we know the machines are infected. We can disinfect machines with a lot of effort. But what we cannot do is something people have asked: Isn't it simple to just act as if you are the controller and tell the worm to disable itself? The worm doesn't listen to us because we don't have the right signature. We don't have that crypto capability. They are doing a much better job with cryptography than we are.

Mr. Weiner. This is detective work, but is one of the emerging theories that what Conficker is is a delivery device for or a distribution device for other spammers or hackers or malware delivery? Like we will rent it to you. This is a great moving vehicle. For 2 weeks we will let you use it, and we are going to rent it to someone else for the next 2 weeks, and this is just the way that it gets around.

Mr. Kaminsky. It is all about monetization. It is about what can they do to make money from their millions and millions of infected nodes. In this case, they have made money by renting it to other people who have their own strategies.

The one thing I would really like the committee to be aware of is there is no reason what Conficker does to one company is the same thing that it does to another company. There is no reason what Conficker does to one computer is going to be the same as

what it does to another.

Mr. Weiner. It is an operating system?

Mr. Kaminsky. It pretty much is. It is a remote-control mechanism, and you can make an individual host -- one host do one thing and another do another. If that is the best way you can make money, go right ahead.

Mr. Weiner. I want to touch on one or two more potential horrors of the future, if not the present. One is the proliferation of mobile computing devices, cellular devices and wireless devices. Is there a reason why we haven't seen -- and maybe we have, but not in the same highly publicized way -- the wide-scale hacking of those devices? More computing is now going there. More communications are now going to handheld devices. Is this the next frontier of cyberwarfare? Have the cybersecurity threats already begun there? Are there reasons why it is less able to do because the technology is not as sophisticated as the network? Tell me if there is reason to believe that could be a vulnerability of the future.

Mr. Kaminsky. Mobile phones have become operating systems. They are quite a bit more complex than the computers we were using back in the 1990s.

The reason we have not seen attacks against them in significant count thus far is not because they are more secure. Any engineer who has actually taken a look I do not want to say has run away screaming, but has certainly found themselves

concerned.

The bad guys figure things out, but not immediately. We are basically enjoying something of a time lag in between when there is awareness of being a problem and when the hackers have built up the expertise to be able to exploit it. This will change over the years, mainly because at the end of the day, all of the things that we have managed to really clean up in operating systems and really fix up there, not all of them have made it into the mobile phones at this time. That is just the reality of things.

Mr. Weiner. Mr. Clinton, do you see the sense of the infrastructure limitations and the infrastructure vulnerabilities have been addressed? And I guess one reason it would be easier to protect is there is a finite number of wireless carriers with a finite number of technological pinch points.

Does it seem like the industry on the wireless side has taken these best practices and have done what you described as the need that 80 or 90 percent of the attacks can be protected if you make best practices?

Mr. Clinton. I really don't know if I can say that about the wireless industry; although generally, the major carriers do a pretty good job.

The core problem, though, as I understand it, not to delve too much in areas that Mr. Joffe and Mr. Kaminsky can answer better, the Internet is really inherently insecure. The core protocols that the Internet was built on were built 35 years ago.

Nobody was thinking about security. They are pretty much completely insecure at their core, which is why we have a patch system to solve these problems. As long as we are using these core protocols, which are basically the same protocols we are using on the mobile systems now, they are going to be insecure, too.

The only thing that I would add here is, I think we need to be careful by focusing just on kind of the high-profile issues like Conficker. I mean, I do a lot of speeches on this and sometimes go out and people say, I used to hear a lot about what you do. There was the Love Bug and Blaster; I don't hear about those thing, Conficker notwithstanding. I guess you guys solved that.

Of course, that is not the case at all. We have simply moved largely from an era -- an era, 5, 10 years ago -- 5 years ago, where the hackers were focused on large-scale public demonstrations of their ability, to an era where we are really focused on designer malware, and the goal is not to show what you can do, it is to steal money.

So we are really not sure how much stuff is out there. A lot of the problem with extortion is people are simply buying silence.

I would caution against just thinking, if we can solve Conficker kinds of things, we have solved this. I think it is harder than that.

Mr. Kaminsky. I wanted to clarify. There is at least one

mobile platform which has been paranoid for years and years, and I can say this because I know the years. The BlackBerry Research in Motion guys have worked for as long as I have known them to build a secure mobile platform. At least in that case, I can say people have looked at it, and their stuff is pretty good.

In fact, a lot of people kind of shrugged their shoulders at the "ObamaBerry" controversy. It is not like President Obama is the first person to ever be putting sensitive information into their BlackBerry.

Mr. Weiner. Mr. Kaminsky, you don't do any consulting work for BlackBerry, do you?

Mr. Kaminsky. No.

Mr. Weiner. I just wanted to make sure that I didn't get some Apple lobbyist complaining or anything.

Mr. Joffe.

Mr. Joffe. One thing to remember is that mobile devices used to be telephones, but they are now becoming much more of a computing platform. We go after Microsoft a lot in terms of their operating system. That is not necessarily where the problem is. It is the applications that people download and use on those devices.

We are beginning to see a move towards mobile payments, for example. One of the things that you have to be very careful about is when we look at the mobile payment applications, they sit on top of the operating system, on top of the phone. They have to be

looked at on their own because you can have the most secure platform you want. If you have an application that enables problems, it doesn't matter how good the operating system, the application itself would be insecure. That is where the problems, most of the problems that we have seen today, are coming from.

Don't think of it as a wireless device. It is nothing more than an existing computer, and it is just as vulnerable and has to be looked at very carefully in the same way we do on regular computing devices.

Mr. Weiner. Finally, on the challenges that we face, how do we know that a router manufactured in China doesn't have some listening ability built into it for Chinese Government officials? Or some computer chip that is made doesn't have a circuit switch that permits anything on that computer to be, with the right command, listened to or going to the right Website? How do we know that hacking in is not the issue, that building in might not be the issue?

Mr. Clinton, you are nodding the most, so why don't you start.

Mr. Clinton. We are very concerned with this problem. My organization started 3 years ago in conjunction with our partners, Carnegie Mellon, to take a look at exactly this problem. And basically, to put it in short form, I think we have come to the opinion that we need to learn how to build secure systems, understanding that some of the parts may be insecure.

We do think, and we have amended our statement, a fairly extensive additional piece of work that we did with Carnegie Mellon and Scott Borg at the Cyber Consequences Unit to move towards developing a framework so that we can put in an extended system of protections so that we can secure the IT supply chain, which is inherently globalized, is going to stay inherently globalized, and is going to be built in part by people who we don't know. They don't have a Social Security system in India. But we can put in, we think, by using a fairly systemic framework that we have tried to begin the articulation from in some of our additional comments, which we also supplied to Ms. Hathaway, a system where we can again change the economics so that we can make it in our best interest and our suppliers' best interest to understand that it is in their best interest to keep these systems truly supplied in a secure fashion, rather than allow them to be counterfeited or in some way hurt.

The one thing that I would say in addition to this is that we try to take a risk-management approach to this. So while we are very secure, we are very worried about the supply chain. This is a problem that is generally not a big problem, we think, for industry. The reason is it is usually easier and less costly if you are going to attack Bank of America to attack it through software or one of these traditional hacks. It is much harder and more difficult to do it through a supply-chain attack by putting something in the computer.

However, from the government's perspective, this is an extremely serious problem, because if a weapons system could be infected through a manufactured attack, you can't detect it. You don't get rid of it when the software is there. And the chances -- it is absolutely possible to put in a back door or a Trojan horse, a logic bomb that will stay there and not be activated until we launch a weapons system, and then the weapons system could either not work or turn around and go against us. So it is a very serious problem.

And if you are a nation state, and you are thinking of weapons of mass destruction, then a supply-chain attack could become very attractive to you, much more attractive to you than if you are just trying to steal credit card information.

Mr. Weiner. Let me pick up on something you said. It is easier not to do it on the supply chain. If you are a nation, if you are China, and you have a lot of manufacturing going on within your boundaries, and you have the ability to manipulate branch managers, could it also be a source for our counterefforts? One thing that we have that the rest of the world envies, we have the technological expertise, and we have a lot of the companies that manufacture these parts are within our walls. A lot of the chip manufacturers are U.S.-based companies. Why couldn't we install things on these chips to make them -- if we want to throw a switch, as we tiptoe into Mr. Nojeim's area of expertise, why don't we install a switch that goes into these routers that lets

us shut them down if they fall into the hands of Iran or a foreign power? I mean, it seems to me that it might actually be in the interest of the Chinese to be doing it to us and the interest of us to be doing it to the Chinese, no?

Mr. Clinton. On the weapons system, I think this is a big problem. In terms of the economic sort of stuff that we have been discussing here, the personal identifiable information sort of thing, one of the things that is a good thing about the globalized economy is that it is, frankly, not in China's interest to have lack of confidence on the Internet or to undermine the American economy. They are big investors in the American economy, so it is probably not so much in their interest to do that.

But if you think of it in a military sense, I would not be shocked to hear that we have people who are thinking about doing it offensively from our point of view. And certainly the expectation is that some of our opponents are thinking about doing it from their point of view, and that is why this kind of framework that we have suggested in our written testimony needs to be developed a lot more.

Mr. Weiner. Mr. Kaminsky, if I were to manufacture a router that had a piece of code or something built into it, and you had enough time to look at it, could you find it?

Mr. Kaminsky. It would be difficult. The reality is attacks at the level where the actual hardware has been corrupted in the first place are very, very difficult to find. The researchers

that Mr. Clinton spoke about at Carnegie Mellon University have done some preliminary work in attempting to detect these actual back doors, but at the level where it is baked into the circuitry, it is actually very difficult to find.

What is not difficult, however, is if you are the one doing the baking, you can pretty much make hardware that no matter what software is run on top, you can ultimately get an exploit into that operating system. So whatever operating system, whatever software, if you control the underlying hardware, you control the underlying logic, you can make a back door, and you will control that system.

Although it is true that we have a lot of very creative companies in the United States, the reality is a lot of the development of both hardware and indeed secure software happens outside the United States: China, India, Taiwan and so on. That is just the reality of the market as it is today.

Mr. Weiner. That sounds like a pretty frightening conclusion, so let's start to end the conversation today talking about the conflict that is going on now within the Obama administration about who should be in charge of this and what they should do.

It seems to me, Mr. Nojeim, that there does seem to be sufficient risk that we do want to give the tools to government to be able to -- if the risk grows too big too fast to critical infrastructure, to our country, to a weapons system that might be

used against us, there needs to be some check on the basic ethos of the Internet being a completely democratized, fairly loose-knit organization. Some have taken that argument to the extension of saying, all right, the supervisory/governing agency that should be at the top of the organizational chart of cybersecurity should be an intelligence or defense agency. What do you say?

Mr. Nojeim. We don't think that is the right approach, and there are a few reasons for that. And the Agency we are talking about is the National Security Agency, for the most part.

NSA has a role, I think, in protecting classified government systems, military systems. But it is not necessarily the case, and it probably isn't the case, that the NSA would be the best entity to protect a private system that is not in the classified realm, it is not in the defense realm.

Let me illustrate it this way. If I am Mr. Kaminsky, and I am working for Microsoft, I might know my systems better than anyone else would know them. The fact that the NSA has experience in penetrating other systems of foreign countries abroad doesn't necessarily make it the best entity to protect systems. Also, the NSA, it wears two hats. Those different roles tug in opposite directions in the cybersecurity area.

One, it is charged with breaking the codes of foreign governments and penetrating their systems, finding vulnerabilities. But if it was given a lead role in cybersecurity over private systems, that role would conflict with the need to

patch up systems that are being used in the United States. Sometimes it is exactly the same system.

So if NSA finds a vulnerability abroad --

Mr. Weiner. Meaning that you wouldn't want to tip off a foreign power that you have spotted this weakness because it might exist in our own?

Mr. Nojeim. Because they wear these two hats of finding the vulnerabilities, and then wanting to plug vulnerabilities in the same software that is on our systems, I think that is a very difficult thing for them to handle, and it probably makes them an inappropriate leader.

I should add that the head of the NSA at the RSA conference just a couple of weeks ago said, we don't want this lead role. We don't want to be doing that.

Mr. Weiner. I think there was some element of kabuki dance going on there.

I think we now understand that one of the reasons that this 60-day review has dragged on, and I don't think there has been an appointment of a chief technology officer, one of the reasons is that they are legitimately hung up on this. Any advice? Is there a need to have all of these disparate agencies that deal with cybersecurity? Is there a need to have them under one umbrella? There does seem to be consensus among folks who have looked at this that there is too much interagency back and forth, elbow throwing, and planning on who is responsible for what that doesn't

lend itself well to a true emergency response.

Do you have any advice to offer the President, Mr. Clinton?

Mr. Clinton. First of all, we generally stay away from this because, being a private-sector organization, we are always telling government, don't micromanage us. So we generally try to stay away from offering advice.

One of my board members would answer this metaphorically by saying if the cybersystem were a soldier on the battlefield with an open wound, and the Intelligence Community were the doctor, the Intelligence Community's approach to that would be to look into that wound and say, my, isn't that interesting, as opposed to, fix it. And we need people who are going to fix it, not try to exploit the vulnerability.

The one piece of advice that we would offer to the administration is regardless of whether you locate this person at the Department of Commerce, such as the Senate bill would suggest, or DHS, where it is supposedly now, or NSA, the important thing is not where it sits, but that you do have an individual or an organization, it could be a group of individuals, who have actual control from the government's perspective. That individual needs to have budgetary authority and the ability to oversee the other organizations. It can't be just kind of a figurehead position.

So it is less important to us where that person sits, although we tend to think it should be somewhere within the White House structure, but that person actually have the ability to do

the coordination. And we also think that government's first role here is to get government's house in order rather than try to figure out how they are going to deal with the private sector, which is why I think the model we have suggested, which is a collaborative model, is something that we would ask the committee to take a look at.

Mr. Kaminsky. There is a scenario that I think has been useful for explaining to people just the scale of problem that we have.

Consider a situation where a major top 10 Website is broken into, not directly but through their ad network. The advertising network is made to deliver an exploit for the Adobe Acrobat document software. The documents are loaded. They cause code execution on anyone who goes to that Web page. The code loads up a botnet. That botnet is used to do two things. First, it sends banking credentials from the infected host to the attacker. Second, it floods various Websites on the Internet with malicious traffic in a desire to force an extortionary attempt to be successful.

Whose fault is this? Is this the fault of the top 10 Website? Is it the fault of the ad network? Is it the fault of Adobe? Or is it the fault of Microsoft for writing the operating system, or the user for using the operating system? Is it the fault of the bank for having credentials at all? Is it the fault of the people who pay extortionary prices?

The fault is the bad guy. The bad guy caused this, and everybody else has a natural alliance against that bad guy.

The problems that we are trying to solve are smeared across company boundaries, individual boundaries; and, indeed, are smeared across the public-private boundary. I agree with what has been said earlier. I don't think that I am qualified to know who or where there should be authority, but there actually does need to be a coordinating authority across all of these disparate actors to guide the public-private partnership towards actually fixing the scale of problems that we face today.

Mr. Weiner. Mr. Joffe.

Mr. Joffe. Thank you, Mr. Chairman.

From my point of view, I, like Dan, come from the geek side of the house, and we don't play in politics and are down in the trenches. The only way we are going to solve this is by, first of all, acknowledging there is an issue, which is exactly what the White House has done with the 60-day review process, the other hearings that have been heard on the Hill, and this hearing. The fact that we are having this kind of hearing, this is remarkable to us in the technical world. Eight, nine years ago, none of us would have been seen up here unless we were involved in something else. So it is really important that there are hearings and we acknowledge there is a problem, and acknowledge that every one of us has a part to play in it: private industry, the government.

At the end of the day, someone has to make a decision when

there is a problem. But what we really have to do is make sure that we get together and talk about the problems and recognize them. As Dan said, we are all united against an enemy. The enemy may not be the bad guy who is trying to steal credentials. Nation states also represent problems for us. Nation state threats are just as large and just as damaging, if not more damaging. There are some organizations that don't care about the financial impact or being able to download plans for the Joint Strike Fighter; they want to seek the complete overthrow and maybe the complete destruction of the United States. And that matters as well.

We have to all work together with all of the stakeholders, folks on the technical side, folks on the policy side, people on the business side, to try and be able to recognize the problems, be able to find solutions, fund the solutions and build the solutions. As long as we are doing that, I think on the technical side we are happy. Who runs it doesn't really matter as long as it works. If it doesn't work, I am sure in a couple of years' times, there will be a new leader.

Mr. Weiner. Mr. Nojeim, it does matter, doesn't it?

Mr. Nojeim. I think it does ultimately, because where the work is located will have an impact on industry participation. And from our perspective, from what we have seen talking to key players in the industry is that one of the things that concerns them is that the program hasn't been transparent enough. If they share information, they don't know how it will be used and where

it goes next. So there is this natural tendency to hold back and to think about what happens next.

Where the program is located, where the operations are located impacts on transparency. And so far transparency has been lacking.

From our view, our perspective, it makes sense to have a coordinating body at the White House to do some policy work, to set budgets and do that kind of high-level thinking about this. But operations, they need to be at a lower level, I think. And DHS is a natural place for a lot of this work.

Mr. Weiner. Perhaps. I think there is the concern that this is generally part of a larger conversation about how you foster all that comes from the Internet, good and bad; how you make sure. As I said in my opening remarks, we have resisted the temptation to be heavy-handed plenty of times before. As the Internet emerged, and there were dirty pictures and hateful speech, these other types of things, sometimes we have gotten it right, and I think we got it wrong with gambling. I think to some degree we lurch back and forth, but we have basically defaulted to a position where we have tried to keep our hands off to the greatest extent possible.

I think the vulnerability is that you want to keep hands off, and you don't want to create a situation where you give too much authority to an agency that is used to collecting information and not used to disseminating it, but you want to have a situation

where we acknowledge that this does represent a bona fide natural security threat. To whom do you give the authority to do what? Do you give the President the authority to have an on/off switch?

You referred to this in your testimony.

Do you give the President or the NSA or the Commerce Department the authority to go ahead and start experimenting with a second tier of the Internet? These are things that we are going to use to plug in important things like the electric grid or our military secrets or the like.

I think one of the things that you four gentlemen have been helpful in shedding light on is that we really are going to have more of these headlines. We do need to be cautious. We go through our cycles in American civic life where we see a couple people bitten by sharks, and suddenly there is an explosion of shark bites going on. There have been tens of thousands of attacks that go on. Recently the New York City Police Department said that they get attacked about 70,000 times a day. And we have to make sure that we don't allow the tail to wag the dog here. We want to be thoughtful about it. I think your testimony has been instructive.

Also, I think it is pretty clear, whether it be the Commerce Department or some role for the FCC, we here on the Commerce Committee are committed and frankly have a history of dealing with these issues, looking at not only the security side, but the commerce side and the energy side. If you look at the things that

we have talked about today, the Internet itself, interstate commerce, energy issues, commerce issues and the like, I think that this is probably going to be the committee where a lot of these things are going to get discussed even further.

Before I recess, I just want to offer some thanks to people who have helped in addition to those of you who have testified. The record will remain open. If there is anything you would like to submit in written form, any questions and answers you would like to submit for the record, we will certainly be happy to take it.

I just want to thank Tiffany Guarascio of my staff; Amy Levine, Tim Powderly, Roger Sherman and Greg Guice of the committee staff; our friends on the Minority side; and all of my colleagues, as well as the Chairman Mr. Boucher, who has been very active and involved on many of these issues.

I thank you all for your testimony. This adjourns the hearing.

[Whereupon, at 2:41 p.m., the subcommittee was adjourned.]