

**HEARING TO RECEIVE A BRIEFING ON
CYBERSECURITY THREATS IN REVIEW OF
THE DEFENSE AUTHORIZATION REQUEST
FOR FISCAL YEAR 2014 AND THE FUTURE
YEARS DEFENSE PROGRAM**

TUESDAY, MARCH 19, 2013

U.S. SENATE,
SUBCOMMITTEE ON EMERGING
THREATS AND CAPABILITIES,
COMMITTEE ON ARMED SERVICES,
Washington, DC.

The subcommittee met, pursuant to notice, at 2:30 p.m. in room SR-222, Russell Senate Office Building, Senator Kay R. Hagan (chairman of the subcommittee) presiding.

Committee members present: Senators Hagan and Fischer.

Majority staff members present: Joseph M. Bryan, professional staff member; Richard W. Fieldhouse, professional staff member; Creighton Greene, professional staff member; Michael J. Kuiken, professional staff member; Thomas K. McConnell, professional staff member; and Robie I. Samanta Roy, professional staff member.

Minority staff members present: Thomas W. Goffus, professional staff member; Ambrose R. Hock, professional staff member; and Daniel A. Lerner, professional staff member.

Staff assistants present: Kathleen A. Kulenkampff, Bradley S. Watson, and Lauren M. Gillis.

Committee members' assistants present: Jeff Fatora, assistant to Senator Nelson; Christopher Cannon, assistant to Senator Hagan; Peter Schirtzinger, assistant to Senator Fischer; Craig Abele, assistant to Senator Graham; Joshua Hodges, assistant to Senator Vitter; and Charles Prosch, assistant to Senator Blunt.

**OPENING STATEMENT OF SENATOR KAY R. HAGAN,
CHAIRMAN**

Senator HAGAN. I would like to bring this Emerging Threats and Capabilities Subcommittee to order, and I want to welcome everybody to our first meeting of this congressional year. I really want to welcome Senator Deb Fischer as the ranking member of this subcommittee. I'm looking forward to working together with you, Senator Fischer. Last two years we certainly had a great working relationship with Senator Portman and I know we will, too. So thank you.

Today we meet to receive a briefing on cybersecurity threats. The Director of National Intelligence, James Clapper, recently testified

that cyber threats are for the first time leading the list of specific threats to our security. The purpose of this briefing will be to help us gain a better and deeper understanding of the nature, variety, and seriousness of the cyber threats to our National security, including their impacts on DOD's networks and operations.

Cyber threats can range from individual hackers to criminal groups stealing financial data to nation states with sophisticated intelligence-gathering disruptive or offensive capabilities that could steal classified information or harm our critical infrastructure and computer networks.

Before we get started, I do want to outline that we're going to hear from our witnesses in both this open session and in the closed session that will follow. We'll start with an unclassified briefing here. Then we will reconvene in the Office of Senate Security for the classified portion of today's hearing.

I do want to encourage members to certainly take the time to go over to the Capitol for the classified briefings. We're going to be briefed there by Ms. Stephanie O'Sullivan, the Principal Deputy Director of National Intelligence. She will brief us on a recent national intelligence estimate on cyber and will be focusing her remarks on cyber industrial espionage, why it's happening, what role it plays in the National policy of certain countries, who benefits, and so forth. This information I think is going to be very useful for all of us who are concerned about this matter in thinking about what we need to be doing next.

Then the other briefer, the testimony for the closed session, will be Lieutenant General John Davis, the Deputy Commander of U.S. Cyber Command. General Davis will brief us on the cyber threat as seen from Cyber Command, which has the responsibility to defend the Nation against cyber attacks that rise to the level of use of force or aggression, to defend the networks of the Department of Defense, and to carry out operations in cyber space in support of our combatant commands.

The unclassified briefing here we are about to receive from Kevin Mandia, who is the founder of the Mandiant Corporation, should require little in the way of introduction since it has certainly been widely reported in the media. The Mandiant Report is in many respects a summation and a confirmation of untold numbers of previous reports and developments. But it's also a unique achievement in the depth of the research and the scope of its documentation. The report is impressive too for its professionalism and lack of sensationalism, and it lets the facts speak for themselves.

This report has provided an important service for our public. Mandiant has produced an intelligence community-quality report without the benefit of the tools and authorities of our government and without the accompanying classification restrictions. So this is an unclassified report that was put together that is being presented to us.

So based on this report, there's simply nothing left in my mind for the public to doubt about the magnitude or relentless character of China's theft of American technology and other valuable business information.

Since this is a briefing format, I'm hoping we can be less formal than in a normal hearing and I want to encourage all of us to feel

free to ask questions or to seek clarifications during the presentation. So if we can just have an opportunity to ask questions and have a give and take, I think it will be a very useful hearing.

I want to conclude this portion of the briefing once again at 3:20 so that we can move to the Capitol for the closed portion.

Before I call on Mr. Mandiant, and thank you so much for your report and for being here, I wanted to ask Senator Fischer for any comments that you may wish to make.

STATEMENT OF SENATOR DEB FISCHER

Senator FISCHER. Thank you, Madam Chair. It's an honor to serve as ranking member of this committee with you. Thank you.

It's also an honor to look forward to the briefings that we will have today and throughout our time. Just last week, in testimony before the Senate Intelligence Committee Director of National Intelligence James Clapper stated the threat of cyber attack has become the top security threat facing the Nation, overtaking the threat of terrorism. This assessment makes clear the risks associated with the cyber domain and it is vitally important that the United States meet them head on.

Thus far, our defense-first policies have failed to deter hostile actors from attacking the United States in cyber space. I believe we must begin to assign accountability and impose consequences on those responsible for aggressive attacks on our systems. Little else will influence those nation states, terrorist organizations, and criminals who seek to hold our National security and our economy at risk through exploitation of the cyber domain.

The issues are complex, technical, and can at times seem very academic. But make no mistake, the consequences are real and potentially far-reaching.

I look forward to hearing from you, Mr. Mandia, at this portion of the hearing and I applaud you and your team for your work. I also look forward to our second panel, where we will receive the classified briefing. Thank you so much.

And thank you, Madam Chair.

Senator HAGAN. Thank you, Senator Fischer.

Mr. Mandia, once again thank you for being here. Thank you for the report that your company has presented, and we look forward to your presentation.

STATEMENT OF KEVIN MANDIA, CHIEF EXECUTIVE OFFICER, MANDIANT CORPORATION; ACCOMPANIED BY RICHARD BEJTLICH, CHIEF SECURITY OFFICER, MANDIANT CORPORATION

Mr. MANDIA. Sure, thank you. Madam Chairman, may I ask that I be joined by my colleague Richard Bejtlich, who will be offering some additional color and commentary to some of the details in the report that we presented to you?

Senator HAGAN. Certainly, and if he could say his name one more time for the record.

Mr. MANDIA. Sure. Richard Bejtlich, spelled B-e-j-t- l-i-c-h.

Senator HAGAN. Great.

Mr. MANDIA. Thank you, Richard.

I'd like to begin by just summarizing the report that Mandiant published, called "Exposing One of China's Cyber Espionage Units." It's important to note that we only exposed one advanced persistent threat group, or threat actor, that we refer to as APT-1. We exposed them based on a couple of reasons, one of those reasons being that we felt that their tools, tactics, and procedures had stagnated over the seven years that we've been responding to them. And we also just felt that in both the private and public sector that the general feeling or emotion was that it was time to bring this to a head. You could sense it and feel it.

So when we published this document it was very important to us that we showed that it wasn't just attacks that were coming out of China targeting the intellectual property of blue chip American and Western European countries that was targeting our IP. It was not just the Chinese, but actually an army unit in China.

The way we did that is we followed two threads of investigation. First, we followed the technical threads of doing 141 investigations where the malware being used or the computers being used to do the attacks were all synonymous with what we ended up grouping as APT-1. That's just an arbitrary name we at Mandiant assigned this group. As we responded to them, the TTP's or the fingerprints of this intrusion group married up at 141 different victim companies.

As we followed that technical thread, it brought us from computer to computer to computer, to basically a region in Shanghai. Anecdotally, we also started doing open source collections. What is in that region of China on Datong Road in the Pudong Region? We went with the nontechnical evidence and we learned of a Unit 61398, whose charter was to do computer network operations, where their people needed to speak English. And when I say computer network operations, by the way, I mean both computer network attack as well as computer network defend.

We had a location of this unit in the Pudong New Area of Shanghai on Datong Road, and just the nontechnical open source evidence brought us to the exact same location. So when we looked at the mission of APT-1, as we witnessed them stealing hundreds of terabytes of data from 141 companies, we witnessed them send fake emails speaking perfect English, we witnessed APT-1 use nearly 1,000 different computer systems over seven years, and then we witnessed them using IP addresses or computers in China, as well as the Chinese character set, and we married their location up with the mission and the scope and capabilities of this Unit 61398, it was absolutely the exact same place.

We had the same region, we had the same mission, we had the same scope of capabilities. So we felt that the Mandiant Report brings the reader and brings the public right up to the front door of this building. We couldn't fly people over there and run down the third floor taking photos, but there was little doubt that—either, there was only two options: APT Threat Group 1 that Mandiant has tracked for seven years is in fact Unit 61398; or, in one of the most closed societies in the world, where they monitor Internet use of your Gmail access or of your Yahoo searches or Google searches, that somehow the Chinese government is flat-out missing a seven-year campaign to pilfer millions and billions of documents from

hundreds of U.S. companies. It's just hard to fathom that that's a real alternative.

So we believe there's no valid conclusion other than a unit of the PLA has in fact been chartered to compromise the U.S. infrastructure and steal our intellectual property.

[The prepared statement of Mr. Mandia follows:]

Senator HAGAN. Impressive opening comments.

Let me just ask you a question on the scope. Multiple times in the report it stressed that even the massive activities that you've directly observed and catalogued is perhaps dwarfed by what you haven't seen, and that you judged that you have observed only a small fraction of what the APT-1 unit alone is doing. So can you expand on that?

Mr. MANDIA. Absolutely. Mandiant can only know the lowest bounds. So we reported on what was in plain view to Mandiant as we were hired by different victim organizations to respond. So our knowledge of APT Group 1 is what I call lateral. We were hired by Company A to respond to APT Group 1, then Company B, and then go on through—

Senator HAGAN. And that was 141 companies?

Mr. MANDIA. You bet, over time it was over 100 companies. And as we respond to each one and we see the same types of malware, the same modus operandi, the same fingerprints, I call them digital fingerprints, tracking it back to APT Group 1, we only know what we know. So all we've done is establish the lowest bounds. There could be thousands of companies that were compromised by APT Group 1 where Mandiant wasn't hired to respond and some other companies were.

Senator HAGAN. You also said the non-technical unit in the Pudong Region. Explain that again to me?

Mr. MANDIA. What I meant is the non-technical resource that we did at Mandiant brought us to the same place where the technical threads and technical evidence brought us to, a small quadrant of Shanghai.

Senator HAGAN. What is your non-technical?

Mr. MANDIA. Non-technical is open source collections, literally Googling for the Chinese character set of Unit 61398. We Googled to find this place, essentially.

Mr. BEJTLICH. Madam Chair, if I could add some color to that. One of the things we did was say: If you were to run an operation for seven years controlling thousands of computers, targeting at least hundreds or probably thousands of western companies, what would you need to do that? You would need a headquarters, you would need power, you would need telecommunications links, you would need infrastructure to support these people.

The activity started, at least from our perspective that we were able to see, in 2006, and in 2007 this building, 130,000 square feet. We got a copy of the document that ran the telecommunications line to this building saying: This is for Unit 61398, and if you don't know who they are, they're very important. They're the second bureau of the third department of the PLA, which does SIGINT, signals intelligence work.

So putting that all together, thinking if this unit existed what would it look like for them on the ground, and there it is. You have

the technical indicators, you have the non-technical indicators. It matched very well.

Senator HAGAN. Mr. Mandia, is it APT Unit 1?

Mr. MANDIA. Yes.

Senator HAGAN. It's a military intelligence unit, but it's marauding through this whole portion of the broad U.S. industrial base. Should we conclude that the Chinese government sees the theft of U.S. technology and know-how as a key element of their national security? And if so, is this because they see this theft as important to their economic growth, and is this economic growth as critical to their regime's stability?

Mr. MANDIA. Sure. I'll start with that and then pass it to Richard. From my experience, this is an extensive effort to pilfer intellectual property out of this country. It's been supported monetarily. It would take thousands of people, thousands of systems. You'd have to have your computer intruders—and those are normally very different people than the folks who benefit from these intrusions, meaning the folks who would read the emails or read the documents that have been pilfered. So the mere infrastructure alone and the time and duration and scope of this effort to steal our secrets has gone on for so long that there's a large amount of investment in it. Based on that investment, it's hard to conclude anything other than that there's an advantage being gained from that investment.

Mr. BEJTLICH. And if you look at what the Chinese have stated as far as their objectives and their different areas of priority, the number one concern for the PLA, or really for the party, is the preservation of the party in power. The number two concern is their economic development. That's why this theft is really a national security concern for them. It isn't an economic concern in the sense that the United States thinks of the economy as the basis for our military power. The Chinese think in terms of the economic and military being together as a national security concern.

So that's why we're a little skeptical that simply telling them to stop, they will stop, because they think this is the engine of growth, this is how we're going to provide jobs for our people, create world-leading brands. We're going to take this innovation from the West and put it into our own products and services. So they do see it as—it's probably the number two priority in their country.

Mr. MANDIA. One of the more interesting things that we did is as we were kind of doing open source collections, as I call it, Googling for evidence to some extent, we were finding things in China that—we're all familiar with Kentucky Fried Chicken. We were finding pictures of absolute replicas in China of Kentucky Fried Chicken, absolute replicas of Starbucks in China.

So as you see these things emerging from there, it's not a great leap to say that the computer intrusions to steal our IP are in fact to shortcut the R and D process. It's to shortcut learning what our marketing plans are, what our sales plans are, how much we charge for things, what our road map is for our products and technologies, how we build things, how we manufacture. All those materials have been taken and what we're starting to see is imitations of it popping up.

Senator HAGAN. Do you want to ask a question?

Senator FISCHER. Thank you, Madam Chair.

In your seven-year investigation, did you find other digital fingerprints out there? And I would imagine you did. To translate that into numbers, how many other groups like this do you think there are, and what's the damage in numbers to companies here in this country?

Mr. BEJTlich. Yes, ma'am. APT-1 is one of at least two dozen numbered groups that Mandiant tracks. Not all of them are Chinese, but many of them are because the Chinese are the most prolific perpetrators of this type of activity. APT-1 is one of those groups that is very broad in itself, but it's just one element of a large campaign. There are other teams working in other cities in other parts of the country that in some cases target other areas of the economy, but in other cases they interact.

We've done work for victims where we've seen two, three, up to five or six independent groups all competing to get access to information of a western company simultaneously. So there is—we wonder in our government about sort of deconfliction of priorities and different military units and such. The Chinese probably have that same concern because they have so many teams stealing data at the same time.

As far as impact, it's tough to—

Senator FISCHER. Could I just interrupt you?

Mr. BEJTlich. Yes, ma'am.

Senator FISCHER. Are you saying that most of them are army computers that are doing this?

Mr. BEJTlich. We can say with confidence that they're Chinese units. We don't know if they're necessarily military. There's a certain hierarchy in China—

Senator FISCHER. Would you say they're government?

Mr. BEJTlich. I would say they're at least government-sanctioned. We can't say for sure, these other units, whether they are uniform-wearing military or if they're contractors or if they're outsourced third parties.

The way to think about the Chinese effort is there's sort of three levels. There's patriotic hacking, there's state-backed militias that are closely affiliated with the universities, and then finally there are the military or military-associated units. APT-1 is an example of that, of that top level. But even then, APT-1 is not the top of the hierarchy. We do see other teams that have other capabilities.

Senator FISCHER. What's "patriotic hacking"?

Mr. BEJTlich. A patriotic hacker is someone who says they are sympathetic to China's sense of itself in the world, they believe that it is their duty to attack western individuals or companies, and the Chinese government tolerates that activity, whereas in the United States if we had someone doing that same sort of activity they would most likely be arrested.

Now, that's not to say the Chinese don't arrest hackers. If you are a hacker in China or Russia, for that matter, and you hack another citizen, they will arrest you and in some cases there's fairly significant consequences. So that's one of the ways that they say: Look, Chinese government, we arrest hackers; we don't like this. Well, they're arresting the ones who are hacking each other.

A good example of that is some hackers set up fake universities in China and were taking in tuition payments and putting out fake degrees. Well, this was all fake and the government ended up shutting it down.

You see the same dynamic in Russia. If you're a Russian hacking another Russian, you're going to go to jail. But if you're a Russian hacking an American, no problem.

Senator FISCHER. If you're a Chinese hacking an American, are you doing it to disrupt or are you doing it to gain information?

Mr. BEJTLICH. At the patriotic hacker level it's generally disruption. But what happens is that indicates that you have an interest and a capability, and you will be recruited into a university. And then if you show even more capability, you may end up in a military unit.

Senator FISCHER. I know you said the second type of hacker was university—you used some other term. What was that?

Mr. BEJTLICH. A militia. There is a—in our own country—I was in, Kevin and I were both in the military. It's a tough situation to have people who want to volunteer their service other than sort of the formal National Guard, Reserve, or active duty. In China you can be in a militia that's sort of a nebulous organization and be allowed to hack, and the more you hack the better. And the best of them are chosen to go into the military.

Mr. MANDIA. I'd like to expound a little bit on the characteristics of the advanced persistent threat hackers that we mostly see and make some generalities about the attacks we're seeing out of China. First and foremost, these attacks are against companies; they're not against individuals at the highest level. It's to steal corporate secrets, not individual secrets necessarily.

But the second thing that's insidious about these attacks is that they actually target humans, though, and they target human weakness. That's why there's been such a complication in fixing the problem. Just, hey, why don't we stop this? But it's more complex than stopping it, because the intrusions that APT-1 and other groups like them are doing are exploiting human weakness.

They do it by sending emails purporting to be from someone you know, and you get these emails, and you may get them to your mobile devices or to your laptop or your desktop at work, and they're soliciting you in pretty darn good English to click on a link, to see a Word document or a Powerpoint document or something that you would expect to get even. And just by clicking on that link or downloading or opening that attachment to that email, you're compromising yourself.

So they're leveraging human weaknesses and human vulnerability and trust to break into these organizations. But they are not targeting an individual at home. And it's very clear to us, after responding to Chinese intrusions for nearly 15 years now in my career, the attacks do follow a rule of engagement, but it's to steal IP, but I've never witnessed Chinese intruders, other than to breach the confidentiality of documents, I've never seen them change things. They're not changing the integrity of the data or making it unavailable intentionally, meaning they're not just shutting down machines and making it so that no one can connect to a machine.

So there has been rules of engagement during the 15 years that I've responded to these types of intruders. But make no mistake, they are targeting our IP. It's very obvious from the moment they break in that they're just pilfering every pdf, Word doc, Powerpoint doc, and email related to the projects or work that they're interested in.

Mr. BEJTICH. The one exception to the individual part is if you're an activist, a Tibetan activist, Falun Gong, those people are targeted incessantly. I met with an activist, a Tibetan activist, in Toronto yesterday and she described a ten-year campaign that her organization has been enduring. She has five years of evidence. She kept all these emails with all these malicious attachments like Kevin described.

They have had to rely on the human defense of, I have to make the decision, do I trust this email. It says that I'm a Tibetan, I need money, I'm going to be arrested. And so they've tried to figure that out as best they can. But outside of that, it is truly an espionage campaign like you've never seen.

Senator FISCHER. With businesses, how much would an American company spend on cyber security and what's the cost to consumers?

Mr. BEJTICH. Prior to working at Mandiant, I was the director of incident response at General Electric, and I had a budget of \$13.33 per employee per year to spend on my team of 40 people. With that budget—with 300,000 employees, you can do the math and figure out what the budget was—I was able to hold the line against that group.

What that will tell you is that unless you are a top company who can hire top talent and scale it out, scale those costs across the business, you can't afford the fences that will stop a Chinese military unit or a Russian unit or anyone else. It is truly a problem that is not—small and medium business, as an example, have an exceptionally difficult time dealing with this because they just can't support a team to hold back a military unit, or even a non-military unit that's very well skilled.

Mr. MANDIA. Thinking about the impact of it, I think we're on the early onset of determining the cost to the consumer, because there's a certain amount of time that needs to elapse to benefit from all the intellectual property that's been stolen. So I think we're on the front end of the power curve, learning from these intrusions to see what would be the consequences, how many jobs might we lose, how much competitive pricing pressure might we get from exports coming out of that region.

So I think we're still learning what was benefited from this enormous data theft, and we'll learn more over the next few years.

Senator FISCHER. Thank you.

Thank you, Madam Chair.

Senator HAGAN. I'm sure we've got a series of questions. On that topic about protecting, and from GE's perspective, or any customer, is it possible to keep the adversaries out of our networks by technical means alone? I mean, techniques such as firewalls, intrusion detection systems, antivirus products, and the like. Or is it necessary to actively monitor and constantly search for the intruders?

I ask this because it should affect the standards that the government is developing for critical infrastructure under the new cyber executive order. And if we need investigative processes as well as, quote, “good hygiene,” that needs to be included in the standards that NIST is developing. I’d love to hear both of your comments on that.

Mr. MANDIA. I’ll give you the high-level results. As we improve our security posture—and by the way, throughout my 20 years of doing cyber security, for the most part the security in this country is getting better. It’s been going in the right direction.

But as we do that, what we’re really doing is reducing the target area for the attacker. What’s lacking is that no matter what we do there’s always going to be a gap in our security. There’s always going to be technologies that are deployed faster than the means to secure them, and attackers will always take advantage of that.

But that doesn’t mean that we just give up. So we have to come up with a process where we mind the security gap that’s always going to exist. That’s one of the things that I’ve observed over the last 20 years is missing. We have this Maginot Line of preventive forces and we’ve established it, and we keep extending it and we keep narrowing the gap. But what we haven’t done a great job of necessarily is minding that gap, observing when are the bad guys getting around our defenses.

So that’s the high-level overture of where we’re at as a country. The gap is shrinking, but we’re not minding it as well as we could.

Mr. BEJTLICH. Madam Chair, the techniques we’ve seen in the highest-performing organizations, whether they’re the military or government or private corporations, people accept that you will be compromised, but you have to find it quickly, scope it effectively so you know the size of the breach, and then contain it. So you detect quickly, you respond quickly, and you contain quickly.

It’s not you deploy some type of technology and you assume it will keep the bad guy out. You have to say that’s going to fail, there’s going to be a security gap, like Kevin mentioned, and once that gap is exploited you react to it quickly.

Senator HAGAN. Back to the APT-1 unit, who receives the stolen information that has been hacked? Is it State-owned enterprises, private companies? And then what do they do with it? You know, I’ve got examples of companies in North Carolina that they were making like outdoor recreation equipment, small scale, and yet all of a sudden they got requests in for replacement parts because the parts that they people had purchased were not the original, it was not their design, it was not their product. And yet now they are being told that you’re responsible for this defect, when it had been hacked, it had been copied, and obviously used not the sturdy material that this company used.

Mr. MANDIA. I’ll answer first on that. From our perspective—and Richard’s going to have a different answer, but I have not—I don’t know where the information goes after the intrusion. As we respond to these incidents, our consultants are in plain view of so much stolen information we can’t possibly go through it all, nor do we. So I just want to leave you with the thought, it’s mind-boggling how many people it would take to go through terabytes and terabytes of information.

When you hear the word “terabyte,” most people don’t even know what the heck that is. But I can assure you, in your whole life you’re never going to read a terabyte of information. I don’t think you’ll ever get through it. So I can only conclude there are a lot of folks. If you want to go through all this information, there’s got to be a whole engine that can take this electronic information in, create what’s called an index for it so you can search it quickly, like a card catalogue, and you have to have the experts or the expertise that can benefit from it, because we’re seeing design documents that make no sense to anyone but the engineers who made them, and you have to have a proficiency and an expertise in very specific topic areas to take benefits of it.

But just from the volume we’ve seen, it would take an immense and costly effort, with lots of resources, to go through this data.

Mr. BEJTLICH. This is the great question for us. There’s either a great intel report or a Ph.D. or a book waiting in it. We try to think in terms of similar activities. Kevin talked about the size of what an activity like that might look like. We know that the Chinese employ tens of thousands, if not more, people who do nothing but censorship. These are people who watch Sina Weibo and these other chat technologies looking for key words, that they then remove; they delete these posts. So if the Chinese are willing to devote tens of thousands of people simply to monitor their own Internet usage, we could be sure that they would have plenty of resources to throw at going through these documents.

However, that clean case of get the information, get it to the right place, and then duplicate the product or service, that’s a tough one for a company like ours to make that. We don’t have people in China. We haven’t found people who are willing to talk about what they have seen. It would be great if there were some defectors or something who would give us some insight into that process.

Senator HAGAN. Let me talk about countering the proliferation of cyber weapons. Export controls and other methods to control the proliferation of dangerous weapons have been in place for decades. Cyber weapons have the potential to cause damage on the scale of weapons of mass destruction, and it’s common knowledge that there is a flourishing black market where one can buy or rent the cyber tools that can penetrate just about any computer system that’s in use today, as well as the infrastructure to carry out even large-scale operations, such as the large collection of compromised computers, commonly referred to as a botnet.

This cyber black market is a dangerous source of capabilities for terrorists, for criminals, and even nation states. Mr. Mandia, from your perspective as a security expert in the private sector, do you believe that it would be possible to develop a system of export controls for cyber weapons analogous to those that we have for other weapons? And do you think that such an idea is workable or even worth considering?

Mr. MANDIA. I can only offer you the perspective of a cyber security practitioner. I immediately went to the technical complications. No matter what we try to impose via legislation, the ability to surreptitiously communicate on the Internet exists. You can have an encrypted end point speak to an encrypted end point and it’s very hard to know the content of those communications.

The challenge of cyber weaponry is that it's highly scaleable. Someone with great expertise here at one site can just email it via an encrypted protocol to somebody with far less capability and technical wherewithal, and yet they have now been empowered to do a Stuxnet-like attack. So that's the challenge. It's almost like trying to put the cat back in the bag. There's encryption that's free, publicly available. There are anonymization techniques that you use on the Internet—

Senator HAGAN. There is what now?

Mr. MANDIA. Anonymization techniques. That's a big word for it's hard to pierce anonymity on the Internet sometimes when people are trying to remain anonymous.

So because of encryption and the anonymity on the Internet, cyber weapons could be traded. I think it would probably be easier to catch any money that might pass hands, quite frankly, because you can trade the actual electronic bits and bytes surreptitiously.

Mr. BEJTLICH. Madam Chair, I was at a conference in Toronto where this very subject came up. We had—I'm neither a lawyer nor an export control expert, but it was made apparent to us that there are laws in place that cover preventing the export of items of torture or these sorts of—from the seventies, where the United States is prohibited from exporting this sort of stuff.

I think if you define certain types of tools as being used for that type of behavior—in other words, some type of software that's used to conduct surveillance on an activist in Syria, and that person is arrested by virtue of the government buying that tool, the Syrian government buying that tool, or something to that effect, I think that we have the legal framework in place to control that sort of export. I'd like to see that happen. I think it's not an easy case, but I think you can make a good case that we should not be exporting software that's then used for that sort of behavior.

If you're looking at other types of software, though, this same tool that can be used to break into a network I can use to test my network to make sure that a bad guy can't break into my own company. So that becomes very difficult. Sometimes it comes down to what the marketing is. Is this tool marketed for nefarious purposes or is it marketed for legitimate purposes to try to improve your own security?

One of the best ways we know to find out if you're vulnerable, one is to check to see if intruders are there; and then the second one is to simulate an intruder. If an intruder—if you simulate the intruder and you can't get access to a certain computer, then you know you're doing pretty well. To do that sort of work, you need that tool.

So that's where it becomes difficult to try to regulate that sort of software. But I do think there's room to sort of carve out the clearly malicious software from the software that has a legitimate purpose.

Senator HAGAN. One more. Mr. Mandia, your company's report and other such reporting from the private sector I think is very helpful for educating the American people about this threat in cyber space. It's also very helpful, I believe, in getting China's attention to this matter and letting them know that we know per-

fectly well what they are doing. We have certainly seen that in the last several weeks since your study came out.

I realize that you sacrifice something when you reveal what you know. China probably will now change some aspects of how they operate and this may make it harder for you to track them in the future. But it seems to me that, as you say, you just can't prevent and deter a crime if all we do is observe the criminals to gather the intelligence. We can't just sit and watch China stealing this property.

If your company was able to collect all of this information on an unclassified basis, it seems to me that the government could also make such releases without undue damage to source and methods. What are your views on the gain versus loss calculation?

Mr. MANDIA. I think that's a great question, and it becomes is there a network-enabling effect of sharing intelligence? That's pretty complex. I can share this with you. Mandiant, when we obtain intelligence we do it what I call laterally. We have to go from company to company to company to company. I think that the government is uniquely positioned at the top of the pyramid where they can get information from the bottom, which means they will have a top-down view that should be and is more comprehensive in scope than what Mandiant can provide going laterally.

So the government is uniquely positioned to know more, have better intelligence, and be able to make that actionable should they be able to share it with prospective victims or imminent victims, meaning the intel showing that something's about to happen or is pending.

I think that the criteria that go into that decision, does the gains outweigh the negative effects, I feel that once you have the capabilities to observe and orient on an attacker, you actually gain intelligence sometimes when you kind of deal the attacker what I call the Mike Tyson upper cut, where you change their—if you change their behaviors, but you're able to swivel and observe and orient quickly again, to some extent you're now in charge of the game that you're being played.

So I think there's a tremendous advantage at times to share the intelligence, but you also need to be postured to swivel for where they go next. The nice thing about it is as we take control of the game and start pushing the mouse into other directions, we can start predicting what they're going to do. I think the minute we're predicting what their reactions will be, we're starting to win at the game.

Senator HAGAN. Interesting.

Senator FISCHER.

Senator FISCHER. Thank you, Madam Chair.

The Chinese premier has made comments since your report has been released. Have you seen those?

Mr. BEJTICH. Yes, I have.

Senator FISCHER. "I think we shouldn't make groundless accusations against each other and spend more time doing practical things that will contribute to cyber security."

Also, the foreign minister said: "Anyone who tries to fabricate or piece together a sensational story to serve a political motive will

not be able to blacken the name of others nor whitewash themselves.”

What’s your response to that?

Mr. BEJTLICH. The main response that I’ve seen from the Chinese that I find curious is that they claim that our attribution is based on IP addresses, when clearly it’s not. IP addresses are but one component. And even an IP address has value when it’s the same IP address, the number that’s assigned to a computer is the same for seven years. I mean, that tells you something.

But what’s funny is that they say you can’t use that measurement to assign attribution, and yet in the very next breath they turn around and say: Well, American IP addresses are attacking us. So they think that somehow it’s logical to deny our part of the argument, but then to use it for their purposes.

I think they were stunned by this. I’m waiting for them to write a report. I just don’t know if they’ll be able to do it, because I feel that they might not have the—they may have some abilities, but to be thorough and professional and just to lay the facts out, I don’t know if they’re in a position to do that. They’ve had a very—not a very sophisticated response if all they can do are talk about IP addresses that were seen attacking.

Because our report isn’t an attack report and other reports that we’ve seen come out since then, those are all attack reports. Our report’s an intrusion report. This shows companies were broken into and data was stolen. 356 days on average an intruder was inside a company, terabytes of data stolen. One company was compromised for almost five years. That’s much, much different than seeing an attack that gets bounced off of someone’s firewall or another technical defense.

Mr. MANDIA. I think there’s always—you run the risk when you deny, deny, deny that overwhelming facts come to the public light. I think that over time we should see a tapering of the denials coming out of China on this. There is no doubt when we released this report one of the factors that brought me to the cusp of let’s release it was the response to the New York Times article that came out in February. The New York Times said: Hey, we were compromised by the Chinese and here’s what they did. And the Chinese once again came back with the statement: It’s irresponsible and unprofessional to accuse us. I went: You know, let’s accuse them.

I think that the more they deny something, the more likely we’ll entertain sharing more information.

Senator FISCHER. Have you seen a change in the APT Group 1’s practices since your report’s been released?

Mr. BEJTLICH. Yes, we have. We’ve seen them try to clean up some of their online presence. We’ve seen them—

Senator FISCHER. How would they do that?

Mr. BEJTLICH. Well, some of the public databases that we or other security researchers can use to identify them, they’ve changed some of those entries. But what’s interesting about that is by noticing the entries were changed it revealed something about who did it.

We’ve seen them change some of their infrastructure, so the computers they were using to hop from China to the West, some of that

has been changed. But we've been able to keep up with them on that perspective as well.

I think what's also fascinating is that since the report was published there's been at least 25, upwards of 30, derivative either efforts or reports that built on our own research. You may have seen a wonderful story in the L.A. Times where some of their on-the-ground reporters found the blog of what apparently is one of the members of these units, where he described the drudgery of working in this unit over the period of several years, how he disliked the fact that it was away from the main city, which this headquarters is often in not a very interesting part of town. He missed his girlfriend. He felt like he was working in a prison because he would work from 8:00 a.m. until 8:00 p.m.

It was very interesting to get a firsthand account from someone who was one of these, self-identified as a Chinese military hacker, in uniform and so forth. So we hope that by bringing the report forward we'll get more and more of this sort of derivative analysis that gives even more detail.

Senator FISCHER. Do you think that with these hackers being able to have access to American companies, can they also shut them down? Does that access give them the ability to shut them down?

Mr. MANDIA. Yes, as we—

Senator FISCHER. But they choose not to at this point?

Mr. MANDIA. Yes. We've responded to APT-1 over 100 times, and these other APT groups hundreds and hundreds of times, and we have never seen what I would describe as destructive activities. We may see every once in a while they'll clear a log file to erase some evidence. So I think that the tools they have in place a lot of the times, not all of them, but some of them do have the access required to do a shutdown. Some of them even have in their back doors, that surreptitious way to access a machine, the ability to shut it down.

Haven't seen it happen yet and I don't anticipate that the Chinese will be a threat that starts shutting down machines. I think other cyber threats will emerge before they do, meaning the Chinese, before they take advantage of that capability.

Senator FISCHER. You mentioned back doors. Are back doors set up in the manufacturing of computers or software? Is that a point we need to be concerned about at the very beginning of where we get our computers?

Mr. BEJTICH. I would be more concerned with just overall software quality. To the extent software is not very well coded and there are vulnerabilities that make it possible for someone to take over that computer, that's a concern. But when we write about back doors in our report, we're talking about methods of access that the Chinese have either introduced or stolen. They start out with using their own tools, but then they evolve to using the tools that you have. In other words, if you connect via a VPN as a user so that you can work from home, that's what they steal, so that now it looks like they're a normal user.

So half of the time when we work these intrusions, eventually they look just like a normal user. And that's what makes it very

difficult for a company to find them and why they're able to stay active for so many years.

Mr. MANDIA. My opinion is we have to be mindful of our supply chain. That's what we're really talking about. I think the minute we turn our backs on that, that obviously that'll be a way to exploit our country again. So traditionally, though, it's so easy to break in right now by exploiting human trust and putting the traditional back doors that we've seen for 20 years on systems. That's what people do today.

But if we ignore the supply chain down to the chip, over time that might sneak up on us and be a challenge. I have not personally—well, that's not true. Throughout my career there have been publicized cases of software having what's called "Easter eggs" in it or some kind of unwanted surprise in it. But I think that's a future problem, but if we ignore it it'll come faster.

Mr. BEJTLICH. We did document a case in our latest M-Trends report that was released this last month where a hard target who had been experiencing this problem for many years found that they were being attacked by a partner and by an outsourced IT supplier who was compromised. So this is the trend now, that if your primary target is hard enough you come in through others. It doesn't necessarily mean you come in through the actual laptop that you buy or that sort of thing, but you come in through partner organizations. And as those harden, like Kevin said, then I think the true supply chain will be the issue.

Senator FISCHER. My last question would be, how do we deter them?

Mr. BEJTLICH. I think signaling is one, one way. I don't have privy to how the decision was made, but when I saw that General Alexander was talking about offense explicitly I think that was a signal. I think that stating that we see you and that this is not acceptable is proper as well.

We need them to scale back their activity to meet the level that we see from other adversaries such as the Russians. There's a sense with the Russians that there are certain lines we don't cross and certain activity stays at a certain level. With the Chinese, they take the gloves off and they go after far too many industries who simply cannot defend themselves.

Mr. MANDIA. My answer is at a higher level of abstraction. There's going to be technical solutions and non-technical solutions, and neither one in and of itself is going to be 100 percent successful. So we'll probably never get to perfection here, because I can't think of one technical way to prevent all attacks. Technology is just evolving too quickly. But I believe that technology is advancing. We're limiting the consequences of intrusions far better today than five years ago.

The up side of a lot of the attacks we've seen, if you want to think of it that way, is we're much better postured in many organizations to withstand the next generation attacks that may come without the code of ethics we've witnessed for 15 years out of Russia and China. It may come from Iran, may come from a non-nation state or a terrorist group. So that the security has come up based on a lot of these activities, but it's the non-technical solutions that I just don't have the proficiency or expertise to advise you on. But

you can't get there with just tech. Technology is not—there's not going to be a silver bullet, so we're going to have to have a diplomatic as well as technology to approach the problem.

Senator FISCHER. Thank you.

Thank you, Madam Chair.

Senator HAGAN. Before we close, do you think that the political leadership in China has been told by their cyber forces that what they've been doing was undetectable? And then would there be some—if so, would there be some pretty tough questions going on right now from the political leaders to their cyber forces?

Mr. BEJTICH. I'm loathe to speculate, but my guess is they didn't say that it was undetectable, but they would have said it's tolerated. And now we're signaling to them that it's not tolerated.

Senator HAGAN. Then I have one more, sort of final wrap-up question. That is—and this is what I ask all the generals that I talk to on this issue, too, and other companies. Tell me about your employee base as far as the educational component of STEM education in our country for the kind of people that you need to be hiring to do this kind of work?

I know that science, technology, engineering, and math is certainly an area of focus that we in our country have got to be paying a lot more attention to, so that we can be sure that we have the people within our military, within our government, within our private industries, within the companies that come to you to help them from an intrusion standpoint. Can you talk a little bit about from what you see from your perspective?

Mr. BEJTICH. Hiring is our biggest challenge. We struggle to find the types of people that will meet our needs. But there are good signs. 15 years ago when I started, when Kevin started, there weren't programs that you could attend to learn how to defend yourself. There were computer science programs, but there were not computer security programs. So we're seeing more of that, which is good.

I still think there's a disconnect between the theory that's taught and then what you really need to do on the job. It would be—both Kevin and I are authors. We write books that people use in school and they learn how to do the real deal as opposed to learning about cryptography, which may or may not be helpful.

So I think we're getting there. I think that the fact that in the military and in the FBI and some other places there are career paths now—that's what's difficult. When you take someone in uniform and they don't have a career path to stay doing this work, that's tough. I think that's changed now and that's encouraging. Even having a Cyber Command I think as a home for people like that is very encouraging.

But there's still plenty more to do. The fact that the Chinese can muster so many people and encourage so many people to learn how to hack and in the United States we still have trouble with that—not that I'm encouraging anyone to learn how to hack necessarily, but to do it for educational purposes and then do it as a job. This is the greatest job in the world as far as I'm concerned and I would love to have more people banging down our doors to try to do it with us.

Mr. MANDIA. The bottom line is there is a shortage, and we're doing what many other companies are doing, supporting local colleges, supporting students, trying to get more people into it. I always believe wherever money goes crime follows. Pretty soon we'll all be paying for things with our Android phones and our iPhones, and the minute we're doing all-digital money we're going to see more digital crime and we're going to need more expertise, and we need to build technology that expands at the scope of those expertises as well.

So we're in an interesting time, but we're trying to make more—as I say, we're trying to groom more cyber pilots to help us.

Senator HAGAN. Well, we certainly do, one, thank you for your report. Thank you for your company's making this public and sharing it with us, and we certainly do thank you for your testimony at this hearing today.

And we will adjourn. Thank you.

[Whereupon, at 3:20 p.m., the subcommittee adjourned.]