AMERICAN ENTERPRISE INSTITUTE

THE CHINESE CYBERTHREAT: CHALLENGES AND SOLUTIONS

DISCUSSION:
SENATOR CORY GARDNER (R-CO), CHAIRMAN, SUBCOMMITTEE ON EAST ASIA, THE PACIFIC, AND INTERNATIONAL CYBERSECURITY POLICY, SENATE FOREIGN RELATIONS COMMITTEE

MODERATOR:
MACKENZIE EAGLEN, AEI

PANELISTS:
RICHARD BEJTLICH, FIREEYE;
PAUL TIAO, HUNTON & WILLIAMS LLP

MODERATOR:
SHANE TEWS, AEI

12:15 PM – 2:00 PM
WEDNESDAY, JULY 22, 2015


TRANSCRIPT PROVIDED BY
DC TRANSCRIPTION – WWW.DCTMR.COM
MACKENZIE EAGLEN: Welcome to AEI. My name is Mackenzie Eaglen. I’m a resident scholar here, working on defense and military, national security issues.

It’s a pleasure to welcome you today to our event on challenges and solutions to the Chinese cyber threat, something – it’s a big topic. It’s an ambitious topic and so I’m really pleased that we’re going to have a two-part event. We’ll get you out on time, right at 2:00 p.m. We’re going to begin our conversation this afternoon, our friendly discussion with Senator Corey Gardner from Colorado for just about a half hour. And then we’re going to pivot to our expert panel, although you could certainly be included in the expert group afterwards and continue the discussion with you guys. Please get up and get more food and drinks as convenient. We’ll just keep this simple and easy.

So you’re probably here because you already know Senator Gardner, but let me just give you a brief example of his commitment to this issue and why we’re so happy you’re here today to talk about it. So he’s the chairman of the East Asia and Cyber Security Subcommittee in the Senate. He’s a former member of the House of Representatives as well, elected in 2010.

And, back in May, at your cybersecurity hearing, it was on establishing a global framework for behavior in cyberspace, something I think – I hope we can talk a little bit about today. Not just norms, but all the way up to red lines and acceptable standards of behavior and codes of conduct. And I believe when the hearing was over, you were the last standing and only one other colleague joined you, but I applaud your tireless commitment to the issue because it is that important, even when no one shows up.

So Coloradan born and raised, family, fifth generation, committed to energy security, agriculture, everything that matters in the heartland, but I will speak to him today about the other issue near and dear to his heart and also one that he spent a lot of time working on in the Senate, including as part of the Foreign Relations Committee.

So, Senator, I just want to start talking. Welcome. Thanks for coming to AEI. We’re going to begin our conversation and we’re going to open it up to the audience for Q and A and you’ll have a moment to ask him a question yourself if you can.

So everyone’s been following the story. Really I think the Target hack really woke up America to sort of the threat of our personal information at risk. But then there was Home Depot and then there was JPMorgan and then there was a health care company, we all know we put our Social Security numbers and everything health care form related.

But then there was the Sony hack that – right before the midterm elections. And when you talked to Pentagon officials, they say that was sort of a turning point in cyber
for government, for the U.S. government and for the Pentagon even in particular. And I kept thinking, well, why Sony and not other events, because there had been so many.

And, of course, now, that’s old news and now we’re talking about the Office of Personnel Management records breach and pretty much anyone who’s ever applied for security clearance, although we have to polygraph information and answers, people who applied before there were even electronic of this so back in the ’80s apparently and affecting a much wider breadth of information than even the other ones previously.

So Americans are attuned to this threat and it’s very real to them in their lives, whether you live in Colorado or live here in Washington. When I listened to the intelligence community director talk about the greatest threats to America, now we hear different answers from different people – cyber, espionage, theft, intellectual property, etcetera – but just the potential for destructive damage, you could put any angle on the cyber but cyber was a threat even before the Islamic state, Russia, anything else.

At the same hearing, the director of National Intelligence said, and we have basically no U.S. cyber deterrence. So, basically, we’re not stopping anybody from attacking us or we’re not – we don’t have a credible response, a plan to proceed, whether it is Sony or Target or the U.S. government’s OPM. And so, of course, everybody just keeps stealing. But yet, if these were armed robbers wearing masks with guns, and they walked into the OPM and then stolen the paper data and driven away in an armored car, we’d try to put them in jail. So what do we do about it?

SENATOR COREY GARDNER (R-CO): It’s a great question, Mackenzie. Thank you for having me today and, to AEI, thanks for hosting this very important conversation.

I think just to highlight how important this issue really is, the first hearing, as you mentioned, that I co-chaired as chairman of the East Asia and Pacific Subcommittee was on cyber issues. And we were able to add cyber, a cyber component to the Foreign Relations Committee.

And, a little bit later on in the conversation, perhaps we’ll talk about how I think I now may have become part of the problem by adding cybersecurity to yet another committee in Congress and how we can address sort of the multiple layers of people involved in cyber and how we can do a better job of focusing on cyber.

But today, I think it’s some important news that kind of will shape the discussion I think going forward on OPM, on China, on our strategy going forward as we seek an overall cybersecurity strategy, a cyber strategy, cyber framework.

And today, in the Washington Post, it was announced that the administration will not name names when it comes to who was involved with OPM. And I guess I – just out of curiosity, how many people have received a letter from OPM? Raise your hand. How
many people have received a letter? So there are people in this room who have received the same letter that I have about the OPM hack, and this creates a significant concern.

The article today in the paper talks about how the administration will not be naming, as many press outlets already have, China as responsible for the OPM breach. But I think that creates a really important dialogue that we have to have a country, as we search for a cyber strategy. You know, the White House is basing our cyber strategy off of a 2011 framework document. There hasn’t been a serious review of that in the four years since that was put forward.

As chairman of the subcommittee, I not only held the first hearing on cybersecurity, but also during the State Department reauthorization mark-up that we held several weeks ago was able to put into that bill a requirement that the State Department issue a cyber strategy. Believe it or not, the State Department doesn’t necessarily have a publicly available stated cyber strategy that provides the rules of the road in a public way to acknowledge what our norms are when it comes to cyber strategy at the State Department.

So it would require that to be development and put forward within 90 days. It was a classified part of it but also a public part of it that we need to show to the world what we are doing to protect these very important pieces of information.

The other part we have to acknowledge is I think it’s important that we be public, that we be very public about who is doing what when it comes to our national security. And I believe the OPM breach is very much a part of that conversation over national security.

If you look at other actors, other leaders around the globe, they have called the United States to task when they believe that something has occurred that they disagreed with or perhaps they were concerned about activities of the United States. What did they do? They called in the United States ambassador, they reached out to very – the most senior, high-level administration officials that you can get and called them to task. We are yet to do that on OPM. In fact, we’re not even really sure what we – what we have that is highly classified that ought to be better protected we know now should have been protected.

So I think the fact that we’re not willing to name names is a grave mistake. I think the fact that we have no strategy is a mistake that we are attempting to fix. And I think the fact that we have to embark on a conversation about what punitive measures must be taken by this government, whether it’s actually following through on the April executive order when it comes to sanctions, or whether it’s continued indictments that we’ve seen just recently with the five PLA officials.

MS. EAGLEN: And I was going to bring up the sanctions – I’m sorry – the indictments, the five people. And you just also mentioned the sanctions as well, targeted, limited, but still a step, I guess, in the right direction. But I see these as two tactical pieces
as what’s missing in this sort of larger strategy, cyber defensive total strategy, if that makes sense, something that I know that you’re thinking about.

So would the State Department document that you’re requiring – would that be the lead for all U.S. government or is that just the State Department? Because then I worry about all the siloing and stove-piping and the states are going to be different than defense or IC?

SEN. GARDNER: In conversations that we’ve had with both the public sector and the private sector – let’s take a conversation we had recently with the private sector. One company realized several years ago that they weren’t doing the best they could in protecting their trustworthiness – issues related to privacy, issues related to possible breaches, issues related to security.

And so, this particular company took one representative from each different department and put them on a trustworthiness committee where they tried to direct the cybersecurity efforts and cyber strategy as a private sector company, what they can do to coordinate conversations across the various parts, segments, business departments.

If you look what’s happening in China, if you look what’s happening in China, President Xi has created a cyber committee that President Xi is the head of, where it’s going to take several years for the consolidation of this committee to take over all the angles of cyber that may be in the various parts of China and the government. But that’s the level of seriousness that China has taken in the issue of cyber strategy, cybersecurity. We don’t seem to have that same level of seriousness within this administration.

And so how do we take the language that we’ve put in the State Department to force through a cyber strategy? How do we make sure that we elevate this – I think it’s important that we publicly talk about who is doing what to this country from a cyberattack – from a cybersecurity point of view because if we don’t, then what’s to stop them? What’s to – what’s to change their minds on whether this is acceptable behavior or not?

So the rules of the road, the norms that we have to create and develop as a country, that we can get other nations, allies and responsible governments to adhere to so that they know that this is unacceptable behavior.

We sent a letter to the administration a couple of weeks ago demanding that they go public – very public – with the people responsible for these acts. And so we get this strategy in place, we codify the executive orders, and we actually start following through. I think these are all important steps. And then make sure that we are bringing up the issue of cybersecurity when we have the opportunities to do so.

As it relates specifically to China, we recently had the strategic and economic dialogues at the end of June and we had an opportunity to bring up the issue of the OPM hacks, the issue of – cyber issues. And of the 127 points of agreement that were reached
out of the strategic and economic dialogue, some of those 127 points included wildlife trafficking agreements and volcano studies; not one of them addressed the issue of cyber.

MS. EAGLEN: That is – that’s really disturbing because it wasn’t until I started looking at the DNI’s public assessment list that he provides to you and to all the American people, then I was having a conversation with Congressman Randy Forbes of Virginia, former colleague of yours, and I said, well, the intelligence community says the single largest threat confronting the U.S. government right now is cyber, particularly cyberespionage, including – that’s basically the theft of data, whether that’s for profit or to win some kind of Cold War intelligence standoff with the U.S. or to possibly help in a potential future conflict, who knows? But theft is theft. And if you have no deterrent, Willie Sutton is going to keep robbing the bank. It’s that simple. And we don’t have any for cyber.

But when I was talking to Congressman Forbes, what he said was – I was at a hearing with the attorney general. It was like pulling teeth. I had to get permission from the chairman – you know how there’s time limits on the Q&A when you’re in these types of hearings, and he said, which country on earth is the single largest perpetrator of the threat of cyber – of the act of cyberespionage? Truly 20 minutes went by, the attorney general is looking to the chairman like, aren’t you going to call this off? And the chairman said, I’m going to let this go until you answer the question. And the answer was China.

So if the single biggest threat is espionage and the single largest perpetrator of that threat is China, we have a problem. And we aren’t –

SEN. GARDNER: We ought to name that problem.

MS. EAGLEN: We have to name that problem.

SEN. GARDNER: We ought to do something about it.

MS. EAGLEN: And we have to link these things. Exactly. And I’m even more disturbed now that there wasn’t a cyber point in that document. So I want to get then to that – to the seeming mismatch here of commercial cyber challenges and breaches and threats and government or traditional cyber.

And so we seem to be reacting government – our government seems to be reacting pretty strongly when the private sector is breached, but not defending our own networks, which the government owns. And yet, the private sector owns the vast majority, something like 80 percent of this infrastructure. What am I missing in this inverted –

SEN. GARDNER: And, in fact, today, again, we’ve said that we aren’t going to be talking about this and we’re not going to be making this public. Again, I think one of
the most effective things that we saw when we indicted the five PLA officials, it actually had some effect on China.

And, again, I think with the executive orders that the president issues in April in response to the – they didn’t even call that a cyberattack or cyberterrorism. They called cybervandalism.

And so an act of cybervandalism, so we do need to understand – be in a position to publicly say this, to create the punitive measures, the punitive targeted measures against the people responsible, to have a strategy that comes forward across the administration, particularly out of the Defense Department.

But I think if you’re looking at the situation as it relates to the commercial sector and the public sector, it is kind of stunning that we would have a very different response. But the rules and the norms that we have to address really get to the heart of that distinction, that heart of the commercial – the heart of the public kind of operations.

Because of our failure, because of our lack of a strategy, we are entering a very – and the lack of a norm or the lack of sort of this international agreement, we’re seeing the real possibility where you could have a commercial sector try to engage in sort of retaliatory measures.

And so what happens when you have a commercial sector that doesn’t see an adequate response or adequate protections from the government, whether that’s the cyber bill that we’ll be dealing with in the next couple of weeks in the Senate or other measures in place or the norms that they would like to see agreed to? Then you have this situation where you have a commercial sector that’s kind of out on its own, a cyber arms race, so to speak, so that you could see.

And so part of the need for this international norms – and if China’s not willing to use the UNGG process, GGE process, to make agreements, then we need to go outside of those forums and those fora and try to find other avenues that we can have these discussions and find like-minded responsible actors who are willing to enter into these norms and agreements so that we can put pressure on actors like Russia and China to behave as responsible governments should when it comes to cyber.

And so that strategy is very important to make sure that we’re protecting the commercial side, the public side, and to make sure that we have a coordinate, cohesive strategy to protect the Internet and our networks nationwide, not just parts and pieces.

MS. EAGLEN: Yes. And you segue perfectly into my sub-question, which is should private sector companies be allowed to hack back or are they doing it already? Does there need to be any oversight or should we just let this all happen in what is essentially a commercial black world?
SEN. GARDNER: The concern is that you develop this cyber arms race if we don’t have the proper policies in the place for an overall government approach, a whole-of-government approach to cyberstrategy.

And so what we need to do, of course, is to find those policies, the international rules of the road so to speak, and to create that framework of responsible behavior. They’re dragging – China, others are dragging their feet. I mean, there’s basic language of the last discussions I believe were some of the U.N. forums that took place where they may have even disagreed with language they agreed to when they entered into the charter of the United Nations.

So how do we make sure that we are pushing these norms of behavior? And if there’s a roadblock, then we have to find ways to get around that and to actually find willing partners, willing nations to enter into these agreements because I do think it’s creating that escalation on the commercial levels is a – is not the direction with policy or the direction of activity that this country wants to have.

MS. EAGLEN: Sure. Fair enough. Well, I could hog the stage all day. I actually just thought of two more questions. But we’re going to open it up quickly because we have such a short amount of time with Senator Gardner. If you don’t raise your hands, I will keep going. So we have about 10 minutes. We’ll start here and then we’ll move our way over. Yes. Could you wait for the mic so that the cameras can hear, please?

Q: Senator, my name is George Win (ph) and I work at USDA. My question is, since you work with other countries in East Asia, you just mentioned, what’s the level of preparedness of other countries in comparison with the United States on that issue? How do other countries prepare ahead or behind us on this kind of issue please.

SEN. GARDNER: Well, thank you. And, again, if you look at China, if you look at the level of importance they are placing on cyber strategy, it’s extremely high. And, you know, again, without having seen everything that they’re doing, I think they’re taking it much more seriously than the U.S. is. And that has led to very serious breaches of the OPM, millions of fingerprints stolen, personal identification information stolen, hacked into.

And so the challenge for us is we don’t even necessarily know what – we haven’t done the full analysis or the proper information to know what ought to be protected, what ought not to be protected. And so how are we going to make sure that we have the information necessary as policymakers, as leaders of various departments and agencies, to make sure that sensitive information is protected in the strongest way possible?

And so, you know, if you’re looking at other nations in the region, I mean, obviously they’re seeing the same responses. They’re part of discussions and dialogues that are taking place, whether it’s the United Nations or beyond. But we are not keeping up with some of the most egregious actors like China as we must do.
MS. EAGLEN: We’ll go over here. Yeah.

Q: Claude Barfield, AEI. I want to go back to the OPM. It seems to me that that would be one of the worst places for the United States to try to say that the Chinese are going against international norms in the sense that Mr. Clapper, Michael Hayden have both said – Clapper just said I tip my hat to them. And Hayden said that if I had been them, I would have done the same thing. The point is, isn’t this a purely spying operation that became public, but isn’t it the kind of thing that Clapper and Hayden are saying that we’re actually doing too?

SEN. GARDNER: Well, again, I think clearly we’re trying to break in to find information, spying, however you want to call it.

Q: But we’re not breaking any norms.

SEN. GARDNER: But I think for the fact that the United States just kind of sits back and says, we’re not going to point fingers, we’re not going to blame anyone, we’re just going to – but yet we’re going to make sure that when Sony is hacked, that we’re going to be very vocal, very loud, we’re going to issue an executive order when Sony is hacked into.

But when the OPM is hacked, and millions of Americans, many of whom are just – you know, common, everyday private sector people have their private information stolen, I think the people in this country expect more. I do think that’s a violation of norms of behavior.

And we need to prepare ourselves internally to make sure that we are protecting that information, to make sure that we have policies in place that would have prevented this from happening in the first place, but we also have to make sure that China understands we’re not going to accept that kind of behavior. We’re not going to sit back and we’re not going to let that happen time and time again.

So it’s on us, it’s our responsibility to protect the information, to make sure that we know the information that needs to be protected, as some of the private sector have said that we do a very poor job at, but also to make sure that from a diplomatic standpoint, make sure that we have a strategy in place to address and respond when – if you want to call it old-school espionage occurs.

MS. EAGLEN: Yeah. That was a point Ellen made in her Post story this morning pretty, which was in the Cold War, no, actually we would publicly identify the spies and expose – get rid of them as shipping and packing home and that was a key part of deterrence is that we would publicly expose you and degrade your operation and your network that you developed here and your government, you know, knows that this happens. Actually, there are some norms of espionage and we’re not responding, I would argue, typically as we would have done in the past.
Behind Claude, we had a question.

Q: Hi. Derek Douglas with Deloitte. Will the Senate be able to vote on the Senate cyber bill before the August recess?

SEN. GARDNER: Thank you. That’s the plan. Again, I think the leaders – one of the first thing he said during a conference I attended was legislative time is the coin of the realm in the Senate. And so his intention is to move to cyber after the highway bill.

And that’s why the House – the Senate will be using the week into August that we were scheduled to use, for cyber. That’s the current plan. I think everybody realizes the importance of that. Recent events highlight the importance of it even more.

Of course, in the last Congress we were able to pass a cyber bill out of the House of Representatives. And this is – this is an important issue that we need to address in the Senate. It’s an important issue that we need to move forward with. It’s important for the private sector. It’s important for the public sector. And look forward to strengthen it in ways that we can.

How do we strengthen it? Number one, I think we take a look at the bill for opportunities to identify areas where we need to do a better job of protecting information, to make sure that we know the information that we need to do a better job of protecting.

And we also, I think – and this goes back to comments I made early on, is I believe we need to take a better look why this cyber discussion is taking place on the legislation, of how Congress is structured to address the needs of a focus on cyber strategy. I’ll give you an example.

A couple of weeks ago, I had the opportunity to go to Colorado and visit with the leadership of Schriever Air Force Base out in Eastern Colorado. Schriever is home to GPS, a number of important command operations. In our conversations with the colonel of the base, we talked about how cyber – Space Command, which is located in Colorado Springs, had been had added – they added to Space Command Cyber Command because of how disparate the command units, the responsibilities were at that point within the Air Force. And so they added to Cyber Command to Space Command.

You know, perhaps we ought to look at the way we structure congressional roles in cyber strategy. We now have the Foreign Relations Committee with cyber oversight. We have Homeland Security with its hands into cyber. We have Intel with hands in cyber. We have Senate Armed Cyber with its hand in cyber. We have the commerce committee with its hand into cyber. That’s not just – that’s not even counting the various subcommittees of each committee that have a role in cyber.

So if you look at what China has done with President Xi and created the committee to focus on cyber issues, if you look at the directions that we’re trying to give to the State Department to create a cyber strategy, that framework that we mentioned
across the executive branch, the coordination and the development of a cohesive, well-
thought, you know, progress-reviewed cyber strategy, maybe we need to do the same 
thing in Congress. Maybe it’s a select committee on cyber. Perhaps that’s the way you go 
forward. Maybe it’s taking the chairman of each various committees, putting them on the 
select committee.

You know, we have to be careful that we’re not reacting to the flavors of the day, 
but I don’t think cyber is a flavor of the day. I think that’s something that is going to be 
with us as long as we are a continuing government.

MS. EAGLEN: So what you’re telling us is it’s no wonder our responses have 
been incoherent, Sony versus OPM, when we look within the Department of Defense, 
their own disaggregated approach to it, the U.S. government entirely – (inaudible) – that 
approach and now Congress is, too. So now we’re all extra worried. OK. But I like your 
solutions.

Q: Gerard Robinson, AEI. In 2013, I traveled to China with the president of our 
for-profit university and part of our job is acknowledged diplomacy. And so we’ve had a 
number of Chinese on campus. We’re going to see more online courses opening up 
particularly with students in China. I can tell you right now that cyber attack is an aspect, 
something that higher ed thought a great deal about. So I would just be interest to getting 
ideas from you how we, particularly as a for-profit provider need to think seriously about 
providing knowledge at a cyber – (off mic.).

SEN. GARDNER: You know, again, I think cyber is one of those issues that – 
we have a lot of meetings in the office with various, you know, public sector companies, 
private sector companies.

And I can remember – I think it was the folks who have J.D. Power within the 
company. And J.D. Power, of course, we all know from the car commercials, right, the 
J.D. Power Award and various banking associations, you know, are reaching the stage 
where some day we’re – you know, whether you’re a rating agency, like Standard and 
Poor, whether you’re J.D. Power Associates, whether you’re some other kind of 
organization, are you going to be basing your bond rating, are you going to be basing 
your J.D. Power Awards, are you going to be basing some kind of creditworthiness, 
which, obviously they are, on your cyber plan, your cyber protections, your cyber 
strategy. You bet they are.

And so, you know, will you see a day where interest rates for a loan are going to 
be affected because one company over another company has a better cyber protection 
plan than another? And that’s the same thing that you could see with public universities.

A couple of years ago, I traveled – I went to a new technology forum that Intel 
was sharing. And met a guy with a little race car track and he had a little remote 
controlled race car that he was running around the track. And he was there to show what
vehicle-to-vehicle communications could do and how it could coordinate to the car that was next to it on the race track.

Well, then he hacked into one of the race cars and he had it accelerate. And so as the race care hit around the car, it went off the road through a cyber attack. I mean, look, every element that we touch in our lives is going to be affected by cyber policy.

And so whether it’s the new advancements we’re making in vehicle-to-vehicle communication to address highway congestion on I-70 through the Eisenhower Tunnel in Colorado, whether it’s a public university that holds financial information, health information, private family information that could be accessed, whether it’s the United Airlines or other airlines that have made the news with various breaches or people threatening or talking about how they have hacked through entertainment systems to take control.

Whether that’s true or not, the issue is the need – the real need for cybersecurity before it escalates into a cyber arms race in the private sector, and in order to prevent the OPM from happening.

MS. EAGLEN: Great question. We have time for more? If there are any brave souls. And with that, it’s a perfect way to say thank you because, Senator, your answers were thoughtful and had tangible solutions that are practical and realistic, and things I think that are smart to do and things that we can do right now which – God bless your colleagues – but it is rare when we have some of them here. So I appreciate that. I know I speak for my audience when I say, thanks for coming to AEI.

SEN. GARDNER: Thanks for having me. Enjoy the rest of the day. Thank you.

SHANE TEWS: Richard and Paul, thank you very much for joining me in this dialogue. I have to admit I have eight million questions so I’m trying to find where to start. It was so interesting to hear the senator’s perspective on that and I think we’ll get to some of the points about specifically the government.

But, Richard, I was reading your blog, which if you all don’t read Richard’s blog, it’s fantastic. You did a blog in 2007 – since if the year of back to the future – where you had recommendations about what the government can be doing to secure their systems more. And if the advice you gave in 2007 had been taken at some point, would we be in a better situation today?

RICHARD BEJTLICH: Well, I’d like to thank you for the question and also thank AEI for the invitation to speak today.

The blog post you read in 2007 came after me blogging for about four years and working in the field for about nine years. so, at that point in my career, I had been working on intrusions in the public sector, in the military and air force, and then in the private sector for eight or nine years.
So, by that time, I’d had many wakeup calls that had been kept more or less private because we didn’t really talk about intrusions back then. But, by that time, we had suffered some serious problems. Just a year earlier – does this sound familiar? – the State Department had been hacked. It was called the hack of the century. The Chinese were named at least within the non-governmental sector as the culprit and everyone was wondering what to do about it. So we’ve just had the same sort of issue now.

The problem I find whenever I testify, and I’ve testified I think four or five times this year, testified several times last year, is every time I go, it has to start with what’s called a threat briefing, meaning the members want to know what’s happening. I feel like I could give the same threat briefing that I’ve given every year and, by the way, Paul was – we were together on some of these. I feel like I could give the same briefing every year, maybe adding one or two more actors to the list of threats we have to worry about.

What I’d really like to get to is a discussion about what we should do about this. And that’s what was so appealing about Mackenzie and Senator Gardner talking is they’re trying to talk about things that we need to do. So, hopefully, today, we can do that as well.

MS. TEWS: Absolutely. Well, why don’t we go there now? I mean, you two are both working on very interesting projects. I feel like you’re two halves of a very interesting solution set. One is understanding the problem more and then explaining what to do about the problem once you’ve identified it.

So China being one of the key things that we’re discussing today, can you talk about the 2013 study that you put out that talked about actually identifying the Chinese and how we deal with the attribution in this area?

MR. BEJTLICH: Certainly. So I’m currently with a company called Mandiant. Prior to Mandiant – well, FireEye. Prior to FireEye, I was with Mandiant, chief security officer at Mandiant. FireEye bought Mandiant about a year and a half ago. In 2013, Mandiant, our company, released a report called APT One. And APT One was our internal designation for a prolific Chinese threat actor.

And I think what caught people’s attention about this report was that we didn’t just say this Chinese problem exists. We didn’t say they have been active for a couple of years. We talked about intrusions going back to 2006 that we had been working since our company started in 2004. We identified the unit of the PLA, their military unit cover designator 61398, their public persona as second bureau, third department of the general staff directorate of the PLA.

And I think what really caught people’s attention was we showed their headquarters. We got on Google Earth, we found the building, and that’s what sort of broke the story out of the security community and onto CNN and everywhere else. So the fact that a private company could identify to such precision who these guys were – and
we did it using not only our technical capabilities, but also open source information, things like finding an order written by the telecommunications company that was laying new fiber cables to give this building Internet connectivity saying, you guys need to hurry up the installation of these cables. Don’t you know that the group that’s going to be there is unit 61398 who does all this signals intelligence work against the U.S. and other Western countries? So I think that – really is one in a line of progressions of activities that have occurred over the years.

So at least now we can talk openly about this. Within a few years, I couldn’t even say “China” and “attacking us” in the same sentence without worrying about whether I was spilling classified information so we’ve made quite a bit of progress in just a few years.

MS. TEWS: I have a new favorite, 61398 will probably be my password.

MR. BEJTLICH: And there’s many more. Right. That’s just one group. We track dozens of these groups. And, of course, there are Russians and others. But there’s some wonderful reporting by the 20409 group that lays out all of these 61 groups that exist. That’s really part of what I call the revolution in open source intelligence. I was an Air Force intelligence officer. There’s better stuff online now than what I had probably when I was in uniform. And it’s all available to read.

MS. TEWS: Paul, you’re helping inform businesses what to do about all this. So we know the government has been in the news and they’re having some issues but where a lot of this really lies is in the private sector. So how do you manage this issue in your area? What do you do about this?

PAUL TIAO: So I work for Hunton and Williams, and we represent all manner of critical infrastructure at major companies on cybersecurity and private issues. And so we actually work very closely with Mandiant and FireEye on a lot of breaches and cybersecurity incidents that we work jointly together.

And what I – so a couple of thoughts. So, one, that report that Mandiant did in 2013 was just a game-changer. It was crucial because it got us – as Richard was saying, it got us over this question of attribution.

So until then, there was always a sort of lingering doubt about it, who really is this and how certain are we that it’s the Chinese? We think it is but can we really act on these cyber breaches if we don’t know with certainty who it is that’s actually doing this?

And the Mandiant report was crucial because it just broke it open. And not only did it put a building on TV and the media, but it also put the names and their faces of the actual hackers. You put a name and a face at a keyboard responsible for these hacks. And it just demystified all that and kind of put it to rest. And then since then, there have been a number of additional reports that have reinforced that perception and identified other units within the PLA that are engaged in this.
So that was – that was crucial because it allowed us to move onto the next question, which is what can we do about this, and it opened up a range of solutions.

So, from our standpoint – we represent these major companies. And the private sector is getting much better especially in certain sectors where the financial sector is probably the most advanced, the telecoms are advanced, energy sector is catching up, and other sectors are rapidly beginning to focus on this.

What we saw in the private sector is that at least in the companies that we represent, they are doing a tremendous amount, way more than they ever did even two years ago, even a year ago, at the C level, at the C-suite, at the board level, the commitment of resources, the willingness to work across – within a sector, across different sectors with the government to address this problem is far greater than ever before. And I assume that you’re seeing the same sort of thing.

So, proactively, the companies are much more creative. They’re putting more resources into it. They are changing the structure. We do a lot of work advising companies on how to reorganize their board, how to reorganize their executive committee, how to reorganize their management structure so that it can more effectively address their information security policies to make sure that they’re addressing, you know, third-party vendor vulnerabilities, that they’ve got a breach response plan in place, that they’ve got the best monitoring or technical sort of defenses.

So there’s a tremendous amount that they’re doing, but the problem is this. You do all that and you can get – you can significantly reduce your risk, especially against the criminal hackers. The hackers world is really two worlds. There’s the opportunistic criminal hackers and then there’s the advanced, persistent threats and nation-state actors.

The criminal hackers are just looking for the lowest line for it. So they’re just going for what’s easy to get to and they’ll do that. And so you do the basic hygiene, you improve your information security practices and policies. You can reduce your risk. People estimated it’s kind of a wag but, you know, about 80 percent.

But if you’re dealing with the nation-state actor, and that’s really what we’re talking about today, then you’re talking about a different sort of a thing. If they really want to get in, they’re going to persist and they’re going to continue to try to get in because as part of their 12 to five year plan, it’s an important part of their industrial development. It’s an important part of the national security development.

If those are the stakes, if that’s the focus, they’re going to persist and they do – you know, you’re right. You could say – you could give the same briefing that you’ve given the last couple of years. But there are some nuances and there are some differences and they’ve gotten way better at social engineering than they ever were before.
And there are some things that they do, you just pretty much can’t stop. If they infect – if they do a strategic web compromise, if they infect a website that your software developers have to go to or that you – you know, if they just infect the website of a conference that you’re going to go, you’re going to go to that website because you need to get information that they infected and you’re there and then you just – you click on the link for like – you know, where the place is or how to register, and you download malware. You cannot avoid that. So if they really want to get in, they’re going to get in.

So then the question is, what can the companies really do? And if there’s a limit to what they can do, then who else needs to step in? And that’s really what where we have to talk about the government. What should the government be doing to address this more effectively because companies really aren’t built to stop those types of attacks? The government needs to step in.

MR. BEJTLICH: Could I talk about that for a second.

MR. TIAO: Sure.

MR. BEJTLICH: So, full disclosure, I’m an Air Force Academy grad so I have some background in like science and math and stuff but I was – I studied history and political science when I was there. Let me give you a little bit of math that will explain Paul’s point very well.

APT One, let’s be generous and say they had around 1,400 people at their headquarters. We knew that they had hundreds. It could be thousands. Let’s put it somewhere in the middle and say 1,400. The reason I picked that number is they were targeting, at least according to our research, the numbers that we could prove, about 140 companies. So let’s say with 1,400 people, they were able to sustain operations against 140 companies.

Now, those 140 companies, they don’t need one person to stop a group of that sophistication. And, by the way, they’re not that sophisticated. There’s other groups we deal with that are 10 times worse. So the individual companies don’t need one person. They’re not going to make it with 10 people. You’re going to need probably 40 to 50 people.

And I speak from experience. Before Mandiant, I was the director of incident response at a small company called General Electric. And I had a budget in the tens of millions with between 40 and 50 people working for me. So what that tells you is that it is four to five times of scale that you get by being an attacker.

So when you do the math, you know, even though we’ve seen the improvements in the private sector, it’s tough to see where all that money is going to come from, and, secondly, where are all the people going to come from? When I built my team, I called every friend I had in the world and said, come work for me and I’ll still, you know, try to groom new people to work with us, but the talent just isn’t there.
So although maybe the top end of the private sector can handle this sort of issue, maybe. I mean, against a nation-state, it’s a tough call. What do you do about the small and medium size? They’re really in trouble.

MS. TEWS: Yeah. It’s a very good point. So you guys are sort of the dream team here. Let’s say that I hypothetically, I’ve got – you’ve just told me that I’ve got China in my system. I have luckily you on retainer and you’re helping me with my governance. What do I do about that?

MR. BEJTLICH: OK. So I do have some answers here. It’s been most recently brought out of me through blogging and also I –

MS. TEWS: You’ve been exercising –

MR. BEJTLICH: You can tell then things aren’t that exciting. I don’t blog as much, I don’t tweet as much, but when things get exciting, I’m writing all the time. I wrote a piece for Brookings recently and I’ve done some private blogging as well. And it’s been motivated by the OPM hack.

We have this false dichotomy that says either you somehow have to build up your defenses to the point where nobody can get in or you’re just helpless. And that’s not true at all. You can be helpless, right, and you’ll just get all your data stolen, or worse. But the other one isn’t going to work either. There is no wall that’s high enough to keep these guys out, because just like El Chapo, they’ll burrow under it and have a motor bike in a tunnel and all these sorts of things.

So what you need to do instead is to prevent an intrusion from becoming a breach. And by that, I mean, you’ve got to keep out as many people as possible – and it was mentioned earlier that – you mentioned, Paul, that, you know, you can keep out certain criminal actors, the hacktivists and such.

But a certain number of guys are going to get in. They’re going to cause an intrusion but you want to stop them before it becomes a breach. In other words, this time that lapses from when they get into your network or get into your data to when they do something bad with it.

And despite – and I’m a big fan of General Hayden and General Alexander and Admiral Rogers but they tend to think in terms of this is a lightening attack. This is an electronic blitzkrieg that happens at the speed of light. It’s not true. I’m doing my whole Ph.D. around this idea of how fast do these intrusions occur. And there are public cases where you can see it takes anywhere from hours to days or, more realistically, it takes weeks.
So what that means is that at any time during that point where the bad guys are in your network, you catch them before they accomplish their mission, you win and they lose. So that is the strategy that we need to encourage.

So if OPM had had friendly forces looking throughout their network all the time for the intruders that they assume were there and they caught them before they caused their damage, we wouldn’t be talking about the OPM breech.

MR. TIAO: So that’s exactly right. And the challenge is how do you get a company to that point? And so companies – some of these companies, big or small companies, there’s tremendous institutional obstacles to actually getting you to that point because most people in these companies don’t understand this. They don’t understand how serious this it. They don’t understand what they need to do to try to put in place the systems to sustain that kind of a program.

To get to that point, you generally need to have significant commitment from your CEO, other C-level executives. To get to that, you need to have educated that person. To get to the point you can educate the C-suite, you need to have a good staff in place. You need to have a chief information security officer. A lot of companies don’t have a chief information security officer. It may seem incredible to us because we live and breathe this, you know, 24/7.

So to the rest of the world, you know, it’s only the last couple of years that cybersecurity has really hit the headlines. And now, you know, everybody kind of understands it but that doesn’t meant that companies are committing the resources.

So what we find is that sort of the best case scenario for a company is they’ve suffered a very small breach, right, where they just managed to avoid really serious consequences so maybe it’s an intrusion, a compromise but not a data breach or a network security breach. And then they realized how lucky they actually were. And so we’ve got a number of companies that are in this sort of situation.

And then you begin to have conversations. You’ve got to have the general counsel involved. You have to have the information technology folks, the information security folks, you have to have HR, communications, and all the stakeholders that actually control or own or manage the data or the networks that are at issue. You’ve got to bring them together.

So companies ideally restructure themselves and create some sort of a task force usually at the management level first, and then, eventually, they’re able to persuade senior executives that it needs to be at a higher level. You want to get to the point where, you know, companies reorganize their boards.

So we have helped companies to create committees on information security or business security, it might address physical and cybersecurity. And then you’ve got advocates on the board of directors, they create a subcommittee there, they hear about
this much more frequently than the rest of the board, they become advocates for the chief information security officer, and for the rest of the team that is trying to make sure that cybersecurity is infused throughout the organization.

That process takes a long time because there’s many, many different actors, most of whom know very little about cybersecurity other than what they – well, not fortunately, but what they read about in the newspapers now.

Two years ago, you couldn’t even have this conversation because everybody thought that you were Chicken Little running around talking about the sky falling. Now, everybody knows the sky is falling, so at least you can have a conversation. It’s not great that the sky is falling but at least we know and everybody knows that the sky is the problem so now we can actually talk about solutions, right? And, you know, reports like the one from Mandiant 2013 help out.

So then, once you have the structure in place, then you can begin talking about what you need to do. So you need to look at your information security policies. And that affects many, many different aspects of your business. You have to have a lot of people involved in that. Then you need to look at different things like your relationships with third-party vendors. These companies have thousands and thousands of third-party vendors, many of which actually have access to key networks and key data.

And then there’s like the target breach, where it’s an HVAC vendor. You wouldn’t think that an HVAC vendor could be part of the vector, the threat vector that gets in, but if that can happen, then you – the bar is pretty low for which you need to be looking at, but if you’re talking about tens of thousands of vendors, tens of thousands of contracts, you want to figure out whether those contracts have good information security language, good identification language, good language on sort of notifying the company about a breach or about an incident. That is a huge amount of work, right? And then you want to have a good breach response plan. And so that takes a long time because as crazy as it may – there’s sort of this odd ironic thing.

So you do this and people want to jump in on it because they think that C-level executives are going to be involved and it’s an opportunity for them to work with people at a very senior level, not realizing that if they actually have a role in the breach, they’re – I mean, it’s a very risky sort of proposition. I mean, breaches are tough.

And so if you put yourself right in the middle of the breach response team, then, you know, you are going to be facing some very, very difficult decisions when or if that incident actually happens. But, anyway, a lot of stakeholders, a lot of people, a lot of turf battling over what these – what the plan should be like.

Then you need to have table-top exercises. And for the companies that are in certain sectors that are comfortable doing this, they should work with the government because the government is doing way more than it ever did before.
Five years ago, it wasn’t a priority for the government to push out information about security threats to the private sector. They were more concerned about sources and methods and just protecting their investigations. And some of that actually is borne out in today’s article in the Post, right? But about five years ago, the government just decided that it is really a priority for us to work with the private sector and to find ways to push out information about threats that the Intel community’s gather and companies are increasingly beginning to embrace those programs and to participate.

So there’s all these things that need to happen. You can tell that it requires the involvement of many different actors within the company, most of whom don’t know anything about this. So that process takes years.

And so we have made at least in a lot of the companies that I work with, we’ve made tremendous progress and you can just see it in all the conferences, there’s so much focus on cybersecurity these days. That’s great, but that doesn’t necessarily translate into – I mean, it does not translate into immediate action within companies because companies are complex institutions.

And I worked at the FBI for four and a half years. It was 35,000 people, and I thought, oh, my goodness. How – you know, just coming out of the U.S. Attorney’s Office, where it’s a flat organization, to actually go to the FBI, sitting with the director and seeing, you know, what he had to do to manage 35,000 people was extraordinary to me. But, you know, some of our clients have 400,000 employees.

And so the magnitude of these institutions that have a lot of the same sort of dysfunctions that government agencies have means that getting to the point where you’ve got this optimal defense system that frankly still doesn’t necessarily keep them out is – it takes a long time. It’s tough.

MR. BEJTLICH: If I could just tell a quick story. So I think what Paul emphasized that is so true in my experience as well is that this is not a technical problem. This is an organizational problem, at least from the victim’s side. We could project outwards towards the threat, but the from the victim’s side, you know, I do at a technology vendor, but there’s no magic technical solution to this problem.

To give an example. I helped an organization that suffered a really terrible breach, and you go through a process called remediation. Remediation means we’re going to try to find out all the places where the intruder is and we’re going to pull him out there and, hopefully, at least hold him back, make it harder for them to get back into the company.

I named the first remediation plan Rolling Thunder. Does anybody recognize that? All right. I knew it was not going to happen the first time around so I named the first remediation, for those of you who aren’t military history majors or I was too young to remember anyway, but it was the first –
MS. TEWS: I thought you were talking about Hell’s Angels in South Dakota.

OK.

MR. BEJTLICH: Oh, no, no. I’m talking about one of the bombing campaigns in Vietnam. So after Rolling Thunder came what? Linebacker One. Guess what this name of our second remediation attempt was. Linebacker One, right, because that didn’t work either.

The third remediation attempts that we tried, and this is after like six months of trying to kick these guys out, I called it Linebacker Two. And, guess what? That one worked. That Linebacker Two, you know, history people, that was the one that brought the Vietnamese to the negotiating table. It didn’t end the war but, you know, at least it was better than the previous ones.

So this problem, at least from the perspective of the victim, what you can do within your four walls is something that you have to sort of solve internally, organizationally, have internal competing dynamics. And it’s the thing that hasn’t happened yet in the government. The private sector’s made a lot of strides in this area. The government is not there yet.

MR. TIAO: And the question of incident response, I mean, we’ve really focused – until just now, we were focusing on preparedness, what did these companies need to do to be prepared for that – to reduce the risk and also to address the actual compromise. But the sort of breach, sort of cybersecurity compromise scenario is – it’s a very difficult sort of situation.

Even if you are prepared, even if you have a breach response plan that – even if you have done table-top exercises and you’ve done red teams and you’ve done all – and you’ve brought in Mandiant, FireEye or other companies like yours to work with the breach response team to actually deal with the scenario and make sure that they are primed and ready to go, it is still very difficult. And it’s very costly. I think one of the things that you all had suggested that we talk about is sort of the costs of this to the private sector.

So all the things that we talked about earlier are very resource intensive. They require – they occupy a tremendous amount of time, of senior executives if it’s actually happening within the company. Ideally, you’ve got senior executives that often occupies a lot of their time. And then, you know, and some of these security systems are very costly. And so there’s a front end cost both in terms of resources and staff time and vendors.

But then, on the back end, if you actually have that incident and if you’re unlucky and they actually did compromise a network, they did compromise significant amounts of data, then you need to move incredibly fast, right? And so, ideally, you’ve got an outside counsel retained. You’ve got a Mandiant or another company like yours retained that
actualy knows your system. And then they come in under cover of sort of legal privilege, through counsel, and you have boots on the ground to begin investigating immediately.

But all that takes time. And then, sometimes it takes – I mean, you can speak to this much more effectively than I can, but sometimes it takes a long time to figure out where the actor is. The Chinese government is notoriously effective at sort of infiltrating networks and then spreading across the network and escalating their privileges and gaining footholds throughout. You want to figure where all those things are because if you want to eradicate them and get them out of your system, they need to know where they actually are. That process takes a long time.

In the meantime, Brian Krebs from the Washington Post may have gotten a hold of this, right? And he may have contacted your communications director to say, hey, I’ve heard about this. I’ve seen information about this on the black market forums, on the Internet, and I’m going to go public. What’s your response? And I’m going to go public in 24 hours, right?

So then you’ve got to do – you’ve got to mobilize your communications team, you know. And if there’s personal identifying information, you’ve got to be looking at which – you know, what sort of data was affected, where those individuals reside.

There’s 47 different state data breach notification laws. You’ve got to look at those laws to figure out what your notification obligations are. And then you might have – and then, meanwhile, you’ve got all manner of people within the institution that are actually asking questions to get information about it. The board might want a briefing, the CEO might want a briefing, all sorts of folks want to have briefings, and it’s very highly profile. And it all has to – everything has to have been done, you know, two days earlier.

So it’s a very intense, very harrowing sort of situation where every couple of hours, there’s some new thing that China changes the way that the team has to address so the team has to have a battle rhythm where they’re talking once, twice, maybe three times a day so that they all know what they need to be doing. This, as you can just sense, is a very time consuming, very costly exercise that involves senior, mid and lower level employees. And so the costs of this are very significant.

And, you know, what we need to do is to identify solutions that are game changers, that create a deterrent to this type of activity. And, to date, we haven’t really identified those things. There’s a lot of different things – not a lot – there’s a handful of things that we’ve begun to sort of throw out there. Is it sanctions? Is it an action of the WTO? Is it an indictment of five PLA hackers? You know, what is it going to be that’s going to be effective? And we certainly have deterred them yet, but these companies are suffering incredible costs.

You now, when all that happens, you’ve got all the costs that are associated with the things I just described, but then you have reputational harm, there’s legal – there’s lawyers. You know, there’s litigation involved. There’s costs of losing the intellectual
property. There’s disincentives to innovate. There’s – if the information does eventually make its way into the hands of a competitor, then you’re put at a competitive disadvantage.

If you look at the PLA indictment, each of those companies that were identified in that indictment were either involved in contractor negotiations with Chinese entities or they were involved in trade disputes.

So in each instance, the information that the Chinese government obtained was a sort of information that could be very useful and could give them an unfair competitive advantage, either in that negotiation or in the trade dispute.

So the sort of harms are really significant and the companies, frankly, need help from the government to try to deal with these things to reduce these costs and to create some sort of cost, to impose some sort of cost to the Chinese government that might begin to have some sort of deterrent effect at some point.

MR. BEJTLICH: I think the first step we have to take is – and I’ve thought of this when the previous panel was here. And the discussion was around cyber. And you say, what do you do about cyber? Well, when you think about it in that way, what do you do? Does anybody know what cyber is? Where is it? How do you affect it? It’s this nebulous thing that’s very difficult to consider.

But when you think in terms of the threat actor, who is it that’s causing the problem, that opens up a whole new arena. So, for example, the Chinese often think this way. They don’t perceive things the way we do. They think about it and they often respond asymmetrically.

So, for example, after we released the APT One report, they saw us as a proxy for the NSA and U.S. government. So what they then looked for were someone that they could hurt who was doing business in China and charge them with espionage. So they’ve picked out a group of Coca Cola employees who were near a Chinese military base, who were using a GPS, and they said, you’re conducting espionage for the U.S. government, and they tried arresting them.

So they think about this – they didn’t say, well, are we going to release a report back at the United States? They said, no. We’ll come around and hit them from a different angle. I think we need to use that sort of approach as well, concentrate on the threat actor, think about areas where we have an advantage, where they have a disadvantage. That’s the whole – you know, the DOD and the whole offset strategy talk that’s going on right now. I think that’s one way to approach it.

Here’s a second idea. There’s been various estimates done, some by Europol, some by Interpol, some by others, that believe that there are only 100 top tier malware authors in the world. These are the guys who create the exploit kits and other pieces of software that you can buy commercially in the underground. If we could apply pressure
to those top 100, we could make a big dent in the overall cyber-crime underground because a lot of the work is carried out not by those guys. It’s by other people who buy all the software.

We just released a blog post the other day about a Nigerian group that was buying this kind of software and using it to attack people. So let’s go after – I did a piece for Brookings called “Targeting the Malware Kingpins.” We go after those guys, that puts pressure on that whole eco-system. And so this is an area actually where DOJ, working with Microsoft and other companies, and even with us, has made some headway, where we go after the people who are at the nexus of these cyber crime areas.

Now, of course, that doesn’t necessarily get at the nation-state arena, but it does give you a couple of things that you could work on.

MR. TIAO: It’s just like in a company or in the government, it’s defense depth. So you have to have multiple avenues at trying to reduce the risk. Some of the risk is sort of easier to deal with. It’s really a matter of cyber hygiene. Some of it is much more challenging because you’re talking about advanced persistent threats.

But I think that we have to throw a lot of different sort of different solutions out there and begin to work these things. And I think the government and the private sector are beginning to do these things. And I think that there’s greater collaboration than there ever was before. But the challenge and the threat is so monumental that it’s just – it’s going to take some time before we see real impact.

But I think that trying to ensure that we use all different types of tools in our kit, whether they’re trade tools or they’re prosecutorial tools or they’re sort of technical tools, it’s really important that we do these things and then analyze them.

Right now, I don’t get the sense that there’s a lot of analysis being done of what could work, what is working and what the impact is. And I think that that’s a really important thing for us to begin to focus on. It is not shocking that there hasn’t been a ton of work on that because it’s only recently that we’ve actually begun to try to create a deterrent effect on these nation-states.

But I think that that’s – it’s crucial that we begin to do that because we have to do something to try to change the nature of the game.

MS. TEWS: So if you are not under any obligation through regulation to submit yourself – if you find out that you’ve been under attack, what is the incentive – especially for, like you mentioned, the bigger companies you’ve – I mean, all the cyber governance points you brought up, very expensive, lawyers involved, lots of people, you know, I find out – and a lot of times, you always hear this story that it’s the FBI knocked on your door and said, hey, there’s somebody you might want to know about in your system. What is the incentive to cooperate with the government and like make sure that that information gets fed into systems that you look at it, FireEye or –
MR. TIAO: The government I think has – I’d be interested in your perspective on this. My sense is that –

MS. TEWS: I mean, the whole idea, how I’m from DHS, I’m here to help is not exactly top line yet. But it could be.

MR. TIAO: So I think that the government has qualitatively – has in some instances qualitatively different types of information than what is gathered in the private sector. I mean, they have a different mission, right? And they’ve got different types of legal authorities to get to the information that they’re collecting about what the threat actors are doing and how they’re doing it, right?

So you’ve got NSA out there, and they have their signals intelligence authorities. You’ve got CIA, and they’ve got their – you know, their intelligence gathering authorities, both technical and human, right? You’ve got the FBI, and they’re in charge – they lead the domestic intelligence and criminal investigations on cyber and other areas, right?

So then all these agencies are working together. The FBI leads this thing called the National Cyber Investigative Joint Task Force. It’s the – there’s an acronym. I just said the name, but it’s in Chantilly.

And so – and that brings together all of the agencies – intel, investigative and cyber – where they’re not just sharing information but they’re actually collaborating together on threat actors. And they’ve identified a whole bunch of different threat actors from – you know, everything from nation-states to criminal actors. And they are working together to actually conduct either investigative operations or Intel operations, or, in some instances, possibly disruptive operations against these actors.

So they have their pulse on a lot of information, a portion of which the private sector is not likely to have. You never know. They might have it, right, because you’ve got companies like Mandiant and others that have really – have a client base all over the world and you’ve got incredible collection and so – and you have authority from these companies to actually analyze that data and to use it in a constructive, proactive way.

You know, but in some instances, the government is going to have different types of information. So especially I think in the instance where you’re dealing with nation-state actors and you’re dealing with government agencies that are conducting classified investigations, I think that increases the likelihood that they will have information that could be useful.

And so if you have a good relationship with an FBI, with a DHS, and you have a relationship of trust, and increasingly those agencies are focused and have made that priority to develop these types of relationships with the financial sector, the energy sector, the telecoms and other key infrastructure sectors, then you can put yourself in the
situation where even if you don’t have a legal obligation to notify individuals or to even notify regulatory agencies, you may want to work with the FBI or DHS agencies that have useful information to see what they have. And they provide technical assistance.

And to see if they can help you understand the nature of the threat, identify other areas within your company that may have been compromised because the government – look, the government – these threat actors go after many, many different companies. You mentioned 140. That was just one unit over one period of time. So then you multiply that by the number of units that are out there, many of which are far more sophisticated than the one that you – the number was 61398? What was it?

MS. TEWS: My new password.

MR. TIAO: Exactly. You know, chances are there’s many other victims that the government has insight to. And they’ve seen what the threat actors have done to compromise those victims, and some of those tactics and methods may have been used on your company as well. So that sort of –

MS. TEWS: It’s like the CDC showing up, going, you have a cyber bowl (sp). This is fascinating. We would like to go take this strain. We’re going to quarantine your servers. I mean, do they show up and say – or is it a cooperative effort? I mean, I wouldn’t know – again, the larger companies are obviously going to have some ideas about this, but go into your medium size or smaller operators that are not necessarily – I mean –

MR. BEJTLICH: Yeah. I can talk about it. So the way it works – and, by the way, this is the single best thing the government, in my opinion, has done in security probably during my career is this FBI notification program. The best statistic I’ve ever heard in security, period, was Ellen Nakashima wrote about it. She said, in 2013, 3,000 U.S. organizations, actually more than 3,000 U.S. organizations were notified by some government entity that they had had a significant cyber breach.

So that doesn’t mean 3,000 incidents. It means 3,000 organizations, many of whom had more than one. And of those 3,000 notifications, two-thirds of them were done by the FBI. Others were done by Air Force OSI and Navy Criminal Investigative Service, and so forth.

So the way it works is you get a phone call or you get a visit in person. And when you get the phone call – I’ve been around for some of these phone calls – an agent says, you know, this is so and so from such and such field office. I need to talk to someone in your security department. And, on a few occasions I know of, somebody – the recipient said, yeah, whatever, and just hung because they didn’t believe it was the FBI calling.

And then, of course, you went through this dance of authenticating, you know, give me your – what field office are you from? I’ll call you back and do that. And, eventually, they say, we’d like to schedule an in-person meeting. And, at the meeting,
generally two agents walk up, you know, wearing suits, the whole thing, just like in the movies. And they’ll carry in printouts, and they’ll say, is this your data? And you look at it and you say, oh, my goodness. Where did you get this? And they’ll say, well, I can’t really tell you but you have a problem.

MS. TEWS: That’s comforting. You don’t know me. I show up in a suit and I have your data. Cooperate.

MR. BEJTLICH: Right. Right. Well, they show their badges and all that stuff. So it’s very difficult for an organization to ignore that. I do know of some cases where the bureau has said informally their policy is, if after five times you ignore them, they will just give up on you. But that’s exceptionally rare.

I mean, nobody wants in there to have records of the government telling them that they’ve been compromised and nothing happening about it, because, in those cases – you know, we have things called whistleblower laws and it’s very possible that a disgruntled person in the IT department might say, we’ve had all these visits from the bureau, no one’s done anything, I’m going to go to the press; I’m going to go to shareholders, and, suddenly, you get a legal situation because – remember, if you’re a publicly traded company and you could show that this is a material risk, you need to be telling the SEC about this.

And public research shows that only about 5 percent of the companies that have had these breaches actually tell the SEC. So the SEC has been very aggressive going after companies saying, hey, hotel X, Y, Z, I’ve noticed a lot of breaches in the hotel sector. Why haven’t you talked about this? Because, guess what? When these guys hit, they hit whole sectors at the same time.

So there’s many different avenues for pressure here. Some of it comes from the government – well, I guess the FTC is another part of the government. You could have shareholder actions. I mean, think about all the people that are piling on to Target and everyone else who’s had a breach in the last several years.

MS. TEWS: Go ahead.

MR. TIAO: So I was going to say that – and so I think Richard’s absolutely right about that. And the executive order that the president issued in 2013, in February 2013 really made it a priority for the agencies to do what they were beginning to do anyway, which is to make it a higher priority to notify companies that they have identified as victims.

One of the things that I think is really an important development – and I see Mike Smith from DOE here – Treasury, DOE, FBI, DHS, other agencies, they are beginning to proactively – develop proactive arrangements, where it’s not just that the FBI has been doing an investigation and, oh, they saw some – they saw a bunch of – (inaudible) – that had, you know, company X’s name on it, and so, you know, they figured that out, took
them two weeks to figure that out, then they farmed it out to a field office, and it took the
field office three days to assign and send an agent, the agent called, you know, the person
blew them off four times in a row and then finally they set up a meeting, and like, you
know, five weeks after the FBI figured out that there was (exfil ?) had already gone out,
you know, three weeks before that, you know, that conversation’s happening, right? So
you’ve got a significant time lag. Better than no notification at all, no information at all,
but a significant time lag.

What’s happening now is that agencies are developing proactive information
sharing arrangements where they’re taking sort of cybersecurity threat information,
mostly just very technical information, not sensitive personal information, and ingesting
it, synthesizing it with other pools of information, and then identifying patterns that they
are proactively telling companies about so that companies are getting earlier notice and
they’ve got a better relationship with these agencies that can give them an opportunity to
begin addressing the problem and to reduce the risk that that compromise becomes an
actual breach.

And so, as the government gets better at that and as companies begin to do a
similar thing just within the private – there’s a lot of private, private information sharing
that we haven’t really talked about that much that is getting better, I think that companies
will get earlier notice and be equipped to actually deal with – you know, to address the
problem when they get that notice.

MS. TEWS: So can you talk about the cyber insurance market, because this is
a kind of interesting lead into that, like, you know, if I’m thinking about this and I’m
hearing these horror stories, and I’m going to my C-suite meeting, when and how do I
propose this and who do I talk to?

MR. BEJTLICH: So I’m a fan of cyber insurance as a concept, and the reason is
this. When you think of the different people who know a lot about intrusions, the list is
fairly short. It’s the organization themselves. It’s generally the company that they hire to
help them. It’s their lawyers, their legal team, external, internal counsel. If they go to law
enforcement, law enforcement will learn a decent amount.

And then, finally, if they have an insurance policy, it’s going to be the insurers.
And the reason the insurers know a lot is that in order to get a payout, you have to
demonstrate all the ways in which you tried to defend yourself but ultimately failed in
order to get your insurance money.

So what’s going to happen over time is that these insurance company is going to
build up this huge corpus of data about what companies are doing and what happened to
them. And they’re going to do correlations that show if a company A, B and C, it doesn’t
make any different whatsoever. You know, if they’re using firewalls and anti-virus, and
who cares? They just get compromised all the time, and that’s one situation.
Another company that says, OK. We’re out there, always looking for bad guys. When we don’t find bag guys, we actually feel bad about that. We want to find them. We want to see when they’re trying to break in. That’s a company that’s being aggressive in finding intruders. And, guess what? They’re not having as many breaches. So we’re going to charge that second group lower premiums as compared to the first group. Maybe we can’t exactly even say exactly what it is, but we know, over time, the second group is more effective than the first group.

Once you have that financial incentive so that it costs money to renew your insurance premium for cyber, you’re going to find – and companies are going to say, what do I have to do to lower my premium? Well, I have to do this thing called hunting on my network? OK. How do I do that? Oh, this guy Bejtlich wrote a paper on it, bring him in, talk to him. That’s how we get a financial incentive around insurance.

And I think that will work better than a lot of the other sort of I think nebulous concepts. We’ve heard of brand reputational damage, brand damage, hits to the stock price – that stuff hasn’t really played out. I mean, who here has stopped shopping at Target or Home Depot, or any of the other places? It doesn’t happen really. Over time, they do better. Very rarely does a company got out of business, but there is – don’t get me wrong. There is an overall corrosive effect of this sort of damage. But, yeah, that’s why overall I’m positive about the insurance market.

MS. TEWS: Is this better than the incentive you had of saying, you’re going to have a meeting with the C-suite, like, hey, I was part of a risk management, the earlier example.

MR. TIAO: Well, yeah. I think that – I think Richard’s exactly right. I think that the insurance industry potentially has an important role in sort of lifting the level of sort of cybersecurity, the level of cybersecurity, the level of information security that companies have.

So, one, my sense is that there’s a lot more insurance – cyber insurance products out there. It’s really – just as an aside, it’s really important that companies look at those policies very carefully because there’s actually a lot of areas where you may or may not have coverage so that’s crucial that you do that, especially now as the policies are still very much in development and they’re evolving quite a bit. And they vary from sector to sector. There’s unique issues in the energy sector where there’s industrial control systems with potential physical consequences. But that’s – so there’s a lot of nuance to it. it’s not a straightforward thing, and there’s a lot of work to be done in the area.

But, potentially, theoretically – and, you know, you said – you started your answer by saying that you support in concept, right? So, conceptually, it could be very helpful. And what I’ve begun to see is that insurance companies are doing a sort of – having their potential policy holders complete more thorough, more complete questionnaires. And they’re beginning to team up. They’re beginning to actually buy cyber network security companies that can do audits, that can go in and do penetration
testing, and that’s another way to ensure that their policy holders have better cybersecurity. And they may be able to offer them different products theoretically.

**MR. BEJTLICH:** They’re hiring us to do that, which I think is cool.

**MR. TIAO:** Right. So I think that there’s a lot of sort of leverage here. And I think the administration recognized that. And so, in its 2013 executive order, it directed DHS to explore the possibility of the government doing something to try to support the development of a cybersecurity insurance market. And the government has been trying to do that. And I think the industry is just picking it up because it is – you know, it’s a good business play for them as well.

So there’s a lot of issues. There’s questions about sort of the amount of coverage and whether it’s efficient, especially for critical infrastructure sectors like the energy sector, especially if there’s an incident where there’s physical consequences and the damage could be just astronomical. But I think that, in concept, it’s something that could be very helpful.

**MR. BEJTLICH:** Can I add one thing onto that? I think one of the outcomes of this whole process and the insurance one as well is the question, why do we even have this data? If we didn’t have the data, it couldn’t be stolen.

So to give you an example. If you have a credit card and – how many people have had a credit card breach? Right? I’m like 10 times over. I’m a popular guy in the underground apparently.

I don’t know if any of you have suffered any loss because of that. Your credit card company may have detected it. They’ve probably sent you a new card. The liability is up to about $50. It’s a system that works fairly well. Now, of course, all that fraud happens and that raises prices for everyone, so that’s bad. But as far as the individual goes, that’s not bad. And the credit card companies and the banks have been doing ever better in that area.

Let’s compare that to the devastating hacks that have just happened, where – I mean, I’ve lost all my health care records through one of the health care breaches that’s occurred. I’ve also lost all my SF86 data – all of that stuff. That can’t be fixed. It’s theoretically possible to get a new Social Security number but it’s practically impossible.

So using that data, you know, hello on the Internet – please don’t do this – you could essentially authenticate as me just about anywhere because you know my social, you know my work history, you know all these different secrets about me that are stored in this paperwork. That can’t be undone.

So I think organizations, both public and private that collect data really need to think about do we need to have this data? And if we collect it, what happens when it gets exposed, because the trajectory of history has shown nobody can keep secrets. The
private sector can’t keep them and the public sector can’t. Not even the NSA can keep secrets, and that’s their primary job.

So if that’s true, we need to move to a system that says, is there other data that we could have that if it gets breached, it’s easy to recover from or it has no – you know, no effect whatsoever. I’ve had some people respond to me on Twitter following the OPM hack, and they’ve sent me their national identifier, their equivalent of a Social Security number. And they sent it because there’s no consequence. That number isn’t used to log into a website and treat it as a secret, and yet if I replied to them with my Social Security number, you know, that would be really stupid.

So we need to think about ways to get rid of Social Security numbers, maybe not collect some of this other data, or, if we do collect it, collect it for the shortest time, and then get rid of it because we don’t really need it.

And, by the way, the next wave that’s going to hit us is when all of these large tech companies that are collecting everybody’s data generally voluntarily – you know, I’m not going to name them. You know who I’m talking about – social media – what happens when their stuff gets stolen or put out there?

This isn’t supposed to be doom and gloom. I am actually positive. (Laughter.)

MS. TEWS: So do you think –

(Cross talk.)

MR. TIAO: – solutions.

MS. TEWS: – that the authentication measures that have been put in place by companies like Facebook or Apple are going to help this situation?

MR. BEJTLICH: Yes. One thing I’m often asked when I have these talks is, is there anything I can do as an individual to better protect myself? If you have the opportunity to go to two-factor authentication, meaning you don’t just put in a username or password, but you also put in a little code that comes in over your phone, go ahead and do that. It’s the single most effective thing you can do to keep a bad guy out of your email. And your email is the most important thing you have. Why is that? It’s the gateway to everything else you have.

Think about if you’ve forgot your username and password to get into your bank account. What do you do? You click a button that says, I forgot my password. And they say, fine, we’ll send you a password reset link. To what? Your email. So your email is the backdoor into everything else you have. So you have to protect your email closely. And I personally like Gmail for two reasons. One, they support two-factor, using many different options. But secondly, they’re very vigilant about telling you when something is happening.
So for example, the other day, one of my daughters logged in to her Gmail account that I run from a new computer. I got an email about it to my master account. And I asked her, is that you? Did you log in? Yes, she did.

And you can also do things like log out of all accounts. Like if you see that someone’s logged in from a place you don’t recognize, you can unlog – you know, log out from all those locations. You get monthly reports about where people are logging. So the level of transparency around Google is very good. And the second reason I like them, they had a massive breach in late ’09, early 2010. Right, we all remember that. Google came out and said, hey, China, don’t hack us. So their security has gotten so much better since then. And they’re really at the forefront of not only security as a company, but better security in their browsers and such. So you need to find somebody like that to protect your email.

MS. TEWS: Last question and then I’ll open up. The senator brought this idea of defining the issue as far as the way government looks at it. So he mentioned the idea of a select committee on cyber. Does help at all, knowing that you guys both spent time in the space? Does the fact that we don’t have – with too many people looking at this with their little sliver of authority make a difference, do you think?

MR. BEJTLICH: I’d love to see it. I mean, it’d be another place we’d have to testify, but – (laughter) –

MS. TEWS: You can become staff director. You can be the first guy to testify. We’ll work it out, OK? (Laughter.)

MR. BEJTLICH: I would love that job if anybody – yeah, I think it would be great. I think that is – this idea – I’m very impressed by what the Chinese are doing, honestly, that whole idea that Senator mentioned, which actually impressed me that the Senator knows what’s happening over there. It was very good.

They are – they’re making it a priority and I think we need to think about how to organize our government properly. We sort of – we should also look into the idea of a cyber force. I’m a former Air Force guy. The reason I’m not in the Air Force anymore is because when it came time for me to change jobs, they said, you can go be a protocol officer in Guam, you can be a logistics officer at the headquarters, or you can go be a basic training officer. And I said, which one of those three has computers in it? And they said, none of them. And so I left the service.

I think we need a place where you have a dedicated force that maybe doesn’t look like the rest of the military. Maybe there’s also a cyber guard, kind of like the Coast Guard. Maybe there’s a cyber corps, like the Peace Corps that you could call up and say, hey, look, I’m a small business. Send me one of your cyber corps guys or ladies to help me out. We need to think about how to change the way government does that.
MS. TEWS: And then we have to figure out that that’s actually that person showing up at your doorstep, just like the FBI. Did you want to add anything there?

MR. TIAO: I think that we need a better approach. Is it realistic that we’re going to have one committee that has sole jurisdiction over an issue, an issue that touches pretty much every aspect of our society and touches so many different committees? I don’t know. So I mean, maybe I’ve just been in this town too long to believe that we can do really significant, meaningful institutional change that has a real impact. Because every solution, every policy solution, every reorg in the government seems to have pros and cons.

I mean, I think you could make it work. You could probably make the current system work. But sometimes when you try to reorganize it, you just end up focusing a lot on the reorg and then whether the reorg is effective and how to make the reorg more effective, as opposed to just doing a better job of – a better core job of what we should be doing anyway and that we’re beginning to identify.

So if we can really make it work, then, yeah, because right now our system isn’t working very well. But I guess I’m a little skeptical.

MR. BEJTLICH: Just briefly, that sort of is one of the knocks against DHS is prior to DHS, we had the NIPC, National Infrastructure and Protection Council, which was sort of a joint group of many government agencies. So each one sort of had their stake in it. Once DHS was created – I’m not trying to knock DHS, it’s just what I’ve heard – once DHS was created and DHS more or less became responsible, then the collaboration wasn’t as good as it had been before. So, yeah, I could see that as well.

MS. TEWS: Great, all right, questions.

Hi. Can you please identify yourself?

Q: Sure. Hi, Robert Sherretta with International Investor. Richard, I came here expressly for you because we found much of your information very reliable in the past. But let me take an issue up with you, something I’ve just heard you comment about. In our estimation – we’re doing a report on this – we think you guys are losing this battle. You mentioned Target. People still continue to shop at Target. We’re actually looking at some of the consumer surveys, indicating people are losing confidence because of the magnitude and scale of some of these attacks and the number of people having identity theft, et cetera. We’re also hearing from the retailers that they’re seeing not just an immediate loss afterward, but more conversion to cash in terms of purchases, which actually hurts their overall purchasing environment.

We’re also hearing from some industries like mortgage companies, which take in a lot of information, that it’s actually hurt the small business formation to a certain degree because of some of the liabilities now that are involved. If they feel that they experienced a data breach, could put them right out of business.
So overall, we’re starting to look at a picture and we’re going to be releasing our own report soon indicating that we think the loss of confidence by consumers, by small businesses in particular is going to change the scale and scope of, let’s just say, the information economy in the future as a result of all of this.

MS. TIEWS: So are you saying the use of computers, like you’re saying like let’s go back to –

Q: I’m saying when it comes to reliability of the Internet to conduct purchases, to conduct business – yes, we’re starting to see a pullback on the part of consumers and business.

MR. BEJTLICH: I think that’s a legitimate concern. It’s sort of the big question that people worry about is are we at a point where the costs outweigh the benefits? And I’m not going to say who it is, but I was briefed in privately to a research report that’s going to be coming out soon. I’m not going to say who it is to steal their thunder. But they found that the costs are now outweighing the benefits, which is, like, whoa, wait a minute, seriously? That’s – someone’s actually done the math on this.

So yeah, I think we could be at a point – and again, I’m not – lots of people say, oh, the security vendors, we’re just trying to say how bad things are so you buy our stuff. These messages are not coming from the security crowd. It’s coming from people like yourself who are outside looking at the effect on everyday people, which I think is significant.

MS. TIEWS: So trusting the networks is very important, continuing to have ways to trust networks.

MR. BEJTLICH: Absolutely. Trust is the basis for everything in computing.

MS. TIEWS: OK, Claude.

Q: Claude – (inaudible) – again. I guess I have two questions or a question and a comment for the Mandiant speaker. You mentioned that the attribution problem, we’re on our way to solving it. You guys are at the forefront of that. For the government, that really doesn’t sometimes get you very far. In a sense that if you take the OPM, we just – part of that article that everybody’s referred to today, was that we’re not going to – two of the reasons we’re not going to name the Chinese. One, we have diplomatic issues that we want to pursue. And secondly, it would expose the NSA or whoever the agency is, their method of operation.

So it only really takes you so far and that’s going to be, I think, a problem. If you look at the Sony, the FBI really screwed that up so badly in the sense that, you know, they first refused to say they knew anything about it, and then they kind of dribbled things out, so you got a situation where people didn’t believe them for a long time. So the
government really doesn’t solve a lot in certain circumstances by just knowing who is there.

Just a second comment on, you mentioned the – the other speaker mentioned the indictment of five Chinese hackers. There’s a cautionary lesson there. We – one of the reasons – one of the indictments of the Chinese hackers related to an antidumping case, where they were trying to get information. That is something that our government reserves the right to do. We have done the same thing in trade actions against the French, against other nations in Europe. So it was a little odd we kind of threw that in. That was a pretty weak indictment anyway. But that really was a contradiction. So that was just a comment on what you said.

MR. BEJTLICH: Just speaking about attribution in general. The single best paper about all the complexities of attribution that I’d recommend anyone to read, do a Google search for Thomas Rid, attribution. He’s my Ph.D. advisor at King’s College London. It covers everything. It’s readable. I highly recommend it.

Like you said, we’ve known about who these guys are for a very long time. And over the last five years, we’ve made significant strides in attribution. And I’m – the one bright side to the whole Snowden debacle – I can’t stand the guy, but the one bright side to that whole thing was if anyone is willing to either read the documents or read the derivative documents – and I don’t read the documents because I don’t want to screw up my clearance, but in all the derivative reporting, you see we have the ability to find out where anybody is doing anything basically.

So if you don’t think you know who’s doing these activities, read what Snowden has discovered. I mean, we have teams out there, according to the documents, according to the reporting that I’ve read, we have teams that are going in and chasing these guys. In other words, the bad guys are coming out at us. We’re going back in and casing them and seeing where they’ve been.

And if you want to read a public example of this, after we released the APT1 report, a company in Luxembourg decided to take our data and hack back. And I don’t recommend this. We didn’t tell them to do this. I didn’t know who these guys were. But they just decided to do it on their own. So they went and hacked back at all this Chinese infrastructure that we had laid out in our report and what do you think they found? All the data that was stolen. And then, they emailed me and said, look what we found. And I said, oh, my God, you really did this? Do you have a lawyer? And they say, well, yeah, but we’re Europeans, who cares? (Laughter.)

So yeah, the attribution problem is – it’s not solved and it’s not solved for everything. It has to, you know, rise to a certain level. You know, a Sony level attack, where there’s digital damage, but then there’s physical threats, that concentrated the whole government on this problem and got to the attribution.
Delivering the information, I would agree, was not handled very well. But think about it. The intel community does not have a good history or experience with talking about what they know. It’s actually counter to the whole culture. So yeah, we have to make a better case around that. And the Rid paper talks about how to deal with that.

MS. TEWS: So what about hacking back? How do you guys feel about that?

MR. BEJTLICH: Don’t do it. It’s not worth it. It’s not worth it. What are you going to accomplish? To me, it’s the one area that the state should retain –

(Cross talk.)

MS. TEWS: – a lecture from my dad, don’t do it. Yes, dad.

MR. BEJTLICH: It’s just not – I mean, the few companies in the world that could do it properly know not to do it. There’s only a few that could even carry this out. But they don’t do it. It just complicates things far too much. The ones – I mean, it’s a natural emotional reaction. I’ve spoken to many boards right after they’ve been hacked and they say, who are these guys, and we want to go right after them. And after about an hour, you talk them off the ledge and explain why it’s not really going to accomplish any of their goals. Now, that doesn’t mean that the government shouldn’t be out there going after these guys, but I don’t recommend private sector does it.

MR. TIAO: So 18 USC Section 1030 is the Computer Fraud Abuse Act. That actually prohibits companies from engaging in the unauthorized access of sort of networks, right? So in this country, it is against the law. I guess in Luxembourg presumably is not, otherwise, they wouldn’t have done that.

MS. TEWS: They don’t have lawyers to tell them not to do it.

MR. TIAO: But this question of sort of active defense or hacking back has been one that’s been actively debated for a number of years now, right, because companies want to do something and that’s a very understandable reaction. And so sometimes – a lot of the debate becomes sort of, well, what is hacking back. So if what you mean by hacking back is to do what this board had been thinking about doing, which is to try to hire a company they can then actually go and hack into a company’s network in violation of 18 USC 1030, that would be a bad idea. And the FBI and the Department of Justice have made it very clear that they intend to prosecute companies or individuals who are doing that sort of thing.

But then, the question really becomes – and there are active debates about whether Congress should change the law and whether there should be sort of whether we should – and in fact, there’s provisions in one of the Senate bills that actually addresses active defense. And it allows companies to engage in certain limited active defense notwithstanding current law, so notwithstanding 18 USC 1030. So it would actually create an exception for a cyber security active defense.
That’s one issue. Another issue is, well, what does it mean to hack back? And a number of companies are actually doing things to make it less – make their companies and their networks less attractive. They’re not hacking back, but they might be planting disinfection. They might be putting information in their networks. They might be creating a sort of a honey net, if you will that, you know, when the threat actor goes in and they steal information, what they steal is this information or they steal information that slows down the company – the bad actor’s networks or they create confusion and doubt. That’s not – I mean, depending on the facts – so this is not a legal advice – but depending on the facts, that may not necessarily be a violation of 18 USC 1030. And so that is a way that the private sector may be able to impose costs or just make their networks less attractive.

And so there are some things that can be done in theory, but I think you just need to tread very carefully and with advice of a counsel.

MR. BEJTLICH: Just a quick story that gets into this grey area, though. Many of you probably know there’re these underground chat rooms, where these guys hand out and they talk to each other. And this is generally in the hacktivist, activist, Anonymous, most sect-type groups. So I have some friends who hang out on these channels because they want to find out what these guys are going to do and who they’re going to attack next. So during one of these conversations –

MS. TEWS: It’s that easy?

MR. BEJTLICH: Oh, yeah. You just have to have the proper cover and OPSEC and all of that. So anyway, these guys are in this channel and the collective decides, hey, you know what, who should we hack next? Let’s hack company A, which is the company that these guys work for. And so my friends are thinking, oh, what are we going to do about this? And so what they did was they said, no, no, you shouldn’t attack company A, they’re a great place to work. They’re environmentally friendly. They help charity.

MS. TEWS: They recycle –

MR. BEJTLICH: They recycle, exactly, and they convinced these guys not to hack company A. So that was some security money well spent, I would say. They talked these guys – now, they didn’t say, go hack –

(Cross talk.)

MR. TIAO: – company B.

MS. TEWS: But company B, they’re recycling, right. (Laughter.)

MR. BEJTLICH: I was going to explicitly say, they did not say, go ahead and attack our competitor or whatever. But what if the Bureau was monitoring that channel
and they say, oh, we see these guys all talking. There’s been talk that that could be a RICO situation, where you go after everyone in the channel because they’re having a discussion about criminal activity. In reality, the security company or the defenders are just trying to keep up with what the bad guys are going to do to get ready in case they need to buy, you know, DDOS protection or hire us or whatever the case is.

So those are some of the grey areas where we could use some clarity.

MR. TIAO: You know, and I think that one of the issues that has sort of began to really bubble to the surface with respect to Congress and consideration of amendments to the Computer Fraud and Abuse Act is what can we do to protect white hat hackers. What can we do to protect the legitimate defenders that are doing what they can and try to identify vulnerabilities and to help make our companies more secure?

And as we raised the penalties and expand the tools that DOJ has, what are we doing to make sure that they’re protected so they can do the things that they do to protect us.

MS. TEWS: It gets into sort of cyber badge idea of doing some auxiliary like the Coast Guard? I’m just here to help.

MR. BEJTLICH: I think if they were – so the Reserves are actually one place where – you know, the Military, the Army and the Air Force Reserve is a great place for people to help. The problem is what happens when stuff really goes down, when something really important happens and they call up the Reserve? Well, guess what, your favorite bank, your favorite medical center, all those people are going to be gone, they’re going to be called up. So this is one of the areas where that might not be the best answer.

MS. TEWS: And – (inaudible) – of children, like all the 12-year-olds – (inaudible) – I’m in. I was a 28-year-old because I took your identification.

MR. TIAO: I don’t think it’s going to be an institutional response. I mean, I think you need to have some sort of exception, some sort of language that protects that authority, that ability to do beneficial sort of network security that sort of begins to get close to the line because it’s the only way that we can identify where our vulnerabilities are. So many companies are now issuing they’re called bug bounties, where they’re inviting white hat hackers to identify the holes in their networks. And that’s going to be a dispersed, sort of loose, not sort of organized institutional response.

I mean, in this city, we often think about things in terms of institutions and creating agencies and so on. This is the sort of thing that we need to sort of give people the freedom to do in their homes and sort of outside of the Constitution – outside of the context of a – definitely within the Constitution, outside of the context of an institution.

MR. BEJTLICH: I'll give you an example. United Airlines just gave over a million frequent flier miles to a good hacker who had discovered flaws and reported it
responsibly. That’s a great success story. We need to have more of those, make it easier for security researchers to visit you, to be able to report what they find. Because guess what – if you don’t make it easy, they’re going to be tempted by the dark side and before you know it they’re selling their skills and getting a quarter of a million dollars to break into your iPhone because they can make good money that way.

And on a related note, you may have seen this Wassenaar Agreement discussion that’s going on. That’s basically an attempt to put an arms control framework around some of the activities that occur in this country. It’s a bad idea. And I think – what it was created for was try to limit spying software used by oppressive regimes, but pretty much universally now it’s being recognized is not working out. Or the language will scoop out all that good security work that’s done and squash it. So keep your eye on that as well.

MS. TEWS: We are out of time, so last thought or a comment as the dream team that I’ve really had a good time interviewing? You guys did all the work.

MR. TIAO: It’s very kind of you to say it. So thank you very much for the opportunity to speak to you. I think that this is a really important forum. Thank you very much for moderating such a, you know, I think it was a very useful discussion and I really enjoyed hearing your thoughts and Richard’s –

MR. BEJTLICH: I’d like to second all that and don’t be afraid if you’re not a person who deals with – you know, don’t deal with bits and bytes. You have a voice in this conversation. For too long, the technologists have dominated this because they’re seen as like great, big wizards who know what no one else knows. Everyone has a stake in this, so feel free to contribute to the conversation.

MS. TEWS: Great, thank you both very much. (Applause.)

(END)