Subject: Vulnerability Assessment: Lessons From Four Cyber Events

Introduction:
Adriane Lapointe,
Visiting Fellow,
CSIS Technology and Public Policy Program

Moderator:
Dr. Jim Lewis,
Director and Senior Fellow,
CSIS Technology and Public Policy Program

Speakers:
Robert L. Dietz,
Former Senior Councilor to the Director,
Central Intelligence Agency

Judith Miller,
Former General Counsel,
U.S. Department Of Justice

Franklin Miller,
Former Special Assistant to President George W. Bush

Robert Giesler,
Former Director of Information Operations and Strategic Studies,
Office of the Secretary of Defense

Washington, D.C.
9:30 A.M.
Wednesday, June 8, 2011

Transcript by
Federal News Service
Washington, D.C.
ADRIANE LAPOINTE: Good morning. We are here to talk today about five cyber incidents with Jim Lewis, Bob Deitz, Judith Miller, Franklin Miller and Bob Giesler. I’m going to turn it over to Jim.

JIM LEWIS: And, Adriane, you should have introduced yourself. We have Adriane Lapointe, who will be –

MS. LAPOINTE: I’m sorry – Adriane Lapointe.

MR. LEWIS: What we’re going to do here today is we’re going to bring up a set of incidents. It was hard to come up with them because every time we thought we had a final slide deck, one of our foreign friends would do something else funky and so we’d have to revise them – revise them – (chuckles) – which drove the panelists a bit wild.

But what do we want to do here today? We have some goals that are a little different from the normal discussions of cyber security. And I think – I’m going to steal Frank’s line. I think that Secretary Lynn teed some of them up for us. When we look at these incidents, the U.S. now has a national doctrine, right? And it was in the international strategy; it was previewed in the president’s May 29th speech. You’ll see more of it when the DOD strategy finally emerges in the next year or two. That was a joke. (Laughter.)

What is that declaratory policy? It’s that cyberspace is a vital national asset and we will use all means to defend it, right? So what does that mean? And we have a very experienced and distinguished panel who can go through these incidents and tell us, when does something justify a military response? When does something justify the use of force? When is Title 10 appropriate? When is Title 50 appropriate? How do we signal to malicious actors in cyberspace our discomfort or our intent to do something in response? What are the measures that we could use? We say we’ll use all means to defend it. Well, what are those means? And how would we deploy them? These are questions I don’t think have been asked publicly before.

So what we’ll do is, Adriane will bring up an incident, we’ll give some relevant details, as if she was briefing these senior officials and then they will tell us how we think the U.S. should respond, what are the constraints, what are the legal requirements. So I think this is going to be a lot of fun. They look a little puzzled now but, you know – (laughter) – they’ll snap out of it. Don’t worry. Adriane?

MS. LAPOINTE: Okay. No briefer was ever this concise.

In January 2010, Google revealed that its network had been hacked and intellectual property had been exfiltrated. The company reported that it had traced the attack to computers at two campuses in China. Google had recently clashed with the Chinese government over
censorship of the Google search engine. The State Department filed a démarche with the Chinese government but received no response.

MR. LEWIS: Do you not have the slides?

MS. LAPOINTE: I’m sorry.

MR. LEWIS: It’s okay.

Okay, so this was – this was a particularly galling incident in some ways. And the question would be, how should the U.S. respond when you see things like this? What should we do? And we’ll go through a set of incidents. Some get closer to something like the use of force, Stuxnet. Some get closer to the ability to confirm attribution. Some are directed at high-value military targets. We have one in here about breaking into defense contractors.

But in this Google episode, what should the U.S. have done, in retrospect, if you have some allegations, some evidence? And we might want to talk about what evidence is necessary for planning a U.S. response. But what would a good response have been to Google, in this particular episode? Does anyone want to – I can talk forever; I’m from a think tank. Go ahead.

ROBERT GIESLER: Well, let me pitch in – Judy, you got it?

JUDITH MILLER: I got it. Yeah, sorry for the delay – mechanical irresponsibility. Anyway, you know, couple things. I do think, going to the point of evidence, if you were actually having a real discussion with officials about this, you would know a lot more than what has just been very briefly said. You’d also know a lot that you didn’t know. I mean, I’m not saying you would have all the answers, but you would have much more available that what has just been teed up for this discussion. And you would have an opportunity to query a whole range of people in the government about what they – and at Google about what they actually knew. And so there is a little bit of, I guess, you know, inherent lack of rigor in discussing this.

And it is – the reason I’m pushing that point is that I think that happens a lot in our discussions of cyber. One of our biggest problems is that we operate at a level of generality and a level of abstraction that makes it really hard to have the kind of detailed discussion about what the U.S. should do in a particular spot. So one of my themes, I guess, in talking about this is that we should be more transparent in talking about the kinds of attacks that we’re up against and what we might be able to do in response without giving up the crown jewels of the specifics.

I mean, you can talk with more candor and effect about what we’re facing than simply saying, oh, it’s cyber and then, you know, somehow thinking you can have a discussion about that.

Second, one of the reasons that I – that I push that point a little bit is that because we never get beyond abstraction, we never actually create a policy to speak of, even though the U.S. government is now in the process of trying to do that. So you would like to have an international framework for having a discussion about this. I mean, you – you know, the law of armed
conflict applies if this were a use of force – based on the facts that we have here, probably wouldn’t be particularly applicable.

But you might very well say, you know, if there was like – you know, China had been doing this for a long time; loads of people have been attacking Google and other systems in the United States. There is a possibility that you could say, even if you can’t attribute this to the Chinese government, if they can’t control their own people in an effective way, there may in fact be some discussion that goes beyond a démarche about their responsibility and what the U.S. government properly could do to position itself in taking steps that don’t look totally ineffectual.

MR. GIESLER: Going to say, we have to – I think the nature of cyber is ambiguity. And so we’re moving into an era where we have to face policy choices with far more ambiguity than we ever have in the past. In the Cold War, where the Soviet Union engaged in egregious espionage against U.S. and nation state secrets as well as with industry, we pretty much knew it ultimately was a KGB or GRU operation and trace it back to a Soviet policy that they were going after us for a competitive as well as national security reason.

But today, in this case, university servers are notoriously vulnerable. It could have been a pass-through to a U.S. competitor launching that probe for IP from the United States, it could have been somebody from the EU looking for IP from a competitor elsewhere or it could have been a Chinese commercial competitor, as well as a Chinese government interested in that.

I note with interest, though, that our default after the Google hack was, this is the Chinese government going after Gmail to try and repress Chinese dissidents. And we made some gross assumptions. We: I’m saying media-driven dialogue made some gross discussions that – assumptions that ultimately, we never could prove. It could very well have easily been a Chinese variant to Google looking for their search algorithms in source code. So I think we have to be very careful immediately couching this as a nation state problem, when, in fact, the larger strategic issue is the trillions of dollars of IP that’s stolen every year on a commercial basis.

China introduces a unique problem in that a lot of their industry is nationalized and a lot of the agencies that are doing or sponsoring hacking also have commercial interests. So you start to have to pry out the intent of this and start accommodating for that very ambiguous intent of the actor, as well as the actual event itself.

FRANKLIN MILLER: I think that one of the things that a policymaker would have to confront at the very beginning of all of this is, what kind of constraints do we want applied to what we may be doing? And so in the world of Title 10 and Title 50, policymakers need to be very careful about setting standards which would apply to everybody else except us because however good we are, we’re not that good that we would not get caught at some point. So, I mean, that’s an overarching element for this entire discussion.

Secondly, and I think that Judy was spot-on when she talked about discussions on rules of the road. And I think there are two elements of rules of the road. One is, in the world of commercial intercourse, we’re going to have to evolve over time some way for people to protect commercial IP. And even that is in China’s interest over time. That’s something that can and
has to be worked out. And just as in the Cold War, we were able to sit down with an implacable enemy, the Soviet Union, and work out means of discussing first, strategic arms and then limiting them, there is a way forward here that requires government involvement.

I think the second part of the rules of the road, which really doesn’t apply to this case but which applies to other cases, is that even in the Cold War – to the point Bob made – there were pretty much rules of the road in espionage. I mean, there were things that we did and that the KGB did and that we didn’t do. And when one side crossed the line, there were ways of letting the other side know. And again, it doesn’t apply here, but I think the concept of rules of the road, both in an official and public way and also in an official and private way, is something that demands a great deal more thought as to how to bring actors together.

And, as Judy said, there is the problem of patriotic criminal hackers, who are either in it for their own commercial benefit or they’re doing it because they think it’s the right thing to do. Clearly, the United States government doesn’t have the ability to take care of all the hackers and the nuts running around this country. Think about the Chinese government. That’s not to absolve the Chinese government for responsibility in a case like this. But it is a problem that, again, fits into the rules of the road and criminal conduct and all the rest.

MS. MILLER: Could I just pile on one point, which is that, on the rules of the road for the U.S. and what’s at stake, I mean, I think Deputy Secretary Lynn this morning certainly made a fairly clear reference to the point that the United States is more dependent at this moment on IT than anyone else. And so we ought to be clear about that. And my own opinion is that it’s more important to protect all the stuff that we are dependent on than to protect the ability to have some agile offensive capability that we would like to use but wouldn’t like to see used against us.

ROBERT L. DEITZ: If I could, I’d like to make a general point that applies to all these scenarios, so I’m only going to mention this once. Actually, before I do, let me say that I’m expressing my own views – I’m not expressing the views of the U.S. government or any agency and I’m not – I have no insider information on any of these events, so I just want to be clear about that.

To me, the problem – I’m not sure it starts here, but it is certainly worsened by the fact that we do not have a regime, a legal regime, to address these issues. What we have are various laws basically designed against hackers or, in the case of NSA, laws dealing with foreign intelligence collection. What we don’t have is a legal regime dealing with – with the protection of IT.

If you listen to news broadcasts about hacker attacks, almost always, it’s something like, it is believed that these attacks come from Country X. You know, imagine in the kinetic world, if we were attacked with a rocket and the military came back and said, well, we’re not sure but we believe the attack came from some country. People would be outraged by that.

But the fact is that because of our legal regime, there is – it is often unclear where attacks come. And that’s, again, because there is not a legal way of doing hacking back, at least a way that’s likely to be successful. What information protectors would like to be able to do is, you
take an attack and you start tracing the jumps backward. But under current law, that’s not possible.

So what we end up with in this country is a fortress regime – you know, a fortress Pentagon, a fortress Fort Meade or a fortress America. And that’s good. I’m not attacking those kinds of defensive measures. But the fact is that that doesn’t – I don’t think is likely to be successful in the long run, any more than fortress America works in the kinetic sense.

And so what I believe is true here – and it’s true in all these scenarios – is we need a new legal regime specifically to address attacks and to – people will often say, well, wait a minute, isn’t that likely to have us have people – NSA folks, for example – running back through university servers?

And the answer is probably yes. But I can’t believe that we could not design a legal regime where that would be possible in a way that would satisfy privacy advocates. I mean, my metaphor for this is, there’s a very big difference between cops breaking into a house in order to search it and firemen breaking into a house to put out a fire. You know, I think it was Holmes, said, even a dog knows the difference between being stumbled over and being kicked. And in this context, intentionality matters.

MR. LEWIS: To just clarify that a little bit, what you mean is an astute opponent would complicate any U.S. response by doing, maybe, the last couple hops through U.S. persons?

MR. DEITZ: It’s my understanding that that’s routinely done. There are people here who probably know more about this than I. But, you know, you start with a – you make some jumps in the foreign country, then you come to this country, go through some university servers, go through, you know, my server at home and so forth, and then finally conduct the attack. And that’s what makes attribution so, so difficult.

MS. MILLER: Just one quick comment, though, which is that part of it is, it’s not just Title 10 and Title 50, it’s also, you know, the divide between military intel and law enforcement, because absolutely, clearly, the computer crimes unit at Justice – it may have to get authorities here and there, but they can do this kind of backtracking without any difficulty and they were doing it in the ’90s.

So it’s not necessarily that we don’t have a legal regime that you can’t patch together and make work. It’s just that we’re patching it together because it’s, you know, sort of trying to make statutes and authorities that were designed, truly, in a different world, a different purpose and trying to make them kind of work, instead of taking a step back, which can always be exciting, and saying to Congress, well, you’ve really got to change some of this.

I do want to agree with one other thing, though, which is that I actually think you can do this and sustain privacy rights. If you bake it in at the get-go so that you have credibility with everyone in this country about what we’re doing, you will – you can do that. You don’t have to give it up and you can, I think, create a consensus of some sort that would allow us to have a legislative change that would be at least a building block for the international rules of the road.
MR. DEITZ: Right.

MR. MILLER: I think that’s right. But I think there is one element in what Bob was saying that complicates all of this. And that is, law enforcement or the Title 50 agencies may be reluctant to reveal the fact that they can trace it back. I mean, there may be times when they will be perfectly prepared to do that and there may be other times when they’re not. And that does complicate our ability to go to this kind of a regime, although I support very much the notion that if we don’t move to that kind of a world where there is a rule of law, it’s going to be bad for everybody.

MR. LEWIS: Dragging that back to your point on there were ways in the past that we could signal the other sides when we were unhappy that they had crossed some line, does that complicate – what would that look like in cyberspace? And does an unwillingness to reveal what we may know complicate that?

MR. MILLER: Sure.

MR. GIESLER: You know, I think the signaling is both over- and undeclared at the same time. You’re not going to handle this with a demarche.

MR. DEITZ: (Chuckles.)

MR. GIESLER: That’s like theater on the international stage, okay? We’ve got that out of our system; we’re happy; now we can go on doing our business. But you also have to show that by demonstrating that that behavior has some equivalence from our perspective. So if you assume PLA is the ones that did the Google hack or PLA continually penetrates DOD networks or any nation state, for that matter, then there are ways you can noisily go about penetrating their networks, just like during the Cold War, we used to fly up and down coastlines in a very, very – sometimes provocative demonstration that says, you know, I’m going to be as aggressive as you are, and I may also have a tiered approach where I’m going to very quietly conduct intelligence operations, but at the same time I’m going to be very noisy and put some sort of equivalence operationally on this so that we can finally start having some adult dialogue at the diplomatic table. But until you start showing an actor that there is equivalence or a reciprocal action at a pain point that finally gets them to pay attention and to adjust their behavior, that will continue.

MR. MILLER: But I think that actually raises – I mean we’re probably going to use this one slide to bring the entire discussion forward. (Laughter.) One of the interesting elements in signaling, or indeed even in responding, is to understand that you don’t have to do so in the same medium. That particularly applies to countries who are not as reliant as we are on cyber. I mean, if you want to inflict pain, or if you want to signal that you have the capability to inflict pain, you need to find the point of pain. And it may not be in the cyber world; it may be elsewhere.

And that’s why I think this entire discussion is a really rich vein, because you have to figure out what the vulnerabilities of the other side are, and you’d have to be able to say, OK, to
the degree that I’m willing to – I know you’re doing something that’s a very bad thing to do, and other things could happen in other realms that would not – that would not be a good thing for you. But it requires us to think through this a whole lot more carefully rather than to go into the reflexive, well, we’ve been attacked so we’re going to use kinetic or non-kinetic or cyber.

MR. LEWIS: One of the things I worry about with signaling – and it’s not a big worry, but, you know, we had a long time to establish Kabuki theater with our Cold War opponents, and so you could do a tacit or implicit signal and they knew what it was, right? And when you talk to some of the potential opponents today, other than the Russians, they don’t have that understanding. So how would you develop this capability?

I was in China a couple weeks ago and was talking to someone from the PLA and brought the notion of equivalence forward, and it was a surprise to them. They were complaining about our intelligence vessels coming into their EEZ, and I said, well, you know, some people use ships for intelligence purposes and some people use other stuff. And that was like: What? Huh? (Laughter.) So how do we – how do we – they didn’t like that. How do we build – there’s a formal rules of the road, that you brought up, but there’s also some informal understandings or rules; how do we build that.

MR. MILLER: Let me jump in, because that’s one of my – this is one of my hobby horses, and I think it applies to our relations with other governments, whether friendly, foreign or neutral. And I think that one of the lessons of the past several decades is that we cannot rely on being too subtle. There are times when we think we -- you know, we have really communicated a message, and the other side hasn’t got a clue. And there are numerous instances.

So whatever it is we do in terms of signaling, it has to be accompanied by a pretty clear message in private to someone in authority who understands what we have done; or we could even say, oh, by the way, you may not have noticed, but we’ve done something because we’re not happy with what you did. So I think it’s a combination of really blunt diplomacy in private and whatever the signal has to be.

MR. LEWIS: Let me use that as a transition point to the next incident, because this one is a little clearer. I’m going to assert at the beginning that we have some strong ideas about who is responsible.

MS. LAPOINTE: In fall of 2010, DOD revealed that classified and unclassified military networks had been penetrated by malware resident on thumb drives given to service members in Iraq in 2008. The exploit created an opportunity for the exfiltration of classified and sensitive data to foreign servers. DOD says the attack was perpetrated by a foreign government.

MR. LEWIS: So in this case – I don’t know, but we didn’t – do you treat this as just, okay, one for their side and now we run around on the defense, or do you – what would a response look like? This clearly, I would think, does not rise to the level of being considered under international law an act of – the use of force.
MS. MILLER: Unless you knew that they left behind – unless you really knew that they left behind things that could blow up the whole system and endanger the department’s ability to respond at all. I mean, you could always get to something that’s more dramatic, but there’s nothing in these facts that would get you even close to thinking about that.

MR. LEWIS: So that’s sort of a – the leave-behind is one of the thresholds we want to –

MS. MILLER: I think so.

MR. GIESLER: I’m not even sure that would be a threshold, because leave-behinds can, in fact, have dual purposes, where you can control data, you can disrupt the integrity of that data or you just pull data off of that. But the fact that they’ve – in this case there’s well-known malware. The means to exfil the data was well known. If it was ever done or not is not subject for the debate, but as we know the data as presented to us, there was no leave-behind, as Judy said, that infers the intent to do damage to that network or the data on that network.

MS. MILLER: But I do think it makes – going back to the point that Frank was making earlier about how you don’t have to be confined to the cyber realm to think about how to respond in a variety of ways, one of the things that I’ve noticed that we tend to do is to just look at what – you know, the actual attack itself, instead of whatever – you know, the SIPRNet attack, in this instance, instead of also saying, well, we have lots of other intel sources and other ways of figuring out what’s going on in the world, it isn’t just confined to the cyber tracing back road and what they did with it. So you can in theory hypothesize that you actually through other sources realize that they actually do have some intent that goes well beyond, you know, what our particular facts are. And that would create a different discussion, I think, but that’s not the discussion that this sets up.

MR. DEITZ: My sense is that this is a – we got outwitted, and, you know, you’re not going to start a war over something like this. And I have a hard time imagining – again, assuming that there were no leave-behinds, it just strikes me that there are morals that ought to be drawn from this for our side, but I can’t imagine doing much of anything else.

MR. GIESLER: You know, we have to, I think, continually desensitize target audiences, our audiences, and particularly policymakers, in saying, you know, this has happened for the last 2000 years --

MR. DEITZ: Exactly.

MR. GIESLER: -- in conflict and in peacetime. And finding an intelligence capability inside of our network is honestly going to happen as a standard and something we have to accept. I think the military is finally grappling with the fact that our networks are going to be penetrated as a norm and we’re going to have to work on how to fight through that. We got that now.

I think from a policy perspective, as intelligence and as forensics start to roll in, you have to make sure you couch that very carefully as far as intent and, more importantly, what data we don’t have as far as the actors are concerned and the intentions. And I think that’s very
important. We tend to still overhype these things, not only in policymaking but also in the media, where it becomes a massive echo chamber that vastly outstrips what really happened on the ground.

MR. MILLER: I think that’s right. And were we having this discussion, they’d throw out most of the people in the room and then, you know, we’d have a real discussion. But someone in the room would stand up and say, well, we need to talk about intelligence preparation of the battlefield, which opens up this giant door, and I’m not going to open that door. But I think – I think you’re absolutely right. I think we have to get used to the notion that people are going to be operating inside our networks and we need to figure out which networks are going to be air gapped and absolutely sacrosanct. I don’t know whether leave-behinds are, you know, necessarily something that you draw a line at or not. And I think that’s –

MS. MILLER: Just one bit of information.

MR. MILLER: Yeah. I just don’t know. But I think that is – it’s the discussion of both of those aspects, about our own intelligence preparation of the battlefields, whatever they may be, and what a potential enemy may do and what we’re prepared to accept and what we’re not prepared to accept that forms the basis for this discussion.

MS. MILLER: There is a more fundamental point that DOD, I think – and Bob, you touched on it – is grappling with right now, which is, you know, if you can come in, if you assume that SIPRNet is open, effectively, which has not been the operating assumption for DOD, or that it can be easily penetrated when need be, even if there is no leave-behind, then that raises all sorts of questions about the reliability of our defense capability in a big way. If the commanders are worried that they’re getting – you know, that they’re being spooked or that they actually can’t use, you know, kinetic force because of the Internet connections that it relies on, that’s a big deal.

So, you know, one of the – going to Frank’s comment – one of the things that I think we ought to have more on the table than I think we’ve had so far is a real discussion about architecture. And I’m not a technical person, so when I say this, I then have to look to the people who actually know – you know, who are computer engineers and things and actually know how this system works. But I think we ought to at least start thinking about whether some of the first principles that we put forward when the Internet was first started, and the ones that we’ve been building on ever since, which are sort of speed, speed, speed, speed, as opposed to security in addition to speed and functionality – you know, I just think we need to take a step back.

And this really would require an international step back, but perhaps with some U.S. leadership around it, about whether there are things that we can do not to, you know, shut down the Internet or make it horrible, but things that we can do that actually build in some of the issues that we’re facing, not just the Department of Defense but, you know, our companies. If you look at the Sony PlayStation example, which has been in the news recently, I think the Wall Street Journal or someone reported that they had quantified their loss to date – and, you know, don’t hold me to this – something like $170 million. You know, I’ve had discussions with CEOs before where – when I was in private practice and what have you – where it was, like, you know,
I can’t invest in this cybersecurity thing, I don’t – you know, I’m not at risk, there’s no problem, you know, and quantify it for me. Well, the Sony PlayStation example, in a totally different realm than national security, I think’s quantified it in a way that would get anyone’s attention. That’s like a – even for a very successful company, that’s real money, and it goes straight to the bottom line.

And I think that might open a different way of discussing whether it’s worth spending a little more money and research to think through a different way for this architecture to operate so that we don’t have to just have the given that every system we have can be penetrated, because that’s – you know, fundamentally, that’s where we are. Defense is always going to lag offense, I personally believe, if we continue with the architecture that we’ve got. And that’s – you know, that’s not a winning game for us.

MR. MILLER: I think there are two things. One, in terms of signaling overtly and clearly, we do have to say there are certain things that are absolutely off limits. And we have to say to other countries, for example, don’t mess with our warning networks, because if you mess with our warning networks, we might do something that you would really regret. And if you found something in a warning network, I mean that should merit a very strong response, and I would say, actually, at the head-of-government level.

The second thing is, Judy’s absolutely right that defense is always going to lag offense. But we also, I think, learn from this incident and others that we can, through training, get our people to be just a little bit smarter. I mean, there is a certain embassy in town here, that will go unnamed, that for Christmas a couple of years ago was handing out thumb drives with lovely pictures of the capital city in winter. You know, don’t take the Christmas present.

So, I mean, you know, there are things that we can tell people. It’s not going to be foolproof, but we can make people a lot more intelligent about the kind of things they’re doing even on the unclassified networks.

MR. LEWIS: Under any set of the rules of the road we have been talking about – and I think we will need some kind of rules of the road – under any set of those rules, would some more forceful response to this be justified, or will this end up being like any other intelligence exploit: They got one; we didn’t; move on? I mean, what would the rules of the road look like for this kind of thing? Because in this case it was significant, it was against the military and it was a foreign government. So is it the same as everything else?

MR. GIESLER: Well, there’s one other element of this particular case, in that it actually disrupted combat operations. It impacted the flow of information in an area of operations, as disclosed in the media. So you run into analogies, well, what if a third party actually interrupted combat operations in Vietnam, and what would we do to that third party? And so the idea of the Chinese involvement in North Vietnam and Russian involvement, we still have rules of the road as far as what we would do to them, that I think remain sacrosanct even in the cyber arena. And I think you will have those rules with any nation – with any evolved nation state, in saying, you know, what you just did was a foul and here’s why, and we don’t expect that kind of behavior again.
I think the problem remains that ambiguity, is you just don’t know who to talk to. And there’s sufficient gap between the responsible officials that you can talk to and a potential actor – in this case, attribution still remains foggy -- that the responsible officials could say, I have no idea what you’re talking about.

So again, I think this is a new era of statecraft. We’re going to have to figure out how to breach that – how to breach that gap between responsibility and the action. And we’re still battering our head against that.

MS. MILLER: But that is why I at least suggested briefly that you could look at the response if you at least have it in a country, right?

MR. GIESLER: Yeah, sure enough.

MS. MILLER: You know, you can look at the responsibility that – you know, it’s not a failed state, it’s the opposite of that, but you nevertheless can look at the country’s responsibility for enforcing rules of the road for its citizens. So maybe one of the rules of the road is, it’s not enough to say, oh, it keeps happening here, it’s happened a billion times, but, you know, geez, we don’t know how it happened. I mean – right?

MR. GIESLER: Yeah, I – Judy, I think that’s ultimately going to have to be the answer. I would offer the implications, though, are that in the Estonian denial-of-service case, 17 percent of the computers that attacked Estonia were in the United States. And so if you flip that scenario and say did the Estonians then have the right to attack us, and conversely, what was the government of the United States’ responsibility for that 17 percent of that attacking force, and what could we have done under the rule of law to alleviate that pain from the Estonian government.

MR. DEITZ: Implicit in what I think both Bob and Judy are saying – but I think it’s worth making it explicit – is that attacks are really cheap. You know, in the old days, you don’t build missiles in your backyard. But these days a sophisticated hacker can do enormous harm. The attack may look to a rational player as if it came from a government, but it could well just have come from, you know, an underemployed youth. And that makes this problem much, much more complicated.

MR. LEWIS: Let me ask two things on this, though, because first, what’s the drawback to going to somebody and saying, stop, even if turns out it wasn’t them? And I guess there’s some embarrassment. I don’t know that that’s ever stopped us from doing things in the past. You know, so what’s the drawback that ambiguity creates?

And the second thing is, how much does aggregation influence ambiguity? Say you have 30 percent certainty that it was a country, it was Russia, and it’s not enough the first time; then you have 30 percent in the second incident and you have 30 percent in the third. At what point do you say, to heck with it, I’m going to go talk to these people and say, look, I discern a pattern, what are you going to do?
So, you know, I don’t – is ambiguity that big a threshold for going to someone? And then at what point does other factors other than specific evidence on a specific incident reduce that ambiguity?

MR. MILLER: I think ambiguity is a factor in a couple of ways. One is, if you go and accuse somebody or demarche somebody and they’re the wrong person, you risk having that information get back to the real perpetrator, thereby reinforcing the perpetrator’s view that I’m in good shape. And so that is one issue. When you go forward, you want to have a pretty good case. And your lawyers are going to make sure that you do, and rightly so.

An aggregated series, I think, starts to undercut the notion of ambiguity. If you – if you’re getting – I mean – you know, I was a policy – (inaudible). Don’t ask me to talk about compounded probabilities.

MR. : You can get there.

MR. MILLER: But I think the third thing – and it’s a point Bob Giesler brought up – is you do need to choose your target – you do need to choose the person to whom you are speaking with great care, because you could go into the foreign ministry at a senior level and you could talk to the foreign minister. You’re absolutely wrong. I know nothing about it. And that could literally be true.

So if you do make these demarches, they might have to be the head of the intelligence service or indeed to the head of state. So –

MS. MILLER: I think about the stealth aircraft and Secretary Gates’ visit to China and, you know – but anyway.

MR. MILLER: Yeah – no –

MS. MILLER: So it happens in other realms.

MR. MILLER: Absolutely.

MR. LEWIS: I will point out that we did – when we thought very carefully about setting up this panel, we wanted it to reflect the realities of Washington. So we have two policy guys, two operators and two lawyers. So that – (soft laughter) – that struck me as a realistic representation of – (laughter). And in –

MR. DEITZ: (Off mic) – another – is that another slander, Judy?

MS. MILLER: Yeah, I know.

(Cross talk.)
MR. DEITZ: I’ve never been in a session where lawyers were not slandered.

MR. LEWIS: But it was a subtle slander.

MR. DEITZ: You have to admit. I mean, it was an implicit, somewhat ambiguous –

MR. LEWIS: It was ambiguous and a signal. So – (laughter) – maybe that means we should go to the next incident, which is a little clearer, I think. And this one is different. It crosses the line. Why don’t you go ahead?

MS. LAPOINTE: Sure. In September 2010, as we’ll all remember, Stuxnet malware caused physical damage and wiped out roughly a fifth of Iran’s nuclear centrifuges. The sophistication of the malware has led experts to suggest that it was produced and deployed by a nation state.

In the U.S., 36 percent of industry-direct executives from critical electricity infrastructure enterprises queried in the 2011 McAfee-CSIS study had found Stuxnet on their systems.

MR. LEWIS: It – this one strikes me as there’s one area where you could say it’s not ambiguous. There was physical destruction. So it would be interesting to know if you all agreed this could qualify as something that was the cyber-equivalent to the use of force. There is actual damage. There’s actual destruction. It’s not dramatic, and there aren’t thrilling TV photos of smoking ruins, but this would, for me, qualify as an act of force.

MS. MILLER: Which doesn’t end the discussion, because even if there is a use of force by the other side against you; for example, if you bring it home to us for a second, you still have to go through an analysis of whether or not the response is then force or something else.

MR. LEWIS: Right.

MS. MILLER: And that is affected a great deal by how much damage really occurred and whether it was really necessary to use force, whether in the same realm or a different realm to respond.

So – but at least I think that the physical destruction – you know, you could up the ante and say the Stuxnet – I mean, hypothetically in the United States, if it or the equivalent, which – it attacks control machines, so that’s a big deal for the electrical grid. So, you know, if you had evidence that there were Stuxnets and – you know, across all the important – (inaudible) – of our electrical grid system and – you know, that would be a really, kind of, interesting problem.

The first problem would be, can we get this out of there before it actually makes everything crash, because that would be a disaster. And if the disaster occurred for sure, that’s a use-of-force against our country that we would then want to think about responding to appropriately and quickly.
MR. GIESLER: I’d offer in control-system attacks, the most damaging attacks have traditionally been from insiders who know not only the system but also the processes they intend to disrupt. So economically, insider threats to critical infrastructure is a big deal.

So if we were all in a room getting this intelligence briefing, I would try to, you know, throw it right back at the briefer and say, well, who says it wasn’t an Iranian insider that caused this? Prove to me that somebody else did this, as opposed to an insider. Prove to me that it actually happened. A lot of this is anecdotal. And prove to me what aspects of this attack were nation state versus economic? What — were the Iranians being — or extorted? You know, I’ll take out your nuclear reprocessing capability if you don’t give me $2 million, which is something we actually see a lot of in global — (inaudible).

So there’s a lot of questions that still have to be answered. Now, as you start tearing apart Stuxnet, you start seeing aspects of a nation-state attack. It was very limited, very targeted. There obviously were lawyers involved who said, you know, make sure you limit the attack proportionally to what you — what your objectives were. I’m speculating now. So one infers that this was a mature nation state saying this is what — these are your limits. One infers that they actually were concerned about international law when they were crafting that. Or because Stuxnet ultimately proliferated, there was either an element of desperation or somebody goofed as far as tradecraft’s concerned.

So I think everybody can authoritatively say that it was a nation-state attack. Nobody has been able to attribute it -- you know, again, the ambiguity of the cyberarena. But the point is, I think, Stuxnet uniquely has — or I should say lowered the threshold for conflict in the cyberworld, because somebody got away with it. Somebody actually damaged a strategic aspect in another country, and I think we now have to say that inherent threshold of deterrence or inhibition for cyber operations has been lowered inextricably for the first time in history.

It’s an interesting concept to explore, because now you have to start saying who’s living in the glass house, and are we prepared? Are the Israelis prepared or — for that matter, or are the Chinese prepared for the next round that is going to inevitably occurred? Because now that Stuxnet out, somebody has the architecture for some advanced payloads and for some advanced control-system attacks that I think we haven’t heard the end of Stuxnet.

MR. MILLER: Three points. I mean, the first is I don’t know that you can set as a threshold the fact that something was destroyed. I mean, it is very serious, but then again, can one say that there’s never been an intelligence operation, ours or somebody else’s, in the history of the Cold War that didn’t destroy something? I mean, Tom Reed’s (sp) got a couple of books out where he says that we blew up a Soviet pipeline in the 1980s. I don’t know whether it’s true or it’s not true, but, you know, OK, take that as a given.

So the question is, is the physical destruction of something the red line, or is it physical destruction which threatens great losses that — we’ll come that that later. So, I mean, that’s sort of — I think physical destruction — yes, no — impact of that destruction. And then Bob’s point, which I think is really worth hitting -- and whoever was behind Stuxnet, one hopes, thought this through — having taken this kind of an action, you would expect that the other side might mount
some retaliatory action. What do you have to deter that, you know? Is there in the world that none of us know about a signal that said “we did this, but don’t even think about coming back” because – and I don’t know that either, but you’re absolutely right. With advanced payloads, people need to think about what the third and the fourth and the fifth step is down the line. And I would think anybody coming in with the really bright idea to an NSC or a principals committee or deputies committee meeting had better have that sort of chain of events thought through at least having built the plausible case that you could get through all of that.

MR. DEITZ: I would just add to Judy’s point, seems to me the issue’s not only the immediate destruction but what else was put there. It seems to me that – and this applies, of course, to our next scenario – but it’s one thing to down something. It’s another thing to put in Trojan horses or whatever; logic bombs, they’re sometimes called, that can cause enormous damage down the road when certain events happen. And it seems to me you’d want to look at those very carefully as well to decide what kind of response is needed.

MS. MILLER: And I used the electric grid in the United States as an example –

MR. DEITZ: Yeah.

MS. MILLER: -- and said a hundred percent takedown –

MR. DEITZ: Yeah.

MS. MILLER: -- as a premise for saying, OK, that would be something that you would want to think really seriously about responding to appropriately – (chuckles) – right?

MR. LEWIS: Yeah.

MS. MILLER: But if you took down instead a tiny bank in – I’m not trying to pick on any state, but some bank someplace that really didn’t have any impact on our economy at all, that would be a very different kind of analysis. Then even if it physically destroyed that network or that little bank, you know, you’d probably not be thinking that we’re starting World War III.

MR. LEWIS: So the scope issue is something we’re just going to have to kind of grope our way towards?

MS. MILLER: Yeah, but –

MR. DEITZ: But scope –

MS. MILLER: I was just going to say, but do it all the time in the kinetic world –

MR. DEITZ: Sure.

MS. MILLER: – and that’s one of the things – this is not – I mean, it’s not rocket science to apply the standards that we have and we’ve used, you know, routinely and, I would argue,
reasonably successfully for, you know, decades in the kinetic world – it’s just that we’re not used to doing it, in part because – going back to my sort of opening point – we’re not transparent enough in talking about what these capabilities are, and we haven’t gotten – we just haven’t gotten practiced enough – and I think through exercises and simulations we could get more so – to actually think through these issues so that when Frank says you’re walking in – you know, if you are walking into a principals or a deputies meeting to talk about some of these issues, the people around the table are not like all deers (sic) in the headlight, we don’t even know what you’re talking about; but instead, they’ve been through it and the way they’ve been through a whole variety of other things that are endemic to national security discussions.

MR. DEITZ: Scope, I just want to add, not only sort of the breadth of the damage but also lying there at the future, cause for potential – (inaudible).

MR. LEWIS: Yeah, I think that those two points are kind of crucial ones in that we have treated cyberwarfare, cyberattack as this, you know, unique thing. And the more we can push it into the realm of traditional experience, noting that there will be areas of ambiguity, that the more we can say that the laws of armed conflict apply, the easier this will be to deal with and the easier it will be to think of responses.

MR. MILLER: But this is –

MR. GIESLER: I was going to say, I think universally, all four of us have lived through that. And the more you deal with cyber, the more you realize it is the same. The same rules of the road apply. The same rules of armed conflict apply in international norms. There’s some fuzziness on the edges, but I know these two in particular have beat me over the head years ago on that topic.

MR. DEITZ: Only when you deserved it. (Laughter.)

MR. GIESLER: And I was encouraged.

MR. MILLER: But I think as we talk about scope, it reverts back to an earlier part of our discussion about rules of the road. And picking up on Judy’s point, a small bank in some state may not be a big deal, but as the world is just so linked in terms of e-commerce and e-banking, it may not be impossible to develop a rule of the road among nation states that you don’t touch the financial sector. I mean, unless it’s World War III, you don’t touch the financial sector because everybody’s implicated in the end. You don’t touch electrical grids – and we’ll come to that. But there may be areas where you can actually get people to cooperate.

MR. DEITZ: You know, I share the view of my colleagues that we do have models from the kinetic world that are applicable. So it’s not – this is not all new. What does make it, I think, somewhat different that we need to understand is, again, some really bad, destructive stuff can be done by just a couple of people. And that’s different. And, I mean, I can – I can easily imagine a scenario in which we demarche some government, and they said, well, we have no idea what the hell you’re talking about and mean it.
And so what I expect might be a little bit different in the future is some of this may end up being more police-style action as opposed to, you know, armed conflict kind of thing.

MR. GIESLER: But again, Bob, we have traditional models for law enforcement.

MR. DEITZ: We do. We do.

MR. GIESLER: And I think the whole debate after 9/11 was how we handle terrorism –

MR. DEITZ: That’s a good point.

MR. GIESLER: -- where terrorists can do massively destructive things and there’s no nation state behind them – (off mic).

MR. DEITZ: Good point.

MR. LEWIS: A good way to test somebody’s response – if you went to another government and said what happened and they said “we have no idea,” maybe the next question should be then, OK, so cooperate with us in the investigation –

MR. DEITZ: What are you doing, yeah.

MR. LEWIS: -- by the law enforcement guys. And if they say no, which at least some of our opponents right now would probably say no, you know, that’s a good tip, you know? So there’s – maybe the next step here is, OK, it wasn’t you. I accept that. Help me investigate.

MS. MILLER: And that’s part of the responsibility of the – that – of the nation state that I was trying to suggest earlier, which is, no, you can’t just say, oh, well, it’s happened, but –

MR. DEITZ: That’s life.

MS. MILLER: That’s life. There’s more to it. But I do think – even – now I’ll sort of switch back slightly. I do think there are lots of sort of examples in the kinetic world that we’re used to that absolutely apply here. But the fact that people don’t get it right away, I think sort of requires us to have a more explicit international conversation about what those rules are and how they do work in this world, even though it shouldn’t be rocket science to figure it out.

MR. LEWIS: What would that international conversation look like? This is a self-interested question.

MS. MILLER: (Chuckles) – well –

MR. GIESLER: I think we send Jim Lewis someplace.

MS. MILLER: You go first. Right, yeah, exactly. I mean, I think it’s hard, because you could – I remember seeing some – you know, there were some efforts, as I recall, pushed in part
by Russia in the ‘90s that had some sort of complexity behind the motivations. I think they were – at least we perceived. And so I don’t – you know, I’m not saying it’s necessarily easy to do, but I think as – I think as countries over time – and I don’t know how quickly a country like China will recognize that the tipping point has come where it has a lot at risk, as much at risk as it does in the game, you know. But, you know, over time countries are going to get more sophisticated about how if this can hit Iran, if it can hit the U.S. Supernet (sp), if it can hit Sony Playstation, if it can hit all these things, maybe there really is something there that we ought to be talking about. And, you know, we sort of do – we have treaties for lots of stuff. We can start having a process that would lead whether to a treaty or just rules of the road, but there are various convening mechanisms that we’ve used in the past. I think we should settle on one or two and go for it.

MR. LEWIS: Someone from the PLA said to me a little while ago that in cyberspace, America has a big rock in its hand, but it also has a big plate-glass window, right? And they realize now – he said China now realizes that we have a rock, but we’ve also got plate-glass windows. And he was sort of making the, you know, mutual-vulnerabilities argument, which I thought was neat.

MR. GIESLER: But what’s interesting is there’s asymmetries in that plate-glass window. And if you talk to PLA, their concern on the Internet is Internet freedom and the ability to control voices and potential internal unrest. Go to the Middle East – the same way. If you come here, you’re going to have a conversation about catastrophic process-control system attacks, you know, the electric power grid or the air traffic control system.

So I think any time you go internationally, you have to be prepared to talk that asymmetry and say, OK, if you let up on taking my IP, I may – I may consider less – relooking our Internet freedom policies and – because you – you know, if you go to the EU, that conversation is going to be so infused with privacy issues, it’s going to be a completely different conversation. So you have to be prepared, I think, almost in a bilateral as opposed to multilateral conversation, to deal with those coming Internet asymmetries.

MR. MILLER: But I think you just opened up a door that we all should have opened up a while ago. And that is, there is a linkage between what happens in this world and the other kinds of policies that we’ve pursued. And so without passing judgment on the administration’s Internet freedom policy – I mean, clearly some governments view that as an extremely unfriendly act. There’s always been – well, always – certainly since the Carter administration and before, there has always been a debate within an administration as to the degree to which human rights becomes – (inaudible) – of our national security goals. And the world is connected. And I think that, again, is something that would have to enter into all of this. And there may be areas where we say we’re going to throttle back a bit on that policy because we understand that we are causing you internal political problems, which are serious and which lead to possible loss of political control.

So I – that is – and it becomes more complicated, because that is a very divisive issue here at home, but it cannot be carved off of this broader international discussion, perhaps even rules of the road.
MR. DEITZ: Before we go marching off to some international conferences, it strikes me it would be useful to focus on some U.S. policy as well.

MS. MILLER: As the first step.

MR. DEITZ: We’ve got – you know, you could – you could hook up any old piece of equipment to the Internet, you know. I find it astonishing – let me say that I’m either burdened or blessed with an ignorance of the technology involved – (soft laughter) – but, you know, when you – when you take the cheapest piece of electrical equipment, there’s a nice tag on it, the UL. And it basically, as I understand it, is certifying that when you plug it in, the device isn’t going to blow up.

So far as I can tell, there’s very little – and there’s nothing equivalent to that in the computer world. And so all kinds of devices can be hooked up to the Internet that are extraordinarily vulnerable. And it seems to me that, you know, under the – under the – under the Interstate Commerce Clause of the Constitution, Congress could easily say, look, there are so many vulnerabilities here, we’re going to tighten up the laws on what’s allowed on the Internet, what devices and so on. Now, I know the Internet’s the vaunted freedom and so forth, but, you know, even Dodge City eventually realized that some laws were useful. And I think we’ve gotten to that point in the Internet world.

MR. LEWIS: One of my rules is never to talk about liability, so I’ll just skip that one. I will come back to it, but let me go to the Internet freedom one. I’ve had both Russian officials and Chinese officials tell me information is a weapon, and the U.S. uses against us. And the classic line for me was a Chinese official told me that Twitter was an American plot to undermine governments. So – but –

MR. GIESLER: But that’s a legitimate – a legitimate observation. You have to factor that obviously when –

MR. LEWIS: Yeah. They also don’t assume that we don’t have greater and greater control over our media than we actually do.

MR. : Right. Right.

MR. LEWIS: I mean, they control theirs. No grown-up country would just let a newspaper – they don’t believe it. So what do you – what do you do in a situation like that? And one of the things that has come up as an idea – and don’t scream – is to harken back to the Helsinki Accords, where you got a certain degree of freedom in exchange for something, recognition of borders, that the other guys wanted. Is that Helsinki model reasonable for this sort of approach? What would it look like, and what would we – we don’t know.

MR. GIESLER: I think we have to acknowledge that the Internet is becoming increasingly nationalized. Syria cuts the entire country off from the Internet, Iran tried to do that; Iraq certainly tried to nationalize the Internet for keeping the population at bay. We certainly
saw the infrastructure when we rolled into Baghdad for that. And I think we have to recognize that the Internet as we knew it is changing rapidly and that it’s becoming an instrument of state power, just like every other capital asset that we faced in the history of mankind.

And I think that’s going to drive such a multiplicity of policy complexities that we’re just going to have to – you know, we’re going to have to deal with far more nuances than we previously have in Internet policy. And I’m not sure we’re there yet.

MR. MILLER: To an authoritarian state, freedom of information is a threat. To us, it’s the lifeblood of our political process. And to the degree that we insist that we’re going to – it’s like Radio Free Europe. The Soviets jammed it, we kept broadcasting. But this is more serious because it can reach hundreds of millions of people. And it’s the kind of discussion – again, I’m not prepared to, off the top of my head, come up with an approach, but I think the idea that you came up with, which is a Helsinki Conference that talks about various national security requirements is not a bad place to start.

MR. LEWIS: We’re – to keep on schedule more or less, why don’t we go to the next slide. And that takes us a little bit away of where we are at the end of this conversation and it gets us back to the middle of the last conversation.

MS. LAPOINTE: Certainly, the phrase “free flow of information” means radically different things to anybody – to the different countries that use it. As of spring 2011, U.S. electrical company networks have been probed thousands of times every week. Forty-six percent of executives surveyed said that their companies’ networks had been infiltrated at least monthly. And 74 percent of them believe that there will be a major cyber incident within the next two years. Senior intelligence officials say that some of these intrusions represent reconnaissance by potential opponents.

MR. GIESLER: So let me get on my soapbox here. (Soft laughter.) You know, briefers, show me the data. Show me the intent that it’s reconnaissance as opposed to a – I love picking on the Chinese – as opposed to a Chinese company who was interested at how a U.S. electrical power utility accommodates for weather fluctuations in its loan-balancing operations? You know, we see – constantly see the collection of data between nation states for commerce purposes. And yet somehow we automatically tag everything in the cyber arena as a national security threat. And I think we have to resist that constantly and constantly batter people like you, Ms. Briefer –

MS. LAPOINTE: Thank you so much.

MR. GIESLER: -- to say what assumptions have gone into this? Show me the data. And if we have none, don’t make that leap, because bad things happen when we make leaps in the national security arena. In fact, in the cyber arena, I would suggest the data says this is not a national security problem. Google, this is your problem. You got in bed from an industrial perspective in China, and you knew that was a hostile environment. You knew that was an ungoverned terrain, and you should have been better prepared. Electric power utilities – you have IP you need to protect. You have operational methodologies that even your competitors
would like to have. And they can go phishing on the Internet. So shame on you, but let me help you fix that.

But if for us from a policy perspective we constantly see ill intent at the nation-state level, then I don’t think that’s good for not only the public-private dialogue as public policy. It certainly isn’t good for international relations if we go jumping into these things with those assumptions a priori.

MR. DEITZ: I agree with Bob, which makes me –

MR. GIESLER: That is scary.

MR. DEITZ: -- sort of question myself. Bob and I are old colleagues. I hope nobody takes that seriously. I agree with him. It – I suspect it’s very tempting for executives of any private company to want to shift costs to a governmental agency. We’re being attacked – implicit in that is you the military or you the police force, you’ve got to stop those attacks on me. I don’t think that’s necessarily an accurate assumption. And it seems to me that Bob is right in the sense of, look, if your system is so vulnerable that you’re being attacked – was it – I mean, the statistics –

MS. LAPOINTE: Monthly.

MR. DEITZ: Yeah, monthly – maybe you ought to tighten up your system and limit that.

MS. MILLER: But, you know, it’s interesting because FERC has some regulatory authority over the grid –

MR. DEITZ: Right. Yeah.

MS. MILLER: -- specifically on this, but it’s very soft.

MR. DEITZ: Yeah. Right.

MS. MILLER: It’s just that they get to review the standards put forward by, you know, the kind of industry group that comes up with them.

MR. DEITZ: Exactly.

MS. MILLER: So the – so nothing’s really happened. I mean, this is a discussion we had in the ’90s. We’re having it right now. Nothing really has changed, although the – perhaps the ability of attackers, whether they’re nation states or just kids, has grown apace.

So, you know, there’s legislation pending on the Hill, and there’s also part of the president’s own initiative to do cyber different approaches – you know, my own bias is that on the electric grid, putting aside whether we have definitive evidence that it’s doing something really malicious right now, it’s clearly a vulnerability and we’ve got to find a way to address it. And I
think you have to mandate some standards from Congress. That’s my personal opinion. That may not be what everyone else thinks. And then you probably have to find a way to finance it, because the utility companies are still in this mode, for better or worse – you know, they’re rate-based. You know, they don’t really want to do anything unless they can – (inaudible). You know, it’s perfectly rational from their perspective. They’ve got to pass the costs on, and if you don’t have a basis for doing that, then they’re not going to spend the money.

So you’ve got to have an integrated approach. I actually think we ought to pick off the grid as a specific example and get it done even as we’re working these others things.

MR. MILLER: I agree. I agree with Judy. Absolutely. And I take two directions. One, based on some experience I had a couple of years ago consulting with one of the larger cyberdefense companies in town, the electrical companies are just not interested. They’re not – they’re not going to spend the money to protect the grid. And I think they should be made to do so. And there may be some federal assistance, but I think that it has to be done.

But I think also this is the kind of message that needs to be put out by the United States government publicly that interference with the grid constitutes an extremely serious act with – which could lead to potential loss of life in the United States and which would be subject to very serious retaliation, whatever that may be.

You know, we here – we here suffer outages after a thunderstorm, and things are bad. I was recently in Tuscaloosa, and after the tornado, they lost power for about eight days. They lost power, they lost water. You know, I mean, you can cascade this.

If you lose the ability to generate or distribute power to an entire region of this country, we are going to be in very serious trouble as a nation. There will be loss of life; there will be huge economic impact. And it is not impossible to take over portions of the SCADA networks and destroy generating capacity, which we don’t have the capability to manufacture in this country anymore. There’s a lag time of, what, two years? So these are serious actions. And I think these are the kinds of things where you’re absolutely right. We need to push industry with legislation, if necessary, but we also need to put down very clear markers. And to me, the two key areas that are right off the bat are the financial sector and the electrical distribution network.

MR. DEITZ: Beyond electrical distribution, pipelines, you know, the whole SCADA industry out there.

MR. MILLER: Yeah. Absolutely.

MR. GIESLER: I think there’s an interesting argument I had about the efficacy of the compliance regime in cyber and witnessed what I would call a – (inaudible) – that, you know, over a period of four or five years, cost $3 billion. And one could argue that the .gov domain is no more secure at the end of that $3 billion. So I think it’s a hybrid where you’ve got to have compliance, a regulatory regime, as well as an assistance regime, but from the – you know, a true partnership between the U.S. government and critical infrastructure that isn’t where the government comes in and beats some poor utility over the head, but actually comes in and helps.
And I think there’s some encouraging trends from both the national security side and DHS, it – moving away from that purely compliance into an assistance regime. And I think that’s – I think that’s the actual key for critical infrastructure – (inaudible).

But I will tell you, they are operating on razor-thin margins, as Judy alluded to. And if you roll in and say, you’ve got to harden all your networks to – up to nation-state standards, they’re just going to roll over and die. So you’ve got to come up with a better solution than that.

MR. LEWIS: That’s why I thought what Frank said was kind of interesting, because it links us back to the – (inaudible) – which is, there are domestic measures you need to take. You know, Bob has brought up some. But there’s also international measures, and you need them both. You need to have some way to tell other countries, this is a particularly sensitive area. And it’s – you can’t do one by itself. We haven’t ever done this before. One by itself is inadequate. And a lot of our cybersecurity focus has been on domestic side, albeit somewhat fecklessly, for the last 15 years. And we’ve never actually done the sort of declaratory approach. And I think you –

MR. MILLER: And somebody will immediately jump up and say, well, now you’re drawing Acheson’s red line in some sand. Everything on the other side of the line is up for grabs.

MR. LEWIS: Right.

MR. MILLER: And I understand that point, but that doesn’t justify inaction and signaling.

MR. LEWIS: This is – this would also seem to be a sort of activity, if it was a government and if they were doing reconnaissance, it is something that we would normally tolerate. It’s a little bit different because they are intruding into U.S. space in a way that other reconnaissance activities didn’t. But if we pushed –

MR. DEITZ: Satellites. You know, I mean they’re photographing down.

MR. MILLER: Well, I – no, that’s – that’s true.

MR. LEWIS: I don’t know that I agree with that.

MS. MILLER: Human spies on the ground.

MR. DEITZ: Yeah.

MR. MILLER: I don’t know that I’d agree with that. I mean, it’s one thing – I don’t know – associate you with my (work ?). It’s one thing to do military targeting. I mean, and God knows we used to have lots of discussions about what targets were legitimate and what targets are not legitimate, and that’s in the kinetic world. If we – well, I don’t know. (Inaudible, laughter.)
MR. DEITZ: I was waiting where this was going.

MS. MILLER: Right. Me, too. (Inaudible) – with baited breath.

MR. MILLER: I’m not sure where it’s going. But I do – I’m not – it seems to me that this demonstrates hostile intent. And to the degree that we can identify the source – let me be clear. Bob’s right. Briefer needs to make very clear that there are leave-behinds that in fact could be activated to disable or destroy the network. But if one found those kinds of things, then I would take that extremely seriously. I expect the government to take that extremely seriously. We were at war with Iraq. We took out the electrical generation – or distribution system and in some cases the generation system in ’91. I was not privy to those discussions at the time. But as – if I were a government official, then I would take this extremely seriously.

MS. MILLER: Well, and to just sort of – when you talk about – and certainly electricity generation is part of the command and control structure of most hostile forces, if we’re actually in a war. And so you then have – you can then, in fact, have a discussion about whether that is an appropriate target, what does that do in terms of collateral damage, is that acceptable if duration is really a big deal? Are you just – there’s a whole set of issues that you can go through in the kinetic world. You have to do the same, I think, in this world. But if your conclusion and your briefer is strong enough and your conclusion is that this predatory activity could take down the entire electrical grid of the country for six months, as opposed to 20 seconds, that would be a big deal, you know. So it just – it really – I mean, the facts actually matter here, as everywhere else.

MR. LEWIS: Suppose there are no leave-behinds, though? Suppose it’s just planning to do a leave-behind? What do you – in the kinetic world, you know, you’ve lowered the temperature and you just sort of – we’ve talked about we’re going to have to get used to living in a world where networks, albeit changes along the lines of what Bob and Judy have said – networks are indefensible. So do we just grin and bear it or do we –

MR. MILLER: Well, I think you do two things. One, you heighten your defenses. We get back to that discussion as to how you pay for it. But there’s also a word that’s crept into the lexicon both here and on Mark Grossman in one of his State Department studies when he was on the outside and did a study for State Department on cyber – and my friend Sir David Omand in the U.K. is using – and that’s resilience. And we need to look at ways to be able to suffer some damage and still to be able to recover. And that is – again, it’s a government policy in cooperation with industry. So one prepares for worst-case situations and decides what triage is necessary, and makes certain that one has the capacity to do that triage.

MS. MILLER: But that’s why I’ve also talked about architecture and going back to first principles.

MR. : Absolutely.

MR. : Absolutely.
MS. MILLER: Because, you know, the Internet grew in this marvelous way, helped along by DARPA originally, and with – and optimized around principles that made sense at the time. But they could be rebalanced, I would argue, and that might make it possible to have, you know, less abject inability to actually defend the network. So, you know, I don’t know whether that’s – you know, I mean, I don’t think it’s an easy task exactly. But, you know, some of my tech friends say, actually, you know, it’s just that no one’s ever – it hasn’t – no one will pay for it, and it hasn’t been a priority as a result.

But again, looking at some of the real damage that’s been inflicted just on regular people like Sony and Lockheed and a variety of other people – you know, this might be a moment where you could actually get some smart people to reconnect on whether there are some things that make sense.

That doesn’t mean the end of the Internet as we know it; just some things we could do to actually make it easier to build security along with privacy and freedom –

MR. DEITZ: Some people have actually suggested a parallel Internet – I mean, one where you would pay a monthly fee for security and, you know, that kind of thing – whether there’s a business model for that, I have no idea. But it’s certainly true that the Internet as initially – DARPANET was never designed for these levels of subscribers and volumes, and so on.

MR. MILLER: I think there’s .mil; there’s .gov. And I think there’s “.critical infrastructure.” And I think those things need to be protected.

MR. GIESLER: You know, the Cold War analogy is, the U.S. paid to harden some aspects of critical infrastructure during the ’50s and the ’60s, and sustain that – run by private industry, but it was federally funded. I think the same can be said for critical infrastructure now from a cyber perspective.

And the resilience issue is interesting, and I think the deputy talked about it this morning when he suggested that there is, you know, an aspect of deterrence that comes from resilience and complexity, as opposed to a big, strategic target that is extremely brittle, that will guarantee and attract hackers like flies. You know, let me see how big a bang I can achieve.

And yet, if we build resilient infrastructure that is hardened, that is continually updated dynamically against new threats, all of a sudden, you’ll find them going after softer targets. It’s like putting a thing on your steering wheel so that somebody steals the car next to you. Well, the same phenomena happens – (laughter) – in the cyberworld. You know, you still get through it, but you know, you just want them to go after Frank’s car instead after –

MS. MILLER: Yeah. Although, there’s a counter to that, a little bit, which is that what you really do if you do all that stuff and you don’t fundamentally change how it operates, is that you make it harder for the kids and the people who are not super-sophisticated. But you still – but you sort of weed out some of the real jerks.
But the – if you have kind of strong people out there, whether nation-states, organized crime, or whatever – who really spends the money on it, you still will be vulnerable. But it does at least narrow the playing field in terms of –

MR. DIETZ: Better than nothing.

MS. MILLER: – what you’re supposed to be looking at.

MR. LEWIS: One of my assumptions is that that is the path we’re on, that – you compare who had capabilities 12 years ago when it was, you know, three kids in Mendocino who could hack DOD. And we’re eventually going to squeeze that lower end, and we’ll be left with nations, advanced criminals, maybe a few others, maybe some terrorists.

And so I think we’re moving towards the high end, and that’s where some of these issues might come up, is that – we’ll be in an environment where our – where we have fewer opponents and not a – fewer opportunities, but we’ll have a harder time stopping them.

MR. GIESLER: But that’s when the whole-of-government approach and law enforcement, in particular, has to get involved. You know, and I think from – the original CNCI simply talked about technology. And I think that’s where – later strategies coming out of the U.S. government, I think, are more important because it – you know, against the nation-state threat, no amount of network hardening is going to stop a dedicated attack forever. So you got to have the diplomacy, you got to have international legal regimes that provide you that holistic solution set.

MR. MILLER: And you could have a deterrent, you know? And you got to figure out what makes the other side hurt, and you have to make clear that if certain things, life won’t be much fun at home.

MR. LEWIS: Let’s use that as a transition point here to the final incident, where I’m going to be a little more gung-ho, and Adriane is too. We’ve changed the name to protect the innocent, as they used to say on “Dragnet.” You can probably figure out who this was.

MS. LAPOINTE: Yes, it’s not too subtle.

MR. LEWIS: Speak for yourself. (Laughter.)

MS. LAPOINTE: So this month, phishing techniques were used to compromise authentication technology used by DOD and major defense contractors. The authentication – (audio break) – put to use in an attempt to penetrate defense contractor networks and exfiltrate data on advanced weaponry.

Based on forensic evidence, the companies involved suspect proxies on behalf of what Jim characterized as a foreign intelligence service in Asia.
MR. LEWIS: OK, so this one – you’re all smiling; I don’t know if that’s good or bad. You know.

MS. LAPOINTE: It was subtle.

MR. LEWIS: This one is interesting for a couple reasons. First, it was a two-step, kind of like Stuxnet, right? Somebody did – we are making some assumptions here, and you could push back on that. But somebody did something that was a preparatory action that was then used later in what would appear to be a more classic espionage activity.

So what’s the response here? And some of the variables might be, how often have we seen this? Is it the same actor? How confident do you feel? If you don’t know what was actually lost, does that inhibit your ability to respond – you know, if the outflow was encrypted and you don’t have a good sense? What do you do in a case like this?

And this is the kind of thing I think we’re going to see consistently in the future: very sophisticated setup to an attack.

You’re all going to take the Fifth – you can’t do that. (Laughter.)

MR. GIESLER: Well, look – well, again, to beat up on the briefer, what you haven’t told me is, was anything lost? You know, we’re describing an act of espionage, whether it’s industrial or nation-state. But you haven’t told me whether there was any damage. You have described a methodology that is a little bit more sophisticated in that, instead of one key that I had to – in order to break into the dungeon, I had to go steal one key – I had to steal two, in this case, in order to get both keys in the same lock.

But it’s fundamentally the same act – the techniques and tactics leading up to that were a little bit more complex. And it’s good news from a defensive side. You forced the attacker to actually do a lot more work, but unfortunately they did that work very well, and did an attack. So we haven’t seen the rest of that story.

But again, I’d recommend – and the media went absolutely crazy on this – again, when they didn’t have any of the data, it says, OK, they did an attack; they did it nicely from a technology perspective. But was there ultimately no story in it? Nothing was lost.

You know, I think, we from a policy perspective, need to hear the rest of that story before we start building all our options that we would present to the White House.

MS. LAPOINTE: But will – can we expect that from industry, necessarily?

MR. GIESLER: I’m sorry?

MS. LAPOINTE: Can we necessarily expect industry to want to give us that information?
MR. GIESLER: You know, I think in this case, you know, with the defense industrial base, there is a great dialogue. You don’t bite the hand that feeds you, so that’s –

MR. DIETZ: Yup – lot of leverage.

MR. GIESLER: Exactly. But I know of cases where that hasn’t happened in the past, and particularly, the farther away you get from government contractors in a purely private sector, my recommendation to my former government colleagues in responding to those kind of answers – don’t roll in and say, give me everything that just happened to you. Roll in and say, let me tell you how I can help you. And then, all of a sudden, you’ll find that dialogue opening up significantly.

MR. MILLER: Let me damage my reputation – (laughter) – a bit. It’s interesting that with the explosion, huge growth, of public posture of the Internet that espionage activities like this get a lot of press play. You know, in the past, if you could burrow in and find something, or get something, people got intelligence medals and nobody was the wiser.

Well, OK – so now it shifted into this realm. This honestly doesn’t excite me very much because it implies – and I have no knowledge – it implies that we’re not doing the same thing to other countries. If that were the case, I would think that that percentage of my tax dollar that goes to the IC is being badly spent. (Laughter.)

So this is going to happen. Shame on us or on our companies that allow really sensitive data to be classified as FOUO, or unclassified, and store it in places where people can get at it. But I mean, this is what intelligence organizations do. And OK, so now it’s on the Internet. This is – this has been going on since time immemorial. This doesn’t bother me that much.

MS. MILLER: It can bother you only in the sense, I think, of the authentication technology that people thought was a strong protector.

MR. MILLER: Sure.

MS. MILLER: So it kind of, again, lands – and maybe one of the reasons the media has been excited about this is, to the extent some of our most sophisticated companies thinking – and the department – thinking that they can rely on this particular kind of technology as another firewall – not officially a firewall, but, you know, a real protective device, and that behind it, you don’t have to – I mean, you still have to have, cyberhygiene, all that stuff. But it’s really something that you can kind of rely on, and this shows that you can’t.

And so what it really does is deliver the message again, which we’ve been saying throughout this discussion, that there isn’t any, you know, sure way of protecting stuff right now. And you know, that’s something I think we really ought to grapple with. Because while it’s – you’re absolutely right, Frank, that it’s always gone on, you know, it’s still in our competitive interest economically, among other things, not to have everything flow in one – (inaudible). Right?
MR. MILLER: Just because this can happen doesn’t mean that we should allow it to happen in terms of allowing data to be unprotected. But as far as carrying into the state-to-state realm, that’s a different story.

Again, shame on us for having data – I mean, what was the story a couple of years ago that there was enough – all the data that was stolen was unclassified, but when aggregated, became classified.

Well, you know, we’re the people doing industrial security at the various companies. That shouldn’t happen. That’s our fault.

MR. LEWIS: I have to admit, I admire the guys who figured this one out because they identified a crucial target that could give them multiple points of entry. So I hope they do get a medal – (laughter).

We’re at the end of our time, and I’m going to do two things. I’m going to quickly say what I got out of this – I thought it was a great panel, and you guys did better than I expected – (chuckles).

MR. DIETZ: Thanks.

MS. MILLER: (Inaudible) – low expectations.

(Cross talk.)

MR. DIETZ: Damnation with faint praise.

MR. LEWIS: I had tremendously high expectations, and they of course exceeded it. (Laughter.)

I got to say quickly, the couple points I got out of this – and I’m going to ask you if you have any final quick words here. I thought the emphasis on ambiguity and uncertainty was interesting. And the notion that we’re in a permeable environment that may not be fixable absent some very large, strategic level changes – the application, the ability to extend the rules, and how we think about policymaking in law that we use for kinetic incidents, the ability to extend that in the cyber as a useful path, and one that’s probably the best thing.

The whole-of-government approach, right, as a way to think about this problem – particularly the rules of the road internationally; ways to signal potential opponents; build common understanding – so I thought that was great.

And finally, the whole discussion of critical infrastructure dragged in something that doesn’t get dragged in very much, which is – you know, for these guys, it’s a business. And they have to remember the magic letters “R-O-I.” And how do we – how do we get into their thinking about investment? And the example of hardening the telecom structure during the Cold War is a classic where we basically paid – we, the government, basically paid for that.
So got a lot of good stuff out of this. Any final words from our distinguished colleagues?

MR. DIETZ: Yeah. If I could just make a comment about the economics of it – you know, with the introduction of the Internet, there were tremendous savings available to companies. And I think companies kind of thought that these were free goods. And I think that the point that a number of us have made is, they’re not free goods; there is a tremendous potential cost. And the question of course is, is who is going to bear that cost?

And that – well, I mean, that’s the foundation of our tort system, is, who pays for injury? And but I think a serious conversation needs to be had on that basis of, is this a government responsibility – you know, protect me? Or do I have some obligation to put good locks on my door?

MS. MILLER: I think the other thing that this discussion demonstrates is that we’re really in the infancy of the policy, and strategic and architectural. It’s odd that we haven’t been able to advance this discussion more in the last 20 years, despite your working on it all the time, Jim, and being amazing. (Laughter.)

And so I would just like to –

MR. LEWIS: Talk about backhanded compliments.

MS. MILLER: (Chuckles.) So I’d like to see a little bit more urgency around this problem because there are just too many examples of – whether it’s Sony or the electric grid or whatever, that there is a real problem to work on. And if we actually thought about it, we might be able to fix it.

MR. MILLER: I agree with that. The only thing I would add to your list is pushing the government to identify what are truly red lines, thinking through the kinds of threats that it would like to make, which would not be mirror-image threats, to make clear that there are things we will not tolerate in this realm.

And the other question, I think, that did come out and bears some thinking and some discussion is, is how do we balance – as Bob started us off on the question, how do we balance some of our policies about Internet freedom, which other states view as hostile acts, with our own concerns about our own vulnerabilities to what they do to us?

MR. GIESLER: I think one of the more fascinating areas of understanding cybersecurity and network intrusions is the psychology of it. And people forget this is not just technology; there’s people involved. And there is a gap between operator and policymaker and legislator. There is a gap between how government – how cultures perceive operations and activities on the Internet that (they ?) have to accommodate for. And then, there is a gap between technology developer and the operator that actually has to use that.
And the psychology of understanding, why do you keep on clicking that URL in an email that comes from some prince in Nigeria – (laughter) – you know, and there is some interesting academic work being involved there, but clearly not enough. And I think the biggest problems I’ve seen in my career have been in – has been the people-ware, and the psychology of trying to convey a very technical problem – and a very emotive problem because of the sense of violation that people get when their computer has been attacked – to a more rational understanding of what is a real problem, what is a threat, and what do we have to go about it.

MR. LEWIS: Great. Please join me in thanking our panel. (Applause.)

MS. LAPOINTE: If you want food, please pick it up from the table in the –

(END)