# Atlantic Council

## The Role of Congress in Cyber Conflict

**Welcome:**
**Jason Healey,**
**Director, Cyber Statecraft Initiative,**
**The Atlantic Council**

**Moderator:**
**Harvey Rishikof,**
**Chair, American Bar Association (ABA) Advisory Standing Committee on Law and National Security; Co-chair, ABA Taskforce on Cyber and Security**

**Speakers:**
**Tom Bossert, President,**
**Civil Defense Solutions**

**Andrew Grotto,**
**Professional Staff Member, Select Committee on Intelligence,**
**U.S. Senate**

**Jason Healey,**
**Director, Cyber Statecraft Initiative, Brent Scowcroft Center on International Security, The Atlantic Council**

**Derek Khanna,**
**Political Consultant, Former Professional Staffer, Republican Study Committee, U.S. House of Representatives**

**Location: Atlantic Council, Washington, D.C.**

**Time: 2:00 p.m. EST**
**Date: Wednesday, February 13, 2013**

*Transcript by*
*Federal News Service*
*Washington, D.C.*

JASON HEALEY: I wanted to welcome you to this conversation about "The Role of Congress in Cyber Conflict." Because of timing, we'll also, of course, have some time to spend on the new executive order, which just came out today. We're sure there are likely to be questions.

I particularly wanted to thank the congressman for joining us today, as well as his excellency, the ambassador from Slovakia, our very distinguished group, as well as – I see former students of mine and others. So we've got a great range of people to have this conversation.

I just – one minute about the Cyber Statecraft Initiative. The role of our program here is to really try to demystify what we call cyber and how that relates to international security. So through events like this, we want to take what you may be hearing from your techies, from the cybersecurity community, and translate that into what that means for us in national security and vice versa.

One of our main programs for that this year is we're coming out with the first cyber conflict history book, which will be out later this year, that really looks at cyber more as military history or national security history, the way that we're used to.

Also, on the 7th of March, we are having a large event which we call the Cyber 9/12 that looks at how we respond after a major cybercrisis. And we'll be broadcasting that live from the Newseum. And you'll be seeing more information about that.

Also, with Catherine Lotrionte and Georgetown University, we're holding an international cyber conference, the third in the series, and that is April 10th – April 10th at Georgetown University. Thank you very much. And I'd like to introduce our very distinguished moderator, Harvey.

HARVEY RISHIKOF: Thank you, Jason. So good afternoon. Thank you for coming. I can see it's Ash Wednesday, and I can see that a lot of people have performed their duties, which is appropriate. And I also want to just thank the Atlantic Council. As you know, I'm the chair of the American Bar Association National Task Force with Judy Miller on Cyber Security and the Law. And we have a major effort focusing on the attorneys of America. And as Judy and I say, there are only 350,000 attorneys in the ABA so what could possibly go wrong trying to organize them?

But it's a great initiative by Laurel Bellows and we are focused on it. And we've had a series of meetings. And we're reaching out to a number of think tanks and organizations. And Jason was very kind, and said we would like to partner with them and work with them, and do whatever we can to help support their initiative and Georgetown's initiative because we all think this is probably the issue for the 21st century is trying to figure out how to resolve the space of cyber and cybersecurity.

We have a very, very distinguished panel with us today. And I think you have their bios, so I'm not going to belabor who they are. I just will just go forward just for the podcast.

It's Tom Bossert, who's president of CVS consulting; Andrew Grotto, who's a professional staff member for the Senate Committee on Intelligence, SCI, as we call it, in the United States Senate; Jason Healey, who's from – is the director of the Cyber Statecraft Initiative, the Brent Scowcroft Center on International Security, Atlantic Council. We have Derek Khanna, the visiting fellow from the Information Society Project at Yale Law School.

And I think we've assembled a very, very talented group of people, all who have written on this subject. And what we're going to start the proceedings is focus first on the role of Congress, but specifically with the War Powers Resolution. I think that is why originally we got together.

And I think I'll just read the WPR element for the audience so that they have a sense of what we're talking about. And it says: under the War Powers Resolution, the president is obliged to report to Congress within 48 hours of any case in which the United States armed forces are introduced, one, into hostilities or situations where imminent involvement in hostilities is clearly indicated by the circumstances; two, into the territory, airspace or waters of a foreign nation – and there's some other language – and then three, in numbers which substantially enlarge United States armed forces equipped for combat already located in a foreign nation.

So the interesting problem in the cyber area, which I will ask each of you to first comment is, how does cyber, if and when trigger a WPR issue in your mind, under your understanding of this how cyber works currently?

So, Jason, why don't we start with you, because it's the home territory for you?

MR. HEALEY: Thank you very much. Now, we want to start out – it's clear that the administration has and deserves wide latitude in deciding on a lot of these issues under their constitutional authority in Article Two of the Constitution. So I absolutely do support that, you know, especially with Congress having granted significant authority under the authorization to use military force in the days after 9/11.

So as a – but as a legal matter or as a policy matter, there's two or three aspects that I just wanted to touch on really briefly.

First, one of the reasons we're holding this conference today, this event today, was DOD's response to Congress in what's called the Section 934 report, which covered a lot of their cyber policy – it was for the NDAA – where essentially they were saying that they would – that the Department of Defense would essentially never – they didn't say never, but they didn't really see why they would ever have to report a cyberconflict to Congress because they – because it did not seem U.S. troops would ever come into harm's way. And if U.S. troops weren't going to come into harm's way, which seems to be the traditional reading of the War Powers Resolution, then Congress really didn't have a role.

And that struck me as an answer I wasn't necessarily comfortable with and that probably needs some examination by some smart people here, especially because I think there's more

reasons to be cautious in cyberconflict than in other areas, for in cyberspace the future is still a jump ball. It's not like conflict in the air, the land or the sea, where we've got hundreds of years of practice between states and law and understanding the interaction. We're brand new into this age. You know, we're really 25 years in for what we're thinking is cyberconflict.

And especially because of the role of the private sector, I'm very cautious in looking for more control – I don't want to say "control" is the wrong word, but more caution on behalf of the executive branch and more checks and balances than we might do, because it could be that if we have – if we're very aggressive with offense today, it might lead to a far worse cyberspace for all of us tomorrow. Cyberspace may be very – more sensitive to conflict and state-sponsored conflict that will make it far worse tomorrow. And then we can talk about more of that later.

I'd also like to just say I don't believe it's just about the War Powers Resolution. It also fits into Title 10, Title 50, the role of covert actions in this, the role of very aggressive intelligence gathering, as well as traditional – you know, things that under the War Powers might be considered traditional military authorities, but that might be more aggressive than we might want to have unchecked. Thank you.

MR. RISHIKOF: OK. Great.

I know you're going to have thoughts on this, Derek.

DEREK KHANNA: Absolutely. I want to kind of go to a little bit more macro of a level here. Obviously, the Obama interpretation of the War Powers Resolution is essentially, if American ground troops are involved, if there isn't a real threat to our armed forces, well, then this antiquated law doesn't really go into effect.

Well, that's really problematic for a number of reasons. It's problematic because it seems to misunderstand the context surrounding the War Powers Resolution. And it's really disturbing, particularly in the context of cyberwar, which it's difficult to predict in the future, but at least in concept – and I can't imagine a situation where cyberwar would involve the use of U.S. armed forces. You could have an espionage situation, but I digress.

So cyberwar presents a whole bunch of new opportunities along the lines that we've already experienced in Libya. And so we have to wonder, how are we going to continue to constrain the executive power in war making if the future of war making is going to involve cyberwar, not necessarily just as a tool of the executive but perhaps the main instrument of war making in the future, as we've already seen that drone warfare has become a main instrument of warfare in a particular theater.

And so it's very critical that we're able to establish checks and balances upon the executive there. And the – and an additional problem here is we often hear sometimes from conservative audiences that, you know, the power of the purse is the main control upon executive power. Well, when you have cyberwar being initiated by intelligence agencies, it's very difficult to see how you would ever use the power of the purse in order to restrain presidential war power in the context of cyber.

The War Powers Resolution was created in order to limit the power of the president, but you also had an additional check and balance, which was actually having 18 to 24-year-olds, primarily men – at the time only men and still only men – being deployed abroad. And you had that kind of blowback from, at the time, the draft. In a cyberwar, you don't have that check and balance either. So we need to ensure that we are able to craft a system that limits executive power consistent with the interests of those who pass the War Powers Resolution.

MR. RISHIKOF: OK. Tom, you've worked in the executive branch and you've worked very closely with Oval Office issues.

TOM BOSSERT: And the legislative branch. I –

MR. RISHIKOF: Are you on board with this or what's your position?

MR. BOSSERT: Well, if I'm not, we'll have a boring panel today. I want to thank the Atlantic Council and thank Jay. And I appreciate Barry Pavel as well and the work you're doing in this field.

And let me give a short answer and then I'll elaborate. The short answer is that the War Powers Resolution does not govern this conduct in my view, to lead with controversy. However, I believe the Constitution is always in place, as we know, does. And Article One grants an enumerated power to the Congress to declare war and not that power to the executive.

So we have an agreement on some points here, but I guess the theme of my day today will be that we suffer from a potential for great interpretative uncertainty and that's in our international understanding of what constitutes war and how we fight it, but in our domestic balances and checks on how we decide, who decides and so forth.

So my controversy of today – the War Powers Resolution by any stretch – the closest stretch I can come to justifying I think the position here articulated by my other panelists is to suggest that if we know the cyber conduct in which we're about to engage is so obviously going to justify a reaction, a violent reaction, a justifiable international reaction that would put us in danger, you could stretch one of the provisions of the War Powers Resolution to suggest that we are putting ourselves in – I think the word or term is "immediate danger." Immediacy becomes strained at that point because it requires not only our presupposition about how the enemy will respond and what they'll think about our intent and – but then their ability and their effectiveness to really put us in danger.

And so, frankly, the Congress has to change it or the DOD and the executive branch, under multiple administrations – I served under the previous one – will continue, I think with some unanimity in reading it the way they do, in the way we did, in the way the presidents I think since it was implemented under President Nixon's objection have.

MR. RISHIKOF: Great. So what's great about the Atlantic Council is they don't just admire problems. They suggest solutions to problems.

So, Andrew, to put you on the spot, one of the papers that was prepared today has the following recommendation after going off 25 pages, but that is the (old ?) way. And it says, quote: "Congress must close this," quote, "limited war close call loophole to the War Powers Resolution. Congress must make clear that offensive action itself, not the scale of that action, requires an authorization of war or an authorization for the use of force." So, as we say, aye or nay on that?

ANDREW GROTTO: Well, let me first echo Tom's thanks to you, Jason, the Atlantic Council, and to you, Harvey, for moderating. And I also should say I think I'm the only member of the panel who, you know, actually works in the government and so I have to give the obligatory whatever I say here is my own view, doesn't reflect the views of any senators. It doesn't reflect the views of the intelligence committee. And it may or may not reflect my own views.

So, you know, I obviously react here to your question, Harvey. I also want to kind of react to some things that have been said already. I think there's kind of two questions: would it be good policy for the executive branch to keep the Congress fully informed about the conduct of its operations in cyberspace? Easy answer: yes, right? I mean – and that strikes me as a pretty simple proposition that I think – you know, OK. Does current law require that? And the answer really kind of depends. And here you need to sort of parse the world of cyberoperations in two: operations occurring under Title 50, that is an intelligence activity, or under Title 10, a military activity. Activities conducted by the intelligence community, they are not armed forces for the purposes of the War Powers Resolution.

However, intelligence community activities are subject to the requirements of the National Security Act, which requires that the Congress be kept fully and currently informed on all intelligence activities, requires a presidential finding and memorandum of notification for covert action activities for programs.

And last but not least, you know – and I think this might be unique to the intelligence community, that the National Security Act requires that all intelligence activities be specifically authorized by the Congress and so the power of the purse I think is amplified – Congress' power of the purse is amplified in the National Security Act vis-à-vis intelligence activities.

Now, Title 10 operations, you know, putting aside the constitutional debate about the War Powers Resolution, you know, I think there – you know, there's obviously, you know, a long history of debate over what kinds of activities are covered by the War Power Resolution, what activities rise to the level of notification and congressional approval under that resolution. I think, you know, a panel like this has probably been held – you know, you could probably go back to the Clinton years and – you know, Bosnia, Kosovo, a lively debate then, same during the '80s, you know, with some of the Reagan administration. You can go to back to I think probably Carter.

And so, to me, you know, on some level, cyber isn't necessarily the problem. It's I think our fundamental – the fundamental tension between the executive branch and the legislative

branch over the conduct of military activities, regardless of what form they take. So, Harvey, does that answer your question?

MR. RISHIKOF: Yeah. I think you scratched the surface.

MR. GROTTO: Right.

MR. RISHIKOF: And I think what's interesting is in the cyber area, we often talk about cyber crime, cyberespionage, and cyberwar. And cybercrime uses Title 18. And you scratched the surface because the recommendation talks – what is offensive cyber? And so, as you know, most of us refer to cyberincidents. We don't really classify it, because when you start classifying the concept, then you have to take action.

So how do you guys see classification of what offense is versus what we think of cyberespionage, which is as old as the Old Testament and has always been done by state nations and it's not to be considered quote-unquote, "a hostile act," which, under international law, also is a term of we say art to define what it is.

So how do you guys understand what offense is? If you were general counsel to the president and said, well, we have to inform Congress when we do something offensive, that's what these guys want, how would you define it in the cyber area? Why don't we do – start going down the other end. Yeah.

MR. BOSSERT: Sure. There's a number of assumptions, I guess, building to that question. I'll start with – it helps me to conceive of cyber largely as a medium and not a domain. And I know there's not much distinction there, but it's useful because the conduct of the people – this is kind of the gun rights debate, right? – it's people who use cyber, not cyber. So this is a medium over which we conduct operations that are an age-old tradecraft. And so for me, I think of this as the one area for interpretive difference. So I'm glad we're into this area because I do believe we're going to agree on a number of our conversation points today.

How do I view offensive? It is an absolute reality and necessity of today's cyberworld that we break into other nations' electronic systems for the purpose of gaining information and espionage, conducting espionage. And I believe that that has been largely viewed at least up until now as somebody that does not constitute an act of war. And could we with the control over those systems, over those electronic systems use them to then shut down a switch or cause some physical consequence? Yes.

And so I think what becomes unique here, unlike in other areas or aspect of this review is we had to look at the consequences to decide whether we think it was an act of war. If you want to talk about offensive, I think we should probably not use that term. Simply it triggers the notion that we're committing an offense, an offense that the international community will not tolerate. I think there's a long history of tolerating espionage on both sides.

MR. GROTTO: Just to add – you know – I mean, I agree. The phrase, you know, "offensive cyber operations," is imprecise, right? And, you know, I prefer to use – you know,

sort of the trifecta: computer network defense, computer network exploitation and computer network attack, CND, CNE and CNA as us cyber nerds refer to the three.

You know, CNA, computer network attack, usually means something along the lines of any action that impairs the availability of information or an information system, affects the integrity, confidentiality of information or information system. Exploitation is merely gaining unauthorized access to an information system without necessarily, you know, manipulating the underlying data, the information without impairing the availability of the system. It's typically limited to, you know, pulling perhaps information back. And, obviously, computer network defense – you know, sometimes, you know, can be kind of hard to draw a line. But, generally, it means defending your own network against unauthorized intrusions.

MR. HEALEY: And we like those definitions. Those have been around since the late '90s. And they really helped when the DOD agreed on those, take a lot of different ideas that had been going around different services and bring them together so that we could all agree. And so the CNA, CNE, CND were very effective at getting us all talking about the same thing.

But what they've also done is they've kept us focused on the purpose of the activity. If you're breaking something, it's CNA, if you're not breaking something, it's CNE. And that's a good way of classifying and thinking, but I've also found that since we instituted those, particularly in the Department of Defense, we then stopped any further thought about what differentiates this kind of conduct, and we have tended to focus on a single mission only.

It's as – so when I think about offense, there's probably four that really kind of fit – that could fit in broadly. Some people fit in intelligence activity, you know, for espionage. I don't, but I think it certainly fits in Congress' role to – and especially to see if we're drawing the line right, especially as we might be seeing more blowback on the private sector.

The three main ways that I've seen nations in practice using offense are: one, the doctrine of battlefield use, of nations saying, you know, we're going to use this and we're going to integrate it with our kinetic military force. We don't have great examples of this. You know, arguably, Georgia, in 2008, Marine Corps General Mills said that he was using cybereffects on the battlefield in Afghanistan. But that might have been more referring to just getting into people's cell phones. And so – but it stands out as – if you talk to DOD people that's certainly what they mean by offense. We're going to – we're going to drop cybers like we dropped bombs from an F-16.

Second is the way the U.S. seems to be quite active with this in using it like drones – sorry to use the D word – but using it as a quiet, covert capability to disrupt either in line with an existing authorization of use of military force or in other ways, in the way that we would use commandoes. We've got to affect someone somewhere, very precisely, very quickly, very quietly, and cyber gives a great way to do that.

Third is the way our adversaries tend to be using it is through proxies. Whether that's China or Russia, they tend not to have uniform people doing this as much. They tend to use state-owned enterprises or patriotic hackers or others.

But what we found when we looked at the history – I'll hold it up again if you want – is that – all of these tend to be looking at single uses, a single tactical engagement, if you will, to get – to start using military terms – rather than saying, all right. Well, what about all of these tactical engagements rollup?

And so when I really think a lot about offense and the role of Congress and a lot of other areas, I find it's best to think of these cyberconflicts and cybercampaigns, because as we found – the more strategically significant a cyberconflict, so that is not the little petty cybercrime stuff, not when someone tries to hack into the DOD, but the real campaigns, whether that's Estonia, 2007, Georgia 2008, Stuxnet – the more strategically significant, the more similar it is to conflict in the other domains, meaning odds are you're going to know who the other adversary involved is. Odds are it's not going to happen at the speed of light. It's going to take place over weeks, months or years.

So it's not network speed. The tactical engagement might be network speed, but that's true in every domain that a tactical engagement might be over quickly. If I was Air Force, the dogfight could be over before you know it. If you're a Marine, you could get ambushed before you even know the adversary is there and the fight's over. The same is true in cyber. You could get hacked. You could get owned. They could have their effect before you know that you're in their system.

But the more strategically significant – the conflict, history has shown – I'm not saying it's always going to be that way – odds are it's going to be this back and forth of adversary versus adversary, attack versus defense, back and forth. And that I think opens up a different conversation about the scope of Congress than what we're hearing from Fort Meade, that this is network speed. Congress can't have a role because it happens like that.

MR. RISHIKOF: OK. So you've opened up the doors, we say in the legal community, and raised the S word, which is Stuxnet.

MR. KHANNA: Oh, right.

MR. RISHIKOF: And whoever was behind Stuxnet – I guess, Derek, the question to you: do you see that as a hostile act that rises to an act of war? Do you see it as – because there was no direct destruction of human beings, carbon units, that there may have been some destruction of property? How do you begin to classify that concept? And in the law of armed conflict or in the law of nations, what would be an appropriate response if you were advising the Iranians as to what they should do vis-à-vis this event that took place, if they can ever manage to get attribution?

MR. KHANNA: Sure. Good question. So my paper deliberately does not define the term "hostilities" for this reason. And it's because the point is that that term is extremely vague and that we need to kind of start these conservations now.

Stewart Baker, assistant DHS secretary, he said the danger is not that some crazy general – I should probably actually quote his words – "The danger is not so much that cyber capabilities will be used without warning by some crazy general, the real worry is that they won't be used at all because the generals don't know what the rules are." And General Michael Hayden said something very similar about Cyber Command. There are a lot of instances where the U.S. government was reluctant to use the cyber tools at its disposal. In Libya, for example, also in the Bin Laden raid there have been media reports that they didn't pull the trigger on cybertools they had at their disposal.

So we need to have these conversations now and figure out, you know, what is offensive? I think Stuxnet is a thorny example. I don't have an easy – I think it's kind of both sides of the polarity.

And I'll throw one more wrench in the kind of discussion here, which is that the tripartite scheme that you created as reference was good, but where do you put logic bombs on that?

MR. GROTTO: CNA.

MR. HEALEY: CNA.

MR. KHANNA: That's CNA?

MR. GROTTO: Yeah.

MR. HEALEY: Yeah.

MR. RISHIKOF: That's easy. It's easy for that crew. I see you wanted to drop in, Tom.

MR. BOSSERT: There's a number of things here. I think to try to go where you're driving instead of some of the earlier points I want to come back to, you had to engage in a conversation about collateral damage, proportionality, and all the other I think key terms that we generally discuss in the context of the law of war, war of nations.

You know, I think Stuxnet provides an interesting case study for two reasons. Let's presuppose for one moment that it may have been us or that we may have been involved. That's not dispositive. And I'll come back to that.

MR. HEALEY: What does that mean for non-lawyers?

MR. BOSSERT: Dispositive means it doesn't –

MR. HEALEY: I don't want to get all –

MR. BOSSERT: It doesn't disprove this case, and here's what I mean by that.

MR. HEALEY: It doesn't carry the day.

MR. BOSSERT: So what it – I guess I would ask a question – I don't want to take the moderator's job by asking a question, but would it matter to anyone on this panel if the Israelis launched the Stuxnet worm into the ethos? And by ethos, I say, from what we understand about the Stuxnet virus, it didn't just affect the Siemens equipment that we were target or that someone was targeting in Iran.

It had an effect – 40 percent of the computers in Iran were affected; 14 (percent) or 15 percent of the computers in Germany; 3 percent of the computers in the U.S. Those are smaller percentages, but they were –nevertheless infected good guys if you will as opposed to infected bad guys. So there was a collateral damage. It wasn't physical. It wasn't human. It wasn't carbon units dying. But there was a – there was a large calculus I think that had to go into that. Would it make any difference to the panelists whether the Israelis hit the button and the United States simply funded or helped with expertise? No difference?

MR. HEALEY: In talking to Congress about it or how we just –

MR. BOSSERT: The reason I ask – the reason I ask is in an international law context, repeatedly, the U.N. and its members, and in particular the Security Council and clearly the United States have found that funding activities doesn't rise to the level of war. That's important because we funded the Mujahedeen and they funded others. And we've engaged in a long activity – the Nicaraguans funded the guerillas. Once you train and arm them –

MR. RISHIKOF: Well, let me answer since – let me answer – I'll play a quick role reversal and get back. But – well, the first is, what's interesting, which is the congressional question is it would make a very big difference if I was one of the injured parties, because I would then know who to sue.

MR. BOSSERT: Sure.

MR. RISHIKOF: So I would then be able to have a cause of action for suing. And that will be another interesting question of both insurance issues at the international level and what sovereign immunity is. So it raises a whole range of problems when you get into this damage issue.

And the Nicaraguan cases, which is a big case in international law, which is this notion of what do we – we call it jus at bellum, the cause of war, because whether or not that was an act of war in this – how we support things became a big issue inside the international system.

MR. GROTTO: There's an ICJ case on that.

MR. RISHIKOF: It is a – (inaudible).

MR. GROTTO: There is an ICJ case.

MR. RISHIKOF: So we have some international law experts in the room so I'm going to do a little break. I'm going to the audience and then go back because I want to get you guys involved. Any questions in this particular section that you'd like to have? Yes, sir. Why don't you identify who you are and ask a question?

Q: Hello. (Off mic.)

MR. RISHIKOF: Josh, there's a microphone. Who are you affiliated with, Josh? Are you a citizen or –

Q: I'm here – (off mic.) (Laughter.) The comment I'll make is you're seeking to define statistics around impacted victims. But, critically, the second – the actual payload of that effect is not believed to have triggered on any other system but on a very narrow range of conditions. So, yes. You know, a code may have been present on other systems, but that's a very different distinction then the code executing to an effect that we would generally consider hostile. So I'd like to phrase that as a (construction ?) for your discussion.

MR. BOSSERT: Well, I think that's right, and I think that's – I'm glad you raised that point. It amplifies – perhaps clarifies what I was trying to say. I'm not entirely sure if those who launched that particular virus were sure or certain at the time of how many or whether other Siemen's equipment elsewhere would be affected.

Now, it turned out in such a way that we were lucky. And I don't think that it would have mattered even if a few other pieces of equipment had been affected because you're at a level of proportionality there that I think fits well within the kind of general rubric of proportionality as it's understood in the laws of war. We've had a lot more collateral damage than that.

But it's simply a point to raise here. And I guess my larger point here is that cyber has created a sub rosa or a subdermal series of ongoing conflicts that are ever present, that have not risen to the level of war. And, in fact, I believe most countries, probably to include the United States are relying on that high threshold, on that high threshold against the instinct to go to kinetic war.

And so what we can do is what we can get away with and what we're going to get away with is in our best interest. And it's expected in international espionage and conflict and intelligence gathering to do what's in our best interest.

So I wanted to put a real point on Stuxnet because we often say, well, we did it, or the Israelis did, not this panel necessarily. And it's highly classified, and there's a good case to be made that the Russians could have done it as well, or had motivation. But forgetting about whether we can attribute it and saying, the Israelis raised their hand and we just helped them I think is an interesting area to explore.

MR. RISHIKOF: Jason, you want to jump in?

MR. HEALEY: Yeah. And I agree. I think the – and I make this case a lot that it wasn't – because it didn't cause that destruction. It seems to be highly tested to make sure that it didn't. I think was very, very interesting.

And, you know, a lot of my favorite international lawyers in the room and others – and I've asked Catherine and others – asked Mike Schmidt. And I liked how Mike Schmidt responded to me. He was like – and I think, Catherine, you've agreed with this – yeah, it was a use of force. I mean, yeah. I mean, clearly an article – you know, it was on the other side of Article 24 in the thing that states aren't supposed to do to one another.

MR. RISHIKOF: That's the United Nations article you're referring to.

MR. HEALEY: Yeah. The U.N. Charter.

MR. RISHIKOF: U.N. charter. Exactly.

MR. HEALEY: And – but what was really interesting was – you know, not even the Iranians themselves made the case that it was an armed attack, you know, going past Article 51 of the U.N. Charter. The Iranians said, not a big deal. So it's interesting to have – I think they could have made a very plausible case that it was, but they chose not to and they chose to shrug it off, just like an American company does.

On the threshold, it is right. There seems to be a lot of conflicts under this threshold, enough – and the U.S. seems to be so involved in that, I question our interest in actual global norms, which we say is one of our policies, because it seems like we're operating quite well under that. And it's difficult to come up with a norm that allows us to be funding Stuxnet or involved in Stuxnet, but that makes Chinese espionage somehow beyond the pale.

MR. RISHIKOF: You have a question up there.

Q: I want to pick up, Tom, on your comment and really ask a threshold –

MR. RISHIKOF: Why don't you say who you are?

Q: My name is Jim Longley and I'm here as an individual, so –

MR. RISHIKOF: We have a lot of citizens here.

Q: I work – let's just say I work in the technical community. And, Tom, I want to pick up on what you said and pose what I view as kind of a threshold question, which is how well do we truly understand cyber? And it's – relating to Stuxnet, did it dawn on whoever was involved in it that cut and paste is a rule of thumb, or attribution? We still don't really have a good handle on it.

And I guess the point I'm asking is you can't – the point I'm making connected with the question is you can't really write policy until you understand the domain or the field you're

dealing with. And 90 percent of that is through experience. So I guess the question is do we have a grip on what the digital grid really represents?

MR. BOSSERT: Great question. In fact, I think the 20 years of history that Jay has empirically put together in a really nice tome points to the fact that we don't yet have enough of an understanding collectively to take real action. In fact, we've seen a number of policies made and remade and reissued. We've got the right objectives.

I don't know if we as a community, as a society understand it well enough. But I do believe those involved in developing the Stuxnet virus understood these issues deeply. And, in fact, it's clear on so many levels of analysis that this was a state kind of sponsored – whatever state that may be, if that – because of that. They seemed to be cognizant of rules of proportionality, of significantly technical kind of expertise.

MR. RISHIKOF: I guess part of the question – I know Jason is going to jump in – is that if you're right – I guess the interesting question is – and so that's such a level of uncertainty in the domain, and you have the executive exercising its discretion in the domain, the question is for Congress, is how far should Congress go to say, given the fact that we're in an arena in which there's no real clear lines, the executive clearly has power, we in Congress would like to be more informed on a more regular basis becomes the question.

MR. BOSSERT: There's a – there's a – we talk about 1,000 paper cuts sometimes. But I think the international group of experts call it 1,000 pinpricks. I like that better. Do we realize that we've been the victim of a strategic 1,000 pinpricks as opposed to a disaggregated 1,000 pinpricks until –

MR. RISHIKOF: We call it – yeah. We call it bee stings so it gives you a little bit more –

MR. BOSSERT: Bee stings. You know, in other words – in other words, if we don't have a strategy I believe is your question, then we're victim to a bunch of disaggregated tactical actions that may together be painted as a tapestry we didn't intend to paint.

Q: Just to throw something in.

MR. RISHIKOF: Sure. Please.

Q: But to just take an extreme example. Somebody gets access to the code and attacks me in my home in Maine.

MR. RISHIKOF: Yeah.

Q: OK, talk about unintended consequences.

MR. BOSSERT: Very unsophisticated ne'er-do-wells will copy and paste that very sophisticated virus and turn it against us. That's absolutely been the case in cyberwarfare, cyberconflict and cybercrime. I think that's a great point.

MR. BOSSERT: So, Andrew, we'll go down, because I think people want to get in on the panel. So Andrew, what's your reaction to this?

MR. GROTTO: Yeah. I want to react to this notion of uncertainty. And I think we need to be a little more precise about what kind of uncertainty we're talking about, you know, as a – you know, at law school, you know, I remember my first year contracts professor used to talk about there's the facts and then the application of the facts to the law. You can have uncertainty in either of those two domains. Either the facts can be unclear, in which case, the application of the law, assuming the law is clear, becomes challenging because you have to, you know, assume certain facts, which then gets into one's own prejudices and biases and so on. Or the law itself can be unclear, in which case, you know, at least in this domain, obviously Congress – you know, we write laws. Sometimes we pass them even. And – you know.

So with respect to cyber, my own two cents is I don't think the law is unclear at all. I think that cyber is like any other instrument of U.S. power. It's – you know, you can evaluate the consequences of a cyberattack on the basis of its effects. We do that with all kinds of different weapons.

And so I think that much of the debate over cyber is attributable to the fact that it is shadowy, it's – a lot of it's classified and spooky, and there's just not a whole lot of understanding about what this world looks like. So I see it as a factual problem, which I want to take back to a point I made right at the very beginning about whether it's good policy for the executive branch to be transparent with the Congress. I think, yes, absolutely. And I think that transparency can go a long way towards giving members of Congress and the citizens they represent confidence that the executive branch is wielding this tool in a lawful matter that comports with our values. I don't mean to suggest that the administration is not being transparent, but as – you know, as a staffer on the Intelligence Committee, you know, we do oversight. You know, I want more transparency. We always want more transparency.

MR. RISHIKOF: Before we get Jason in – I think the key issue for this day is will that executive transparency be voluntary or will that transparency be regulated? That's the key. Jason, go ahead.

MR. HEALEY: It's a great question. Sure. Thank you. I'm going to pick up your point on blowback and I'm going to look at this being new. It is one of my concerns, because it is easier in this – I don't – you know, if we're sending out special forces to hit someone in Yemen, we've got an AC-47 out of – you know, over Somalia, or we're using – or we're using drones in Yemen, that doesn't directly affect you, me, us. We don't have a drone strikeable target in our house, but we all touch into cyberspace. And, in fact, the younger you are, the more likely you are to feel that this is a commons and this belongs somehow to you and you have a stake in this thing, cyberspace.

And so there's a specific concern about someone taking code and reusing it. I'm actually a bit less concerned about that than in the general parts of – you know, at the White House launch today, the executive order, they talk specifically about the denial of service attacks against Wall Street, that administration and Congress have been pretty clear that they say Iran is responsible. And isn't this – look at these threats, General Alexander said. We need to do something.

Well, there's a case to be made that was government actions including in cyberspace that might have drawn these attacks as blowback onto the finance sector. And I'm not saying that has to restrict the administration from doing anything. I'm saying it has to be a caution. I mean, Congress might have a role in that caution to say, look, are we sure we want to do this? Do we really understand how this might affect our already vulnerable infrastructure?

On policy, I do want to push back. I think we know this much better than we believe, that we've been allowing the spooks to classify it. We've been allowing the geeks to mystify it, because when you look back over 25 years, you see these statements of people involved, you see the statements of policymakers and what they included, and it all makes sense to us today. And if it were changing so quickly, we would look back and we would say, oh, those things those people were writing 25 years ago – look at Fred Flintstone carving his cyberpolicy, you know, into stone. But it's not. You look at these quotes and they're indistinguishable from today.

To put it into a military context, you could take a fighter pilot from a Sopwith Camel in 1917 and have him talk to a Raptor jock today. And you know what? Within 30 seconds, they're going to be talking about shooting down their what. You know, they're going to be doing all this stuff about the thrill of a dogfight even though the technology of an F-22 makes that Sopwith Camel look absolutely like a toy, because the fundamental underlying nature of conflict in the aerial domain of dogfighting hasn't changed. And that's what – I think when you look at the conflicts from 1986, that the underlying dynamics haven't changed very much. So that way, we could look at these policies and we could understand it better. It's just that we haven't.

MR. RISHIKOF: I'll let Derek respond and then I have two people who want to jump in. But we always say, when I used to be at DOD, that PILOT really stands for personnel in lieu of technology.

MR. KHANNA: It was Adam, right?

MR. GROTTO: Andy.

MR. KHANNA: Andy. If what you said is true and there isn't uncertainty, well –

MR. GROTTO: Uncertainty about the law.

MR. KHANNA: Uncertainty about law.

MR. GROTTO: That's different.

MR. KHANNA: I just want to read a brief quotation and you can say if he's wrong or if I'm misinterpreting his quotation. This is from General Michal Hayden, previous director of NSA and director of CIA in 2011. "U.S. Cyber Command has been in existence for over a year and no one is familiar with the command or its – or no one who is familiar with the command or its mission believes our current policy law or doctrine is adequate to our needs or our capabilities. Most disappointingly, the doctrinal policy and legal dilemmas we currently face remain unresolved, even though they've been around for the better part of a decade." Has that changed since 2011 or was he wrong?

MR. GROTTO: Well, wrong about everything? (Laughter.) So what he's – I don't see the context of the quote, but, you know, there's been a lively debate for several years now about the U.S. government's broader cyberenterprise as distinct from the use of cyber as essentially a weapon of statecraft vis-à-vis –

MR. KHANNA: Let me give you a more specific question then. If the media reports are true and before our raid in Pakistan to get bin Laden we actually were going to use a cyberattack against their radar facilities but we decided not to use it because of the legal uncertainty, because we weren't sure if it would be an issue of the War Powers Resolution, which is what the New York Times has reported, would that be a problem? And when a similar situation was reported for Libya, which required us to send our Air Force to destroy it, which put our American service members in jeopardy, if those reports are true, would that change your reflection on – (off mic) –

MR. GROTTO: I think it's a problem of doctrine more than law.

MR. RISHIKOF: Well, I guess – this to the panel – the question is do you think tuning out a radar system of a foreign power when we're going to be planning to use potentially lethal force is a WPR moment?

MR. BOSSERT: Yeah. Let me weigh – let me weigh in on that because almost every example that we read or hypothesize, in this case we've taken I think what's maybe a true story and –

MR. RISHIKOF: But let's just say, just hypothetical. Just – (inaudible) – stay with hypothetical.

MR. BOSSERT: Well, but what we do is we always combine it with something that otherwise would trigger the War Powers Resolution. So we're mounting a coalition of forces to kick Iraq out of Kuwait and to seek regime change or not. There's a discussion there. All of those things trigger the War Powers Resolution and the requirement to report the Congress, and the 60-day, 90-day triggers. The particular cyber tactical choice there was I think irrelevant to that.

MR. RISHIKOF: It's more of a tactical issue. Let me ask – I've had a two-finger position, which in our world means you want to intervene directly on this issue.

Q: Thank you. Thank you for having this panel. I love this conversation. We need to have it more and fast. My name is Lorelei Kelly. I'm at the Open Technology Institute at the New America Foundation.

And one of the – I worked on the Hill for a decade on issues of peacekeeping and peace building in this murky area where the military was being called on to do not only policing activities but sort of social capital building. And we've gotten to the point where, you know, you have the Marines mentoring the police in Afghanistan. And you have these authorities migrating into the Defense Department. You've probably seen this.

And I see this as the next big sort of Rubicon that we might cross, simply because capacity, personnel, resources are at DOD. They get good at it and then it sort of never migrates back into the civilian sphere. I'm working with a bunch of hackers now so you can imagine this makes everyone's hair stand up. The question –

MR. RISHIKOF: Lawfully. You work with them lawfully.

Q: Lawfully, yeah. (Laughter.)

MR. RISHIKOF: For the record. Yes. For the record.

Q: Yeah, we're doing really good stuff. But the question I have is like where does something like Posse Comitatus fit into this? It seems like it's something that should have been talked about and reauthorized several times over the last decade. And this – if the military says, you guys don't have any business doing this because no troops are at risk, then it must be a policing operation. If it's a policing operation, then what is the military doing? That's a clear violation of an almost 200-year-old law that we haven't talked about in a long time.

MR. RISHIKOF: So this raises the famous, you know, Title 10, Title 50 and Title 18, which we call – we may need a Title 78. We may need a Title 78 in order to cover this, because Congress' challenge is raised, is should we then be using more law enforcement power in this domain, which then allows us to deputize, because Posse Comitatus is deputizing citizens, like this group here, and getting them involved, which is – touches the issue that's close to many of our hearts of what we call comprehensive private sector response or some form of active defense that's being used.

This is that – this question sort of pulls this panel into almost the inadequacy of the WPR as being such a 20th century concept given the 21st century set of problems. So where do you all break on that?

MR. GROTTO: So are we talking about computer network attack against a U.S. target? I'm just kind of – I'm puzzled at what exactly we're trying to –

MR. RISHIKOF: A private sector –

MR. BOSSERT: Domestic application I think is what –

MR. RISHIKOF: A private sector company is attacked.

Q: What's the division of labor and – (off mic) – and security in this case, because we don't have – (off mic) –

MR. RISHIKOF: So that's a different issue which we'll go to, which is the organization of the state on this issue. But just for the panelist to say that low-level response, if it's not going to trigger a WPR is it going to be more of a combination law enforcement private sector joint response that starts to move beyond its own network and start to go somewhere else, and which part of the government should be involved in which – yeah. That's sort of the problem.

MR. GROTTO: I guess – I just am still a little puzzled at – I mean, you know – so, obviously, DOD, Cyber Command, NSA, they have a tremendous amount of technical expertise that would be foolish for the country not to try and leverage. That said, obviously, you know, they don't have the authorities to perform law enforcement functions. Typically, the way it works is – you know, if a – you know, there's a threat and it's on a U.S. – and it was like just – you know, U.S. infrastructure is used in part to carry out the threat, the FBI will have the lead. It's a Title 18 matter. It's pretty easy.

MR. BOSSERT: Yeah. There's a number of questions inherent in this that are going to be pretty broad to discuss, perhaps too many. But there's a number of Rubicons that we have crossed. And I think the first and the most obvious is that we've now, as a globe, plugged into an inherently unsafe common protocol of sharing information and controlling electronic or digital devices.

Despite the wisdom of that, we have crossed that Rubicon, the notion of – the point of no return is my understanding of that term. Whether that river is still where it was at the time this quote was made – and I think there's an equal argument to be made that it's not. We've crossed that Rubicon probably three or four times. And, in fact, we're reauthorized and change and reauthorized three or four times the Insurrection Act as opposed to the Posse Comitatus Act, which is the flipside of when the president can violate that statute.

So I think the question here is when can we use our intelligence gathering authorities domestically I think it's a very touchy issue, and it touches on drones and other things. And I think the answer is we shouldn't without following the prescriptions of the law enforcement community. And that's a much different set of standards and rules.

MR. HEALEY: And I would take this in two different directions. And they're – and they're based on the distinctions that Harvey started off with, with between is this action best thought of as crime, in which case, the Atlantic Council has been looking and hope they were going to have Dimitri Petrov (ph) writing for us soon, a set of proposals on what the private sector could be doing to help defend themselves in a more active manner and that would include getting deputized by a valid – you know, credential, law enforcement agency to be deputized, to take some action that they would normalize – that would otherwise be illegal to take. And that

would be valid and that would be an interesting way to go about it on the crime – on the crime side. And that's not entirely just smacking back.

MR. GROTTO: It's pulling the posse out of Posse Comitatus.

MR. HEALEY: You know, and that's not saying it's going to – it necessarily gets into a slap fight. There are some other more balanced things that you can get to that aren't just striking back.

MR. BOSSERT: Yeah. There's a lot of examples here. You know, if you're an Internet service provider and you know that you're – there's a botnet attack going on with your customers, using their devices, they've been taken over, what can you do about it? You know, we've had conversations in this case where it's played out and we've had Internet service providers have to go and seek a subpoena against another U.S. company.

MR. RISHIKOF: I think Jason was in mid-sentence. Go ahead.

MR. HEALEY: No. No. But it's a good point. And it's easier for the private sector to do a lot of these things because they don't have to get into this knockdown, drag-out conversation about authorities. They're able to do quite a bit without – you know, within the law, and that's just when they start getting into this gray area of the law.

The second point is when we're talking about – where I hear Posse Comitatus come up more is – where also, is when we're looking not at crime but at actual warfare. And I want to bring up the point that a lot of what we're talking about for cyberconflict is just what we have seen. And we can think about other kinds of cyberconflicts. Again, we're just 25 years into this.

I tend to come across a lot of people that make the assumption that the cyberconflicts 25 years from now are going to be similar to the ones today just with cooler technologies. But it could end up being a real war. You know, where – and that has real dead people and real death and destruction on our side and their side. And maybe the nations decide to use kinetic strikes back, but maybe for some reason, they don't. That might be seen as an escalation and they decide – just like in the early nuclear age, as they said, well, of course, any war is going to be nuclear war. But as it turns out, that wasn't true, that we would stay below that threshold, even though Russian fighter – Soviet fighter pilots were fighting American fighter pilots in Korea and everybody decided not to go nuclear. It may in future that we decide not to go cyber.

If you have that real war going on, all of a sudden, DOD's role is not going to be defense afforded to civil authorities. It's not going to be what can we – you know, great, let's share some more information with the private sector, like was in today's EO. It's going to be the president and the American citizens are saying, no, you have to protect us. You've got to get involved. And I think that shifts from what I understand a lot of how we might look at Posse Comitatus and other things about the military and other – you know, Article Two constitutional authorities being used in the United States.

MR. HEALEY: Do you want to jump in? Do you have anything to add?

MR. KHANNA: Well, Posse Comitatus is a lot to talk about. Unfortunately, it's kind of been watered down. I guess the 21st century Posse Comitatus – posse was originally when a U.S. marshal would wrangle up people in the territories and say, hey, join my posse so we can crime fight. I kind of think of the 21st century posse as – I don't know, FBI gathering up 18-year-old hackers and – but I digress.

But one thing that is kind of interesting, kind of related to that – I'm not sure if it was Duqu or if it was Flame, but it was a virus that could basically completely compromised the system and gave you full access and surveillance, even accessing the web cam, even accessing allegedly Bluetooth devices within a range of that device.

We've already talked about how Stuxnet, of course, leaked across the world affecting 3 percent of American computers. I haven't seen much data on Duqu or Flame's infiltration in the United States. But it would be interesting if, hypothetically, the United States created Flame or Duqu, and those software – those virus affected American citizens and, you know, was being used for espionage against American citizens as part of a dragnet, not necessarily intentionally but just because of how software spread and if that would present particular Fourth Amendment issues.

MR. GROTTO: It would. Yes. It would big time.

MR. RISHIKOF: The Fourth Amendment, trespass issues. So just for the record, my Latin training was crossing the Rubicon meant when a general returning to Rome would have to leave his troops on the other side of the Rubicon. And if the general crossed the – crossed the river with his troops is considered an attack on the Senate. So that's the – that's the origin of that, from Latin training. Yeah. But the issue is – I know we have another question here so I have some thoughts, but why don't you shoot and then –

Q: I'm Barbara Slavin. I'm a senior fellow here at the Atlantic Council. And, Jason, you've already sort of answered this, but what if the denial – dedicated denial of service attacks had been more severe? What if money had been stolen, data destroyed in a way that materially affected millions of people in this country? You have bank accounts, not just the banks that had to spend a fortune fending off these attacks?

Are Americans within their rights in terms of suing the U.S. government for starting this conflict with Stuxnet? I mean, where is the responsibility for the blowback? Do we all just have to accept it? And where do you think this conflict is going to go? Do you think – because judging from my impression of U.S. policy on Iran, the president of the United States does not want to get into a kinetic war with Iran, but he's willing to do all sorts of other things? Where do you think this could go? And what could be the ramification of that?

MR. RISHIKOF: So it's a scope and scale issue, but thanks to the law, we have standing issues. The court has been quite restrictive in standing issues to uncertain – sort of citizen rights suits is usually in a very narrow door.

MR. HEALEY: I mean, one of my colleagues – I used to work for Goldman Sachs – I was talking to one of my colleagues that worked for one of the New York big Wall Street banks. And he said – and this was several months ago and attacks have continued. He estimated their bank had spent at least $10 million in mitigating the denial service attacks up to that point.

And Jeff Moss, who's one of the – famous hacker now and now involved in D.C. policy, I've heard him talk about how the attacks were multiple times larger than any attack that had ever been seen in this history of the Internet. You know, beforehand, there had been like 30 to 40 gigabytes a second, and now there are 200 – you know, over 200 gigabytes a second. So it's much larger than you could ever guess that – you know, expect a single institution to have defended themselves for a multiple of the largest thing that had ever been seen historically.

So I think it's an interesting case. You know – I mean, they're not going to get a tax deduction back on that money that they're spending that – for an attack that the government is, you know, behind their hand saying it was in fact Iran. That was assumedly either for Stuxnet or because of the finance sector role in sanctions on Iran, or both, or just because the Iranians can be crazy bastards sometimes. So it's interesting.

As Harvey said, there's probably not a legal case. I think that it says that there's more of a case for more (scrutiny ?) of these to say how will these blowback to us, whether that happens within the administration, which worries me because no one – few people in the administration that are in those rooms will ever have had a private sector background.

MR. RISHIKOF: I guess part of the issue is – let's go – we'll do the big level question and then the lower level question.

The big level question is – the panel's thrust was what should be the role of Congress inside the War Powers Resolution? So one of the arguments that could be made is that probably one of the most successful international public policy positions in our generation was basically the mutually assured destruction, nuclear example, in which there was a series of doctrines that were generated by the United States government that generally were accepted by the rest of the other nuclear powers. And, as a result, we did not have a nuclear exchange and we also kept the lid on nuclear proliferation. And we had a sort of open kimono notion that if you were going to strike us, we would strike you to the level of destroying you.

But Congress really didn't get involved in that level of power. So there's an argument to be made, should Congress not, therefore, based on this debate, not get involved, and, therefore, allow the executive an extraordinary amount of discretion and simultaneous ambiguity, because we used to say the only country that actually used nuclear weapons was the United States and we demonstrated to the world that we would under certain circumstances.

So is – so it reverses this issue, which is that, would it be better then for Congress not to get involved on the war issue but get much more involved at the second level issues, which a lot of people are arguing about – liability issues, sharing of information issues, that that's where the Congress' role should be in this arena. And, as you know, over the last – there's been a lot of pieces of legislation that have not gone through the Congress. Across the way, there's another

think tank that are holding them – another Congress will be introducing new legislation on this, that the real center of gravity in this world is the private sector, its information, and what information we can give the private sector to help, that's the center of gravity, not the war issue center of gravity, how do you guys react to that phenomena? Why don't we start with SCI. SCI?

MR. GROTTO: Sure. Andy Grotto, because I don't want to speak for the committee.

MR. RISHIKOF: Of course. Andy, of course. I'm sorry. Andy.

MR. GROTTO: Harvey, you know, I'm not sure I like the nuclear – the mutual assured destruction analogy. I mean, nuclear policy evolved, you know, from, you know, early doctrines in the late '40s of, you know, let's just – these are unlike – these are just like any other weapons to, you know, today where, you know, we view them as, you know, a pretty extraordinary tool and hopefully one we never have to use, with lots of intense debate in the executive branch, in the Congress and between the two branches over the past 60 years.

You know, Congress played a role in everything from, you know, the treaty negotiations, you know, beginning in the, you know, kind of late '50s, early '60s to the finding of a nuclear complex. You know, in the '50s and '60s, there was a so-called iron triangle between the JCAE, the Joint Atomic Energy Commission, and industry, you know. And so there's just a lot of history there that I'm not sure the analogy quite works.

And, in fact, you know, in some ways, the analogy may serve as a cautionary tale for how Congress ought to do oversight. You know, there's been some talk in the past of some senators have suggested, well, there needs to be a cyber committee, you know, a select committee on cyber, right, to kind of unify oversight. And I actually think that's a bad idea because my concern would be that you'd see a repeat of that iron triangle phenomenon that we saw in the 1950s and '60s that really kind of captured nuclear policy for basically two generations.

MR. RISHIKOF: So I just – keeping in mind – do you think we need a cyber Yalta? (Laughter.)

MR. HEALEY: Yeah. Alex Klimburg did a paper on the cyber Yalta. He felt like we're at that point now where we now know the Russians – you know, the Soviet Union and Stalin's going to go a very different direction and the war time comity is not going to continue. I thought it was a very interesting question. I hadn't thought about it like that.

I think one of the differences is, you know, MAD that was a war fighting strategy and how we would use these weapons, but we never did use the weapons. The issue here is that we are using these capabilities. And the administration, in its 934 report, said Congress doesn't have a role in how we're using these weapons because it's either traditional military activities or we're not putting U.S. forces at risk.

MR. GROTTO: I'm not sure they said that actually. I have a different interpretation.

MR. HEALEY: OK.

MR. GROTTO: You know – well, just – I didn't mean to interrupt you. I'll be real brief. Just – actually, I did mean to interrupt you. Sorry.

MR. HEALEY: No. No. No. Please go ahead.

MR. GROTTO: I hate it when people say that to me.

MR. RISHIKOF: I think it's too late for that.

MR. GROTTO: Yeah. No. I have the legal analysis that the administration put out for Libya. And, to me, you know, the key point here is that – you know, I see limited nature, scope and duration of anticipated actions, a reference to a significant chance of escalation. I'm not sure that it's possible to extrapolate from the 934 report that cyber would never trigger the War Powers Resolution.

MR. HEALEY: I mean, certainly the bits of escalation and the more the administration is talking about things like escalation and some of the other elements of what – (inaudible) – talked about in his testimony, which is referenced in our paper, but, you know, in their 934 report, cyberoperations might not include the introduction of armed forces into the area of hostilities. They may be a component of larger operations that could trigger notification and reporting in accordance with the war powers, which was Tom's point. The department will continue to assess each of its actions to determine when.

So they don't mention any of the other elements of co-analysis. They're just saying because we're not introducing armed forces into the area of hostilities, which, if you look at, I want to say, every other DOD policy, even the Section 934 report, they're saying there are hostile acts in cyberspace and our forces are operating in and through cyberspace. So I think it's difficult to make – point in every other document – you know, the ones that aren't going to Congress – that we're operating in and through cyberspace and there are hostile acts, and then say, well, we're not introducing forces into hostilities.

MR. GROTTO: Well, does a cruise missile launch that a suspected, you know, chemical weapons, biological weapons facility in Sudan trigger the War Powers Resolution? Does a cyberattack that achieves the same objective trigger the War Powers Resolution? Again, I'm not sure that – there's a part of me that thinks we may be making too much of cyber as a tool whereas –

MR. HEALEY: I agree. I think that's the exact technology that I think –

MR. RISHIKOF: On that –

MR. GROTTO: Sorry.

MR. RISHIKOF: But on that issue, which is great, which it raises the old – and you mentioned under Title 10, there's something called traditional military activity. We call it TMA among the cognoscente. So the TMA issue and how DOD has defined the TMA issue through its Title 10 activities has gotten a lot of press vis-à-vis the traditional Title 50, which we've said requires a certain notification to the Gang of Eight, which is the HPSCI, SPSCI leadership and –

MR. GROTTO: Well, it's the full committee.

MR. RISHIKOF: Full committee.

MR. GROTTO: The Gang of Eight is a special subset.

MR. RISHIKOF: So now, the full committee, that sort of notification. And I think this notion of where cyber falls, is it just another tactic that falls under TMA or has it risen to something given its potential that should require a greater notification? That's sort of the knob of the issue.

MR. GROTTO: And just to be even more precise – I mean, the Gang of Eight, you know, stuff, concerns – I mean, you have to distinguish between an activity and a covert action, right? A covert action is – and, you know, there are – there are important distinctions that matter in terms of notification. You know, a computer network and exploitation activity may not be a covert action.

MR. RISHIKOF: And if it is – and if it is a covert action, then you would –

MR. GROTTO: Then it's – then it's subject to that's –

MR. RISHIKOF: Then you think it would require notification.

MR. GROTTO: All of the – the National Security Act says –

MR. RISHIKOF: Right. On 47 aspects.

MR. GROTTO: – all intelligence activities should be currently and – Congress needs to be kept currently and fully informed of all intelligence activities.

MR. RISHIKOF: Right. Because, as you know, the official position of the American government is that the drone activity is a covert action. That's why no U.S. official will comment on it.

MR. HEALEY: Yeah. And it's interesting. You know, I like Andy's point. You know, the language that I just read, you could put in cruise missile strike. You know, it might not introduce – it might not include introduction of armed forces – (inaudible) – their hostilities, except that if we could use cruise missile strikes covertly and without people knowing and considering that may be traditional military activities that we don't have to talk about. So there

is that difference, you know, the missile rolls off the rail – you know, it comes out of the box and –

Q: (Off mic.)

MR. RISHIKOF: There's – we have a man that's been very patient there and wants to ask a question. Sir.

Q: (Off mic.) I'm also an American citizen, but I formerly was with the Semiconductor Industry Association. My question –

MR. HEALEY: And as a point of order, today, you hear that attribution is a problem for cyber. It's not here. This is attribution. This is open. I should have done that in the introductory remarks. Thank you.

MR. GROTTO: It's actually an overstated problem in cyber too. (Laughter.) Sorry.

Q: My question is actually really basic and that is I don't understand – I guess in distinguishing or my rudimentary course becoming an Army officer about military law, they explained a lot about sabotage, right? What's permissible, it's a guerrilla action. How – I don't understand how offensive cyberactivities are not just normal sabotage. Congress has every right to weigh in on what the rules of war is and how a soldier could be told to execute. And I don't understand how this is distinguished.

MR. RISHIKOF: Do you want me to take this?

MR. BOSSERT: I'm not sure anyone up here is suggesting that it's not. For me, to the extent that maybe my initial remarks might have led you to think that, my simple narrow point there was my reading of the War Powers Resolution was such that most of the cyberactions or activities that we've talked about here today, absent some other coupling with a larger strategic initiative and use of armed forces do not meet the – do not trigger that words, the plain black and white words there.

Words are important. Especially in this space we've got a – we've got a significant amount of interpretative difference. And people are misunderstanding these things that – I think the DOD has been pretty clear in saying that they don't ever intend to notify, to follow the formal prescriptions of the War Powers Resolution to notify and set a 60-day clock on themselves when they're using cyberactivities to – especially those activities that don't result in kinetic effect.

Q: I guess I'm just confused because in a real kinetic conflict that I've been in, we weren't authorized to sabotage civilian resources, even if it would have been a substantial benefit –

MR. BOSSERT: That's a – that's a much different question. In other words –

Q: – to our – well, I've seen there are parallel actions, right? There's an offensive attack that's sabotage against – and there's no kinetic war. There's no real war. And that distinguishes –

MR. RISHIKOF: I think part of the issue is which classification regime you're under as a matter of law at the time. So we always say, why is it that under certain circumstances you give people medals as opposed to prosecuting them for being – for homicide? (Laughter.) And we say, usually, the presence of a military band is the key there because you know you're at war.

So the issue though is we're saying – which would raise here as sabotage is usually done in a war context. So the question is are we at war with the world currently vis-à-vis activities that are taking place? And that's where Congress would have to play a role because, historically, Congress was the entity that defined when we're at war and who we're at war with.

And the AUMF, the Authorizing for Use of Military Force, was unique because it didn't identify an enemy and it included both persons and organizations which we had never done before. The Congress had never given that latitude.

But this issue for us inside the cyber context is that if you take someone like Joel Brenner's book, which you read recently, Joel's position is we used to think we're either at war or at peace. And cyber has created a new third stage in which our frenemies and our adversaries are conducting extraordinary activities that are 1,000 sets of beestings and we seem to have no mechanism about how to respond appropriately, because it's confused. Crime, espionage and war have all been condensed down. And this argument would be –

MR. GROTTO: And what happened to the Cold War?

MR. BOSSERT: Well, it was something very similar. Yeah.

MR. RISHIKOF: What is in the Cold War is we used proxies, but we also did not feel at any given point in time in the Cold War that critical, vital secrets were being stolen, nor did we ever feel directly, except for the missile – the Cuban missile crisis that CONUS itself was at risk, whereas cyber's capacity to make the risk factor so much greater at a shorter period of time is a bit different.

MR. BOSSERT: There's a – there's a just to not completely duck that question, let's suppose – let's suppose this group did agree we were at war and let's suppose Congress declared it so that we had no constitutional conflict here to discuss. There is still the international kind of law construct of distinction, distinguishing between a civilian target, a military target and then a military objective. And I think in the cyber context, that's the most fascinating conversation that we can have. There will be a military objective associated with almost every Internet connection in this world once we go to war. And the cascading consequences will be on civilian – civilians as individuals, but also on civilian economic constructs – banks, financial centers, communications capabilities.

MR. KHANNA: Sure.

MR. RISHIKOF: What? We have a two –

Q: (Off mic.)

MR. RISHIKOF: You might say who you are, sir.

Q: I'm sorry. Frank Kramer, Atlantic Council. The issue under law where, first, as you said, whether there's military necessity, and then, the proportionality issue comes up or the distinction point comes up, which is how much, if you will, collateral damage is there and how do you judge that vis-à-vis the value of the military necessity. So you have to make a judgment in that context. So the fact that – you know, a bank is hurt doesn't end the conversation. It starts the conversation.

MR. BOSSERT: I don't – I don't – first, I agree. Second, distinction between a military objective and proportionality are two separate analyses.

Q: That's what I'm saying.

MR. BOSSERT: Yeah – no. I agree. I agree.

Q: Proportionality doesn't mean –

MR. BOSSERT: But I guess in the cyber context, proportionality is going to be a very difficult conversation because the military objective associated with attacking any area of cyberspace on which the military relies to communicate or to conduct war is going to also be that which our economies and our – and our other infrastructures rely.

MR. HEALEY: I'd like to put a hold just for a second on this because we're starting – we're getting – on the 28th of March, we're going to be holding an event for the launch of the Tallinn Manual, so this is a group of international lawyers, with Mike Schmidt and others, that have gotten together to look exactly at these issues of how international humanitarian law applies in these issues of distinction and proportionality apply specifically. They've put together this large manual that says, here's what the black letter law is, here's where there's consensus among international lawyers. So it is a fascinating conversation and I'm –

MR. BOSSERT: We're upstaging the next event. Yeah.

MR. HEALEY: – back for that March 28th event when we'll have Mike Schmidt down here to launch that manual.

MR. RISHIKOF: Well, let me just ask the large question, which is the executive order was signed today. There was a Presidential Decision Directive 21 was also executed. And that raised the question of how does the panel feel about the way the executive branch has organized itself for the cyber issue? And what role do you think Congress should play in assisting the executive branch in organizing itself to deal with these problems, or should they – should the

Congress stand aside and say, look, it's your issue, it's your problem, come forward and we'll be satisfied? Or should Congress be a little bit more involved than it has been over the last number of years in the cyber arena? Let me go down the row. I'll leave Andrew last. We'll start with you, on the executive order and organization of the state currently from a cyber perspective.

MR. KHANNA: I'm still researching some of the components of the executive order. Obviously, information sharing is a good thing. I think most people up here probably support information sharing. There's clearly more that can be done. We haven't seen that much on data breaches, for example, but I think that that's something that should be up for discussion.

I think that that's something that consumers don't normally think about is the idea that their consumer data, their personal information can be – has often been breached and people still go back to that same company. And that's an example where the government may need to intervene or may need to understand, you know, what – why are there so many data breaches and what can be done on the backside, because most of this data resides on servers that are pretty vulnerable.

MR. HEALEY: Thank you. Two thoughts. It struck me as interesting when the White House launched the executive order today that they said this was an important first step. And it struck me that how many officials would have had, when they released a policy document back to 1990 – since at least 1998 was President Clinton PDD 63 – have called what they were doing an important first step. And the policies and actions that they list in those policies have stayed relatively consistent over those 15 years.

So I think, you know, the EO was good. It did lay out important steps that should be taken and can help. You know, I can nitpick on some of them, but I'll hold off in that they were generally useful things. I'm just not sure why we're making such a big deal about things that are relatively work-a-day pieces.

To tie it to larger policy – now, EOs aren't supposed to be setting policy. They're supposed to be just – you know, give actions to implement. To tie it to our previous discussion, if you look at U.S. policies, there's nothing that gives room for using covert action. There's nothing that I can read that talks about getting into offense that's not part of some kind of larger conflict. There's very little policy that talks about how we seem to be using it right now. It's all great – this all fits in with American norms and values and we might respond if attacked. And I'm looking forward to that policy that says –

Q: (Off mic.)

MR. HEALEY: Then, that inflames – then –

Q: (Off mic.)

MR. HEALEY: You're just trying to get me to say mean, awful things into my mike. (Laughter.) But we talked about – if we said – if we even said, there are times when we would be willing to use this like any other kind of power, then heck with our government. We do not

believe anything – heck with the executive order. Heck with everything else we'll put out, because we say we care about defense. We say we care about norms. And if we're going to stab people in the back when it's to our advantage, then who is ever going to believe the State Department about the other things that we talk about?

If we even just said there are times when we will try and use – then when we'll use this. We want to integrate it into part of our – of our offensive actions. There will even be times when we might consider this like any other covert – at the time when they reached the international strategy, I was in a closed-door session and I had a White House official say to me, we're releasing this and now other nations can judge us by our actions. We're saying that we want to operate according to norms and according to U.S. principles that we all hold dear as Americans.

And how are people going to judge the United States if they say, all right, it looks like you were behind Stuxnet. It looks – you know, we're seeing a lot of this, about how you're looking to use it as covert action to stab people in the back. We seem to have examples of this. But, you know what? It doesn't fit in with your other policy statements on how you're going to do this.

MR. RISHIKOF: Let me ask this question, because a lot of this turns on the lack of attribution in the system – I'm trying to defend yourself against yourself – is that a lot of it turns on lack of attribution. And if we resolve the attribution problem, what some people think it's not it's that far away technologically speaking, well, then, a lot of these issues evaporate about the ability to use it covertly because the attribution will have to be there vis-à-vis how actions take place.

Q: (Off mic) – covert action when we had attribution or not, cyber is not the issue and covert action is. Every single president of this country since beginning of time, including Carter, who you would have thought based upon his public statements of –

MR. HEALEY: I think it's on.

Q: – my, you know, moral, ethical concerns, every single president has implemented and used covert action.

MR. RISHIKOF: That's not my question. My question is that the essence of covert action is not attribution, but the issue is currently now, technologically, lack of attribution is part of the instrument, whereas if that instrument is now going to be able to have attribution when it's used, that would remove it and take it off the table from that set of apparatus. The question: would we all be willing to have a regime in which that ability existed, would that be better for the international norms or does problem of attribution only contributes to the issue? And where do you break on that?

MR. GROTTO: There's attribution and there's attribution. I mean, you know – covert action, you know – so, you know, it's tied the hand of the U.S. government, but you have to ask from whom, right? Sometimes, you know, covert action is a tool of statecraft and we actually, you know, might want our adversaries to at least have a pretty good guess for who's, you know,

up to no good in their country or against their interests. It doesn't mean that it's not covert action.

In the cyber domain specifically, you know, I think – so two or three years ago, I think, you know, attribution was really hard for the private sector and for the U.S. government. I think it – I think things have changed a lot. And I think that companies and the government are much, much, much better at attributing cyberevents especially at – you know, I mean, if you start talking about, you know, the highest end actors, right, I mean, the more sophisticated, right? I mean, that's by definition – you know, they're hard to detect, but – you know. I mean, I don't think it's – you know, for example – you know, we know that the Chinese conduct industrial espionage against our companies. I mean, you know – and attribution, that's not the problem. It's crafting the appropriate policy response that achieves U.S. objectives and defines those objectives. Those – that's the hard part. You know –

MR. RISHIKOF: I know you say that, but as a matter of law, if you look at 18 USC – 1831 or 32, which is the Economic Espionage Act, we only actually have a handful of cases in which we've been able to make the attribution in law.

MR. GROTTO: It's very hard to prove. It's very hard to prove in law.

MR. RISHIKOF: So that's – so because the technology – that level of complication – I guess the question is whether or not Congress would be really interested in saying, look, we want to devote a lot of funds to solve the attribution technological issue because we want retribution.

Q: There's one option that I know Congress is looking at that right now – I talked to McConnell and others on the issue – is prosecution, you need a high standard, right? So economic espionage is not going to get us there at the statute, but you can use, you know, trade tariffs. You don't need – you don't need to –

MR. RISHIKOF: That level.

Q: – yeah. You don't need evidence to prove an accord. And Congress is not – talking to Mike Rogers, they're not going to do anything with the Economic Espionage Act.

MR. RISHIKOF: But they may do something with trade tariffs.

Q: Well, that's what they've been saying.

MR. GROTTO: Well, trade is tough because, you know, I think there's, you know, a golden rule to consider when talking about international – the international implications of our cyberpolicies. And if the Chinese do it to us, what would we think?

MR. BOSSERT: I don't think trade is any more difficult to discuss than war.

MR. GROTTO: Right. Yeah.

MR. BOSSERT: And –

MR. GROTTO: So just to real fast finish the thread. My own two cents was that, you know, there's a supply problem and a demand problem in – for – in the cyberespionage domain, country neutral, right? You know, countries – you know, go out and spy on behalf of their companies because the companies want the information. I think we need to look at both the supply side – obviously, we need to try to get the government – the governments that do this to change their behavior. I think it's very tough to do at least in the near term.

What I would like to see the U.S. government collectively do, and I think industry obviously – you know, we all need to be creative about how to do this, but address the demand side of the equation. How do you get the CEO and general counsel at a company that benefits from industrial espionage to think twice before receiving the information from the state sponsor? I think – I think that's an area of – worthy of exploration because – you know, if you can get that – the company thinking, you know what? Gosh, it's not worth the benefit for the prospect of liability, because, you know, they all want to do business in the United States still and – so then I think you talk about civil remedies rather than criminal remedies where the burdens of proof are different and – but go – please, go ahead.

MR. BOSSERT: No, this was interesting. We've expanded the scope a couple of times. It's going to whisper down the alley so I think I'll take them kind of in – out of order, reverse order here.

For a moment there, in the middle of this discussion, we were talking about something much bigger than the way we govern ourselves between Congress and the executive branch. And we were touching on things to me that are troubling, and I'll say this. Regardless of how we conduct ourselves internally, we have a sovereign right to defend ourselves. And that is a sacrosanct thing to discuss here.

We've sometimes gotten a little too mired in who's got authority and who doesn't. I tend to agree with the comment we've heard from the crowd here that covert actions are always taking place and they're always going to take place. I want to – I want to amplify that a little bit. That does not mean that they're taking place extra-judicially.

We've got – we've got systems set up for them to follow on, to notify certain members of Congress and certain very close circles, and we found that to be a practical solution to a – to a structural dilemma. Sharing these things with 535 members and their staff would be tantamount to unclassifying them. So that's just a quick observation from my point of view.

And I think that, among other things, I like your mutually assured destruction analogy from the perspective of this. We have a – we have a grand debate going on here about how much pain we can make each other feel, whether it's criminal prosecution or whether it's war or whether it's a trade tariff. But unless there's a disincentive – back to my earlier point – nation states are going to act in their best interest. And we're no different. And interestingly I think, we've had the upper hand. I think it's safe to say the United States is still number one in cyber trade craft in the world, followed closely by, you know, five or six others – Russia, China,

France, Great Britain – but we're still in the lead. And so I think some of what we've seen over the last 25 years is a maturity in the – and an arrogance that's kind of understandable. I don't condone it, but it is the case.

MR. RISHIKOF: We have another question.

MR. BOSSERT: And I guess one last thought here, the executive order – I want to be positive. I think the president mentioned cybersecurity in a State of the Union address, and that is absolutely right on 100 percent. I'm very glad he did it. I was – you know, in terms of when I stood and when I didn't, that – I would have stood for that particular comment.

I think those – we look at those speeches in history, it's funny what we take as important and what we go back and look at as funny. In the comment that he made immediately preceding – I don't remember; I'm paraphrasing here – but he was talking almost in a lecturing way about how we have to live within the ideals that we uphold and otherwise others in – you know, we won't be able to lead in the world. And then he pivoted to cybersecurity. I thought that was probably not by design. But I don't think we would want to live by some of the rules that we're creating. I think that – yeah.

MR. RISHIKOF: Another question.

Q: Harvey, I just follow up on your question. My name is Cliff Stearns. I've been in Congress 24 years. And I've done many oversight hearings as chairman of the Oversight Committee on Energy and Commerce.

I think whether you're Republican or Democrat, I think the Republicans are against this executive order the president's doing. They look like that it's a unilateral action by the president, which is not constitutional. The Democrats all think, well, listen. The Republicans won't do anything in the House and Mike Rogers had a bill. It went nowhere. There's a Senate bill that went nowhere. So the fracture, the balkanization in Congress has created this impasse so the president's taking initiative.

So I think – whether you're Republican or Democrat, you can understand his frustration. He wants to get something out, basic principle. But if that executive order ignites or starts appropriation process, then it probably is unconstitutional for him to start advocating and spending money without the House of Representatives approving it. So I think that would answer the question.

I think – what I found that in the – I was the ranking Republican on telecommunications for four years – Rick Boucher was the chairman – and then I had two years on the oversight committee. What I found is unless people are actually bodily harmed, there is not a trigger here.

We saw when – with Stuxnet and Iran, they couldn't do anything because there was no bodily harm. It was just we were smarter than them and they were not smart enough to detect it. And so we've almost taken this – what some members have felt is that we should be smart

enough to protect ourselves from cybersecurity, and if we're not, then it's our loss and it's really not an action of war but we're just stupid.

So, at this point, the United States should take the position – you know, the World Powers Act would come into effect if somebody got killed, and there was mayhem, and there was huge amount of deaths. But, otherwise, I think it's sort of up into who's brainier and who's able to handle this. And that is really the intellectual challenge we have here because cybersecurity, if it disrupts a nuclear power plant and we cause loss of electricity, that's not going to spring anything. But if it causes an explosion, that's going to. So I think that's a demarcation that you're talking about.

MR. RISHIKOF: It's very interesting because so much of our law and way of thinking about it is distinguishing between the physical world and the virtual world, and then, human casualties and property.

So one of the issues that cyber is raising though, it's eroding the concept of virtual and physical so you can use software and remote programming that have extraordinarily physical effects that will then have potential consequences for carbon units and people. So that's sort of the dilemma.

But I think we want – I think you can understand why people want to hold on very tenaciously to the concept if there's no loss of life, you don't want to do the War Powers Resolution.

MR. BOSSERT: One of the dilemmas we've seen here – I'm sorry.

MR. RISHIKOF: But that's sort of the dilemma for the system because so quickly, what we think an algorithm that's exploiting concern into an offensive weapon that will be able to take down a dam that will then have human aspects. So that's the knife's edge that we seem to be with the system, but you can understand why there are many people who want to maintain those traditional categories, because it makes life easier.

Does the panel feel these categories will remain over the next 10 or 15 years or do you see the erosion of the categories which will put the congressmen in a hard place?

MR. BOSSERT: I forget who said it, but somebody said that this is less of a dilemma between two competing forces and it's more of a debate with multiple moving pieces.

And so I guess I would agree with what you said and ask one question, Congressman. This notion of we need to be smart enough and if we don't, we're just kind of stupid about this, I want to define we.

One of the things that troubles I think everyone on this panel is the market's not working. And at least in my worldview, I'd like to think that the market would work this out. If this is a utility – we can talk about whether the Internet is a utility and should be regulated as such, but a

global utility is something we've never seen before and how we would manage that is equally problematic.

But we've – I work for companies – big, publicly traded companies that think through their tradeoffs in a way that are not stupid versus not stupid. They are in a way of short-term profit versus long-term potential risk. And they're simply allowing themselves to be open to vulnerabilities. And for a number of reasons, a number of reasons to include that they don't have enough money to compete with a motivated Chinese intelligence collection apparatus that can spend billions when they can only spend millions.

And so there are a number of things that I agree with you on, but when you talk about "we," I think that in terms of the question, is Congress appropriately organized, no. I don't know if there's a better way to organize it. I'm not the smartest guy in the room to tell you, but I'll tell you that the fiefdoms of power are going to cross this problem or this problem is going to cross those fiefdoms. And I think that's what we've seen it's already difficult to get something out of one committee.

But any cyber legislation, any true comprehensive cyberstrategy, we can defend ourselves in ways outside of the military and be smart in a lot of other ways in terms of law enforcement and tax policy and regulatory policy and trade tariffs and so on is going to end up – you know, to get down to the congressional weeds of it, the parliamentarians are going to give that to every committee on the Hill. And that's going to create a great difficulty.

MR. RISHIKOF: Remember, I was involved with the Project on National Security Reform with Jim Locher. And he did great work, and is behind Goldwater-Nichols, and we always laugh as one of our last reports was it's time for Congress to reorganize itself. And we were receiving funding from Congress. And Congress said, thank you very much, Jim, for that thoughtful idea, but we're moving on now. So that's another issue that's involved.

MR. BOSSERT: So Congress may not have to reorganize themselves, but it's going to require some executive leadership to set out a strategy on which they can chew because this is going to cross too many different I think power centers.

MR. RISHIKOF: Andrew.

MR. GROTTO: Well, we – you know, I'm from the Intelligence Committee Staff on the majority side. And Chairman Feinstein, who's one of the cosponsors of the comprehensive bipartisan cybersecurity legislation last year, she authored – and I was her staff – staff lead for her negotiator and drafter of the information title of the bipartisan bill. And that bill, you know, on the Senate side – you know, we have a rule called Rule 14 that basically the leader can use to bypass the committees. And that was how the bill was essentially expedited last year. Now –

MR. BOSSERT: But it passed.

MR. GROTTO: Now, other parts of the bill. Yeah. I know. It was filibustered twice. And now, the components of the bill, especially the parts on critical infrastructure, had been

subject to hearings the preceding two years and in fact had been marked up and passed out of the Commerce Committee and the Homeland Security Committee.

This time around – you know, I obviously can't – certainly won't – can't and won't speak for our leadership, but my hunch is that we will probably go through the regular committee process this time, simply because we have new members. It's a new Congress. And I think that – you know, on some important issues – you know, just take the issue I know best, information sharing – you know, there are some hotly debated contested questions that I think would benefit from debate.

So, for example, there's a very lively debate that broke out between the cosponsors of the bipartisan bill and the Republican alternative that Senator Chambliss, Senator McCain and others sponsored about whether information sharing is fundamentally a civilian or military enterprise. We took the view that it is a civilian enterprise. Senator McCain said that really the NSA ought to be front and center. That a – that's an important question and I think it – you know, we ought to debate that.

MR. RISHIKOF: It's a Rubicon question.

MR. GROTTO: Yeah, it's a Rubicon question. And I think – you know, that – I'm –

MR. BOSSERT: Gordian knot.

MR. GROTTO: Yeah. So I think – you know, as messy as it will be to go through, you know, the regular committee process, I think actually it will help illuminate and clarify the choices and make for a – for a better bill in the end.

MR. HEALEY: I think it's a great question. And I want to make three points. You know, one is to follow up on Tom. You know, when it comes to – we might – we rock on offense and we've gotten really good on offense, but those are all resources that aren't being used on defense. We are incredibly vulnerable and incredibly dependent. And if we – you know, if we use the we're smarter than them, then the Chinese are going to be feeling awfully smart because they're eating our lunch right now.

One of my friends, Bob Goreley always makes the joke, you know, we don't need a cyber czar. We already have one. It's Putin because Russian espionage is so deep – (inaudible).

The – I'm a bit concerned with – you know, with giving the executive branch the just don't kill anyone and things are OK standard because I think they'll run with that. And when I look at, to be more articulate on these than mere growling, the – it reminds me – as if we were going to say we were going to talk to the world comprehensively about the importance of maritime and, you know, we're going to talk about the critical importance of trade and how important trade that travels the seas are, and we're going to talk about the freedom of navigation, and we want security of the sea lanes, and all these norms, and we talk about how bad piracy is and how we're going to work to stamp out piracy.

And we barely kind of hint that we have a U.S. Navy; we sort of will talk about that, but the org charts are FOUO and – but what they actually do is kind of classified. And we sure don't mention anything about minding harbors. And when people wonder how really do we think about, you know, what we're going to do in the maritime domain, and we never talk about five-inch guns and anything else. And if that's all we talked about and we classified everything about the U.S. Navy, the rest of the world would say, this is kind of a – maybe there's a mismatch here between what they say and what their CIA and their sailors seem to be actually doing.

And so that's my only point on this, and maybe this is going to affect, you know, our merchant seamen that are trying to travel the world and are they going to get affected. You know, what's going to be the blowback on them on that. I'm just saying that we need to be a bit more careful than I think we are.

MR. RISHIKOF: So on that point, I'll let you speak, but we did a big project on piracy. What we realized was the key to piracy is Lloyd's of London. (Laughter.) And because Lloyd's does this underwriting business and the shipping industry has it as just a cost of business, as long as the – everyone follows the rules and you don't kill the sailors, everyone can tolerate the system from a market perspective.

So one of the interesting aspects is where is the insurance companies in the cyber area? And I think it's a question, Tom, before they're drawn in and that's going to be fascinating.

MR. BOSSERT: That is the future of our –

MR. RISHIKOF: So I think – let me give you the last word, Derek.

MR. KHANNA: Sure. In answer to your question, I would argue that our current paradigm, even not involving cyberwar, is insufficient when you look at drone war in particular, which is we have a tool of war that allows for us to use our civilian agencies to seemingly bypass the checks and balances that we have with the executive both for the War Powers Resolution but also through other tools at Congress' disposal.

So from my perspective, it's already problematic. And from my perspective, cyberwar takes that to a whole another level. So some actions of cyberwar have very close analogies to that of kinetic operations. If you were able theoretically to hack into somebody's phone and make the phone explode and assassinate them, that would be very similar to a sniper's bullet, no real difference there.

But that still wouldn't constitute the introduction of U.S. armed forces. And, obviously, that's a small-scale operation so let's just do something bigger. Let's say that when the Iranians develop their first nuclear warhead, we made it known to them that if you develop a nuclear warhead, we will destroy the nuclear warhead. And we had infiltrated their systems so absolutely that once their warhead was constructed – again, theoretically; this is a little bit more complicated than I'm going to make it sound – we had a virus in their system that detonated that nuclear warhead inside of Natanz, in their own facilities, killing potentially hundreds of thousands of Iranians. Now that's clearly an act of war. Under the War Powers Resolution, at

least my reading of it and I think your reading too, that would not be the introduction of U.S. armed forces.

MR. GROTTO: Not my reading. Or, no, it may not be introduction – that case I think is an easy case. I think that is – you know, you're talking about the scope, duration, nature of – I mean, a nuclear bomb going off I think is –

MR. KHANNA: The law says the introduction of U.S. armed forces. Are bits and bytes U.S. armed forces? What about if it's CIA launching the attack versus the NSA because the actor has to be –

Q: (Off mic) – of war hostilities is based on the legal threshold of what hostilities means. And the drafters knew that in the legislation that the administration that – and that's the scope, duration and intensity.

MR. KHANNA: Yes, but it's –

Q: (Off mic.)

MR. KHANNA: It's actor and act. It's hostilities and introduction of U.S. armed forces, which has a legal meaning, which doesn't mean CIA.

MR. RISHIKOF: I guess we'll end of this.

MR. KHANNA: But the second part of that is, even if the War Powers Resolution is invoked, which we disagree on, the real teeth of the War Powers Resolution are that within 60 days, you have to pull out your troops. What does that mean in cyberwar? So even if the War Powers Resolution is invoked, it has no real application. And that's why we need to structurally revise this.

MR. RISHIKOF: I guess that's a great way to end because, just as a citizen, I would think if we're going to be setting off a nuclear bomb that Congress should be informed more or less. It would be nice for them not to read that in the paper the next day.

I guess the first thing is I want to particularly thank the panelists, who have done an extraordinary job. I want to thank the audience, but more, particularly, I want to thank the Atlantic Council, because I've written a book in which we have an edited chapter on think tanks. And we score all the think tanks in the city. And one of the rules of scores was is it a think tank that is bringing together people to discuss vital and important issues? And is it having an impact on how that public policy debate is going to take place and be resolved? And I think, Jason, you and the Atlantic Council are fulfilling the top grades on that – of what a think tank should be doing in town. I think we all want to thank you for that even and bringing us together. And we look forward to more events that you're going to having, OK?

MR. HEALEY: Thank you. Thank you. (Applause.)

With moderators like you, Harvey, that makes it easy. Just some closing points. On the insurance point, we are going to be doing a big event – series of events this year with Zurich Financial looking for – (inaudible) – aggregation of cyberrisks and that will apply, of course, to insurance. Please remember our event, the Cyber 9/12, at the Newseum on 7 March. I'm working with Catherine Lotrionte for her international cyber conference on the 10th of April, our book in June.

And last, you'll see – we're the Cyber Statecraft Initiative and – because we think we need more cyber statesmen and women, so I'm going to be presenting our cyber statesmen mug for each of our panelist for helping –

(End of audio.)

(END)