American University National Security Law Brief

Volume 3 | Issue 1 Article 6

2012

Fall Cyberwar Symposium : Keynote Speaker

American University National Security Law Brief

KEYNOTE SPEAKER

STEVE VLADECK: I think that we're going to get started with our keynote speaker. I'm Steve Vladeck. I teach here at WCL, and it's really a pleasure for me to introduce today's keynote speaker, Duncan Hollis, from Temple University's Beasley School of Law.

Duncan is the Associate Dean for Academic Affairs and Professor of Law at Temple. His scholarship focuses on the issues of authority in international and foreign affairs law, researching the actors who exercise authority in the formation, interpretation, and application of international law. He also researches "who has" the authority to apply such law to or for national actors, and uses treaties as a focal point in his research. He is a prolific author. He's the Editor of the brand-new Oxford Guide to Treaties, which is currently the subject of a fascinating symposium on Opinio Juris. Opinio Juris is an international law blog. If you don't already read it, you should. I think that the most recent post is by Harold Koh, who is the current Legal Adviser at the State Department, although maybe not for that much longer.

His scholarship has widely appeared in various books and journals, including the TEXAS LAW REVIEW, the SOUTHERN CALIFORNIA LAW REVIEW, the VIRGINIA JOURNAL OF INTERNATIONAL LAW, and the BERKELEY JOURNAL OF INTERNATIONAL LAW. But perhaps most impressively, Duncan actually has practical experience, too. After he graduated from BC Law School at the very top of his class, he worked for the International Department at Steptoe and then spent six years working at the Office of the Legal Adviser at the U.S. Department of State. So he actually, you know, isn't just making this presentation up.

But I have to say that perhaps most importantly - well, to me anyway - Duncan is an old professional friend of mine, or at least a longstanding professional friend of mine, and we just were reminding each other of how we met. We met at a symposium back in 2006 at Lewis & Clark Law School in Oregon, where Duncan gave a talk about information operations. This was a symposium about all sorts of current issues in national security law, and [information operations was not as well-discussed within this field of law as it is now]. This is the real dirty secret, right? In our field, there are always current issues that are worth discussing, except that we were all sitting there saying, "Holy cow, this is really awesome and neat and totally hypothetical and, you know, maybe in 20 years he's going to really be on to something." We actually - we knew then that he was already on to something.
So here we are, six years later, and not only is information operations at the heart of a lot of these conversations, but Duncan really has sort of gotten out ahead in what will be perhaps the most im-

portant field of national security law in the next five to ten years. So please join me and welcome our keynote speaker, Professor Duncan Hollis.

PROFESSOR DUNCAN HOLLIS: Thanks. Thanks, Steve, for that entirely kind introduction, and to the AMERICAN UNIVERSITY INTERNATIONAL LAW REVIEW and to the NATIONAL SECURITY LAW BRIEF for inviting me to this conference.

I want to start off with a couple of stories, neither of which involves Lewis & Clark Law School; the first actually was in 2001. I was still living here in Washington at the time and was still at the Legal Adviser's Office, and I got asked to be part of a U.S. delegation to the Council of Europe to negotiate the final clauses of the Convention on Cybercrime, notwithstanding the fact that I didn't do anything with cyber or crime. And, you know, I was, frankly, working in other areas of international law at the time. But it struck me as a forward-thinking treaty, right? The idea was we were going to deal with the fact that information technology had increasingly become a new tool that criminals were using to pursue illicit ends, and that that very technology was also becoming a new target for criminal activity.

So we have this treaty, it's negotiated, and basically the general purpose of the treaty is to get states to harmonize their cybercrime laws. First, we're going to agree on certain cybercrimes, and everybody will criminalize them domestically; things like illegal access or data interference. And then, second, everybody will agree to cooperate on combating those crimes.

Today, the Convention on Cybercrime has 26 parties, including the United States. Unfortunately, I don't think that we can say that it's been a great success. States that folks hoped would join, like Russia, refused to do so, and the reality is that the envisioned cooperation under the treaty tends to take months, not seconds or milliseconds, which is really all the time that it takes to commit a cybercrime. So that's kind of my first personal story. The second story is the one we were hearing earlier this morning, and that is the story of the demilitarization of cyberspace, right? Over the last decades, militaries, like criminals before them, have started to recognize that information technology presents both new tools for warfare and new targets in warfare. So today we've got dozens of militaries building up and deploying "cyber forces", including our own here in the United States with the 2010 establishment of USCYBERCOM, which is tasked to further national security in both cyber defense and offense. And at the same time, we have folks talking about information technology as a target; this was notably referenced earlier this morning, being Secretary Panetta's recent statements a few weeks back that the U.S. is vulnerable to a digital Pearl Harbor.

Now, I lead with these stories to highlight the different ways we might construct a legal framework for cyberattacks. Now, let me take a brief tangent and make clear what I mean by a cyberattack. What I'm talking about is kind of the standard definition: information technology is used to deny access to, to disable, to disrupt, to degrade, or even to destroy another computer or a network or the

infrastructure of that computer and its network support. And in that respect, we should distinguish cyberattacks from what are called cyber-exploitations, right? Cyber-exploits are basically Internet espionage, old-fashioned spying. You're getting onto somebody's network, but you're not disabling, disrupting, or degrading it in any way; you're just snooping around.

In any case, I think that we're at the beginning of a conversation, maybe a fight as it were, about what legal regime is best suited for cyberattacks, right? And I also think the decade-long debate over global terrorism suggests a possible roadmap for how that fight or discussion is going to play out. There, [in the context of the global war on terror], you'll recall that four options emerged for how law should respond to the global terror threat.

Option one: Terrorism is a crime, right? It's going to be dealt with by domestic criminal laws and law enforcement transnational cooperation, and some still insist that this is the only way that we should deal with terrorism.

Option two: The U.S. view after 9/11; the U.S. government says "No, terrorism is not a crime, it is war." And the laws of war are the only appropriate regulatory framework from which to combat this threat.

A third group tried to say "Hey, why can't we all just get along," and said "Why can't it be both? Why can't it be both crime and war, and we can use both legal regimes to try and regulate or mitigate the threat?"

Fourth, and finally, some - most notably, the first of today's speakers, Professor Ken Anderson – were, for a while, pressing the none-of-above button, right? The none-of-the-above button is, wait a minute; maybe it's neither crime nor war. Maybe it's something different and for which we need a new legal regime.

I think we're seeing the same jockeying among camps playing out in the cyber-context now, right? So we have a war camp, I think illustrated by this morning's panel discussion; by the existence of USCYBERCOM; by the, you know, now famous Stuxnet virus disabling Iranian nuclear centrifuges. But there's also a crime camp out there that says "No, no, cyberspace should be dealt with through criminal law means." China is actually the most notable proponent of this camp. The Chinese government continues to officially refuse to admit that the laws of armed conflict, that is, the laws of a war, are applicable in cyberspace. They just think that cyberspace is totally off limits for those rules. Now, some states and scholars have tacked to option three: that cyber is both crime and war. Indeed, that's how the Estonian government responded in 2007 to the directed denial of service attacks on it that took down their networks for a period of time. The Estonian government said, you know, "This is an act of war." At the same time, they also made extradition requests and sought mutual legal assistance to deal with the threat under their own criminal laws.

So perhaps not surprisingly, having explored those three bases, what I want to do with my time here this afternoon with you is to explore option four in cyberspace: The none-of-the-above idea.

Let me be clear at the outset though. I am not, I repeat not, contesting that cyberattacks may be subject to both the existing rules of criminal law or to the existing rules on the use of force and the laws of war. But I do think that the Chinese position is simply wrong. It's true that the cybercrime convention is the only cyber-specific set of rules and international law that are out there, and it's also true that that treaty specifically exempts government authorities from the treaty's ambitions. So, if it's a state-sponsored cyberattack, it's not a cybercrime under that treaty.

But that does not mean we're in some sort of law-free zone. Those of you who have studied international humanitarian law may recall the famous core principle called the Martens Clause, right? Just because a method of conflict isn't prohibited does not mean that it's necessarily permitted, and indeed, the law of armed conflict has a long history of enveloping and integrating new forms of warfare under its ambit, whether it's submarines, air power, or nuclear, biological, and chemical weapons. So I have no problem saying that the laws, both domestic and international law, may apply to cyberattacks.

What I do dispute is the efficacy of that status quo, right? And I dispute it in two respects. First, I don't think that the existing rules serve as a sufficient and complete response to the regulation of cyberattacks today. I think we need new rules. And second, I think that we need new types of new rules, right?

Some say what we need to do is simply refine the criminal law or refine the laws of war to adjust to this cyberthreat environment. But I want to pitch a different type of regulatory response to you today; what I call an e-SOS for cyberspace. My first point is relatively straightforward, and that is that there are substantial flaws in the current "law by analogy approach" that we use for cyberthreats. I've written about it at some length, but let me distill it down to two, right? There's a problem of uncertainty, and there's a problem of complexity.

In terms of uncertainty, what I'm talking about is what we could call translation problems; we need to take this centuries-long doctrinal set of rules and practices and translate it into the cyber-context and apply it to cyber-conflicts. I can expand on that uncertainty if we have time for Q&A, but let me flag just one obvious example, right? The so-called jus ad bellum: the rules on the use of force. As many of you may know, the U.N. Charter prohibits states from using or threatening to use force unless the state is either acting in self-defense or is acting under the authorization of the Security Council.

So, how does that rule translate into cyber? Interestingly, if you actually look at the U.N. Charter,

Article 40 talks about how the disruption of communications is not a use of force. So, one could actually say that maybe the Chinese are right in saying that the U.N. Charter doesn't apply to cyberattacks. Pretty much with the exception of China, very few people agree with this conclusion. Murray Machervey says that cannot be what the U.N. Charter means. The problem is that consensus quickly breaks down when you ask people "when exactly does a cyberattack rise to the level of a use of force?" Or, just as importantly, when, if you're a victim of a cyberattack, can you treat it as an armed attack to which you can exercise the inherent right of self-defense, and by which right of self-defense you could exercise, of course, through cyber means, but also via kinetic means, right? Guns, bombs, missiles, and the like.

So take Stuxnet, for example, right? I've been to, say, half a dozen conferences on cyber just in the last year. And I think there's been one universal truth to those conversations, and that is that there is absolutely no agreement on whether or not Stuxnet was or was not compliant with the jus ad bellum, right? Was it a use of force, or was it not? I've heard very distinguished, very well-thought-through defenses of both why it was and why it wasn't a use of force.

Now, there's been a recent effort, the so-called Tallinn manual, to try to undertake the necessary translation of the existing rules into cyber. It was a project overseen by Professor Mike Schmitt of the Naval War College, who's been at this for a long time and has done a bunch of serious and influential scholarship on international and humanitarian law generally, and also with respect to cyberspace specifically.

And I think the idea was that he would pull together experts writing in their private capacity to try and codify what the existing rules are. And I think that the manual should be praised; it just came out this summer. It should be praised for sorting out the issues, right? Where are the hard questions regarding cyber, and what is the universe of opinions and answers?

But if you actually take a close look at the text on some of the most important questions, it's not clear the Tallinn manual gives us that many answers, right? It gives us kind of general statements, and then a lot of divided views; such as a majority of folks took this view, a minority took that, or there was a disagreement about X, Y, or Z in cyber.

Now, on the jus ad bellum, the Tallinn manual does give us a triggering rule, right? It says in Rule 11, "a cyber-operation constitutes a use of force when its scale and effects are comparable to non-cyber operations rising to the level of a use of force", right? So we're just going to analogize to whatever in the non-cyber context is the use of force. If it has a comparable effect in scale - and scale, that's a use of force. I wonder, though, whether states are going to bite on that rule.

For example, I don't know how this line drawing works with respect to Stuxnet, right? Can we really compare its scale or effect to non-cyber operations? After all, what it did, getting in there and target-

ing one or a couple of series of centrifuges and doing nothing else but spinning them out of control, was something that no one had thought possible before. It was, as Professor Vladeck said when he introduced me, "what we used to think about cyber was its science fiction", right?

And so if it's really something we've never seen before, how can we say that it's comparable to some non-cyber operation rising to the level of a use of force?

On the other hand, do we really believe that if the tables were turned and this had been happening at a U.S. nuclear facility, that the United States would just sit back and say, "Oh, well, that's just a criminal act; that doesn't implicate the rules on the use of force or the laws of armed conflict in any way." And this is when a cyberattack actually destroys something. There's the larger question of what happens when it's just disrupting or disabling something; taking down the New York Stock Exchange for a day, or moving everybody's Bank of America bank accounts two decimal places to the left, right? Is that the sort of effect and scale that is comparable to some use of force in a kinetic context?

Now, the commentary on Rule 11 tries to help us out, right? It says "Oh, but we'll tell you. There's a multi-factored analysis by which you can assess whether the effects are going to rise to the level of the use of force," and there's actually seven different lines of analyses, right? We're going to analyze the attack's severity, its immediacy, its directness, its invasiveness, et cetera.

I'm generally in agreement that effects do matter, and I think that Professor Schmitt's work was critical to getting folks to focus on the effects of cyber as a way to reconcile existing legal rules to it. But, I'll be honest; I'm a bit less sanguine about the ability of operators on the ground to apply seven factors to a cyber-operation in real time, particularly if you're on the receiving end of a prior attack. I think it smacks more of a certain standard that a court might look to apply than some ex-anti-rule that can guide folks in actual operations.

So I think we've made some real progress in clarifying how international law might apply to severe cyberattacks, but I think there's still too much uncertainty out there. And make no mistake; uncertainty is not a good place to be, right? We're in a situation where I think we've got either one of two situations.

Either we're left without any real sense of what the legal rules are on what you can and can't do in terms of using force, and that may mean that you don't use it at all, right? Even when you could disable a power grid instead of bombing it, right? You could not have any collateral damage, or have collateral damage on the networks. We might not use it at all, right? That's one view.

Or we're in a world - and perhaps this is more worrisome - where people assume they know what the rules are. I think the Defense Department is pretty confident that it knows what the rules are for

cyberspace, but we just haven't gotten around to telling anyone yet just what those rules are. And I worry about that, too, because I worry that when they do, we may discover that other people, the Chinese, the Russians, don't agree on the U.S. views of the rules, and so we end up having pretty widespread disagreement about the rules of the game. So there's a problem of uncertainty.

There's also a problem of what I would call, somewhat paradoxically, the complexity of the existing system. What do I mean by this? Well, most existing analyses by international lawyers at least have focused on cyberconflicts and cyberattacks with respect to international humanitarian law, and more specifically to the context of international armed conflicts, right? You know, war between two states, China and the United States, or China and Russia, or what have you.

I think the reality is that that's a really small slice of what people are worried about today, right? I think that you heard Professor Barry talking earlier about that as well - you know, we're unlikely to have a pure cyberwar. What's likely to happen is that if you're in an armed conflict, cyber may be a force multiplier; it may be used in the context of a conflict, but it's not going to necessarily be the only vehicle for conducting one.

What most people worry though isn't that proverbial war between two nation states; it's terrorist cyberterrorism attacks by terrorists if they figure out how to use these tools. It's cyberthreats by various non-state actors, and there, you know, international armed conflict rules don't have all that much to say. The laws of armed conflict do regulate it a bit, but what happens when it falls below that threshold? What happens at, say, one step, one tick, below something that people would say "Oh, yeah, that's an armed attack" or "That's the use of force?" Then we've got a whole mess of overlapping legal regimes that purport to regulate both what states can do offensively, you know, in sending out attacks from their forces, or defensively, when put under attack, right? You have to worry suddenly about the International Telecommunications Union, which, by the way, next month is going to take up revisions to its regulations and there's going to actually be a push for the ITU to take over the Internet. Rest assured, I understand the United States government is not onboard with that move, but we must deal with these regulations on international telecommunications. We have to deal with rules on satellites in outer space, rules on the law of the sea, and even at some of the most basic rules for interstate relations, as it were.

So to pick up on one of the hypotheticals presented in the earlier session, take a cyberattack by terrorists on the United States, a really bad attack might trigger the right of self-defense, although notably the International Court of Justice disagrees and says that non-state actor attacks always fall under criminal law. You can't use the use of force regime to respond to an attack by a non-state actor. The U.S. doesn't accept that view, but it does accept that if you're attacked by a non-state actor, your duty is to go to the state where you think the attack came from and ask them to handle it. And if they don't, if they are unable or unwilling, then you might be able to engage in self-defense.

But note one of the defining features of cyberthreats or cyber-capacities is speed, how quickly it can work. And once you start to impose these process requirements, there's a real question of "can we effectively deal with the threat if you have to have all these whole conversations in real-time when the threat itself can be executed in milliseconds", right?

And in some ways, you're not allowed to directly respond, particularly if it falls below that use of force or armed attack threshold. There, the principle of non-intervention rules, right? You're not supposed to intervene in other state sovereign territory. It requires that you are literally left to the whim of that other state from which you think the attack originated, and you have to say to that state, "Pretty please, will you stop this? Will you help us out?" And you're not really in a position to do anything without violating international law, right?

And, so all told, I think these problems of uncertainty and the complexity of the existing legal regime suggest a system that is extraordinarily hard for nation states to navigate, right? Is it that reasonable to expect militaries and their lawyers to process all these legal questions simultaneously, particularly in an environment that often is characterized by near immediate threats?
And do we want, in some ways, the disincentive to use this technology that that uncertainty and complexity creates, or might we not actually prefer a world in which cyber is being used in lieu of boots on the ground or ships at sea? So in other words, I think we need to at least think about moving beyond the existing law by analogy paradigm even as it currently tries to regulate these new threats and these new tools for crime and war.

So what do we do? Well, certainly I think we could, like the Tallinn manual, try and clarify and translate the rules, and get more certainty and simplicity, and maybe get less complexity. But I'd argue that those efforts are somewhat misguided. I think that there's a fundamental problem with using cybercrime rules, or the rules on the use of force or conflict to address severe cyberthreats.
The reason I think that this is so is because both criminal law and existing international law depend, for their operation, on a key element, and that element is prescription, right? What we do with prescriptive laws is target the bad actor, right? We're going to forbid acts by specific persons, groups, or governments, and we're going to hold accountable those we catch having engaged in the prescribed behavior. But for prescription to work, you need something that's really hard to do in cyberspace; you need attribution, right? The ability to identify with sufficient certainty who the bad actor is, whether it's an individual hacker, some hacktivist group, some criminal organization, or even a state's military.

But make no mistake that today deterrents through attribution is the law's existing response to cyberthreats, right? For some, it's the only response. So Major General Keith Alexander, who now heads up Cyber-Command, has said, quote, the bottom line is, quote, the only way to deter cyberattack is to work to catch perpetrators and take strong and public action when we do so.

And I'd argue, notwithstanding some comments from the panel earlier this morning, that this approach is problematic in an environment where anonymity, not attribution, prevails. Certainly, attribution can occur sometimes if the attackers are stupid, or if they're unlucky, or if they're secondary intelligence; and sometimes secondary sources divulge the identity of the attackers. Or as in the case of Stuxnet, maybe one of the perpetrators wanted to signal who had done it, right?
But the reality is as much progress as I think NSA has made - and maybe they know who's doing some of the attacks, but they're not telling anyone, and they're certainly not telling the banking folks, the oil folks, the water filtration folks, you know, what they need to be worried about, who they need to be worried about being the victim of.

And so I'm not sure from a technical perspective that we're as far past this attribution problem as some might suggest, because the reality is that if you have sufficient technical skill, and if it's cheap, that the attacks can occur remotely from anywhere, even from the Starbucks across the street, right? You can go over there and you can plug in, and maybe you could, you know, organize your command and control of your own botnet, and you could take control of hundreds of thousands of computers and ask them to do something. You know, those with skill can hide their origins, or they can send up for that false flag and make it look like somebody else did it, right? And in some situations, what's really worrisome is that the victim may not even realize they've been subject to a cyberattack at all, right? There's always that kind of question of, well, was that blackout actually somebody - was it really a tree branch, or was it a cyberattack being perpetrated?

Now, how do we deal with this attribution problem? Well, maybe we, as the law sometimes does, assume attribution based on things like the type of the attack, its target, or the country of origin. I am not terribly confident that such assumptions can work, right? I don't know if any of you remember, but there was this thing called Solar Sunrise. In 1998, the Defense Department was under what, at the time, was the most serious set of cyberattacks hacks on its system that it had encountered to date. Senior Defense Department officials told the White House that the attack had to be coming from Iraq, given that, at the time, we were going after Iraq for violating the no-fly zone, et cetera. And the U.S. government was convinced that it was Iraq or Iraqi proxies that were responsible, when in fact it was three teenagers: One in California and two in Israel.

More recently though, people said, "Well, let's not worry about whether or not only certain attacks can come from nation states the way we assume only certain nuclear or chemical attacks can come from nation states. Maybe we just trace it, right? Maybe we look to where it's coming from and hold wherever we find the attack's origins to be coming from; we'll hold them responsible." Of course, that would mean the United Kingdom was responsible for the July 4th, 2009 attacks on the United States, White House, Treasury Department, and Secret Service servers, as well as a number of South Korean websites, both corporate and government, because investigators traced those attacks to Brighton, England.

Or, more dramatically, perhaps, it would mean that the United States is responsible for approximately a quarter of all cyberattacks occurring in the world today, since that's where they're coming from, with China following closely behind. So I'm not sure the assumption of attribution is going to work terribly well.

Well, how can we fix that? How can we make the existing rules work? Well, as Larry Lessig famously wrote , code is law. And unlike other environments where a weapon must conform to the law of physics, in cyberspace we can construct the laws of nature, as it were. We can rewire the Internet to remove the attribution problem so that you would have to know where an attack is coming from or who is responsible for it.

Is this feasible? Technically, it would be pretty difficult; economically, I think the transition costs would be tremendous; and so far I'm assuming that we're all in agreement that attribution is a problem at all. It's at this point I want to remind everyone that there are for some who view the anonymity that the Internet affords as something to be championed, a vehicle for free expression, for privacy, for a tool to be used against autocratic regimes and oppression everywhere. And for those folks, we don't want to fix the attribution problem; we want to preserve it.

So we're actually now in a situation where legal prescriptions, whether criminal law or international law, are premised on an attribution that occurs rarely, if at all. Less than five percent of cyber-criminals are arrested or convicted. No state has officially taken responsibility for a cyberattack, although you may get a wink and a nudge from U.S. government officials on Stuxnet, nor is there any consensus on a state having done one in violation of international law even if you could attribute it to them. We don't even know if certain various accidents involving computer error, such as the North American blackouts or the like, are actually the results of error, or some subtle planning.
So I want, then, to convey to you that you need to think about how this attribution problem affects the ability of law. The ability of law which, as law students and lawyers, we're all concerned with; how the ability of law to regulate this problem. High-level attackers can, today, attack with impunity. They are not being deterred by anything law has to say, and I think that's consistent with what we've already heard.

More worrisome still, as I suggested already, is that the attribution problem exacerbates that uncertainty problem I already highlighted, right? Because we have a real risk that victims and attackers may be applying different sets of rules to an attack. The Defense Department has told us we will act in self-defense. The United States will act in self-defense even if we don't know precisely who launched an attack. So say that a cyberattack disables critical infrastructure in the United States and kills people, ok? The United States could treat it as an unlawful use of force, an armed attack, and respond against the territory where it thinks it's originated with force.

Of course, what if it was a false flag and the U.S was wrong in its assumptions, its intelligence got it

wrong? That happens sometimes, right? Or it simply looked like it came from that state, right? Even if it did originate there, what happens when the nation state didn't know about it, right? There's the practical stories that how North Korea does cyberattacks is they get on a plane and they go to a hotel room somewhere and plug in for the weekend, hack, and then go home, because, you know, North Korea's infrastructure doesn't support their ability to launch attacks from within their territory, right? So they're doing it out of some hotel in Shanghai. How do we distinguish that? Is that a Chinese - a cyberattack, or one from North Korea?

The state, of course, who relies on these attacks and things - well, maybe it's cybercrime - might say, "Well, we should deal with this through law enforcement means." But once the U.S. has employed force, they're going to view the U.S. employment of force as itself a violation of international law, and they may respond with force, and suddenly we have an unintended escalation of a situation into an armed conflict. So the bottom line for me is that I don't think law can deal with the most severe cyberthreats simply by regulating the bad actors.

So what else can law do? Well, we could try and regulate the instrument by which the bad actors deliver their threats; regulate information technology. Russia's been barking up that tree for the last ten years. But I think banning cyber-weapons seems a difficult proposition, let alone figuring out how you're going to verify that cyber-weapons have been taken offline, and not to mention the problems of privacy and free expression that the Russians are also keen on regulating as a weapon.

And if you can't regulate the bad actors or the instruments they use, well, the other thing we could regulate is the victims, right? We could say, by licensing requirements or liability requirements, that "victims, you need to harden yourselves", right? You need to take mandatory security steps, or you have to allow the government to monitor and control your computer systems and networks to ensure that you don't get attacked. That is, unsurprisingly, very controversial in certain Internet circles. You can recall events from a few months ago, the SOPA and PIPA reactions, and Wikipedia going down for a day, to see the depth at which people oppose regulating what users can do on the Internet. And indeed, I think fear of these sorts of requirements in part frustrates the efforts of the United States in getting cyber-security regulation, which we're going to talk about after lunch. So how do we regulate cyberthreats in a world where you can't regulate the bad actors, you can't regulate the technology they use to attack, or the victim's defenses? This is a problem.

So for the last couple of years, I've been pitching a modest proposal: that we could devise a different regulatory scheme; what I call the duty to assist, all right? An e-SOS, right? The idea is let's look at what the law does with other threats out there that are difficult to prescribe and stop or to regulate the technology. Hurricane Sandy, for example. If you're a ship at sea last week in Hurricane Sandy and you're in trouble, you can send out an SOS, and anyone who hears that call is legally obligated to respond. And indeed actually, the victim can sort among the various responders and pick the one best suited to lend its aid.

There have even been more dramatic instances of the SOS in recent years. There was, in 2007, a North Korean vessel that was attacked by Somali pirates off the coast of Africa. The ship sent out the SOS signal, and the United States destroyer, the James E. Williams, responds, and engages the pirates in a fire fight and manages to kill a few and capture the rest and save the North Korean vessel and its crew. This is a country where we have thousands of troops marshaled on their border, and we're doing everything short of going to war to stop them from pursuing their own national security interests, and yet, when they call for help using an SOS, we came to their aid.

Now, packet switching is not sailing any more than cyberspace is real space, but I do think there are similarities between the environments of sea and cyber, right? In both environments, there's a tremendous range of threats, from "Oh, Microsoft Outlook has crashed" to "Holy crap, they've taken down the North American power grid," right?

There's a whole range of threats, and there's a whole range of causes. Sometimes it is the technology, some kind of operating error that brings things to a halt. Sometimes it's outsiders; sometimes it is insiders. And all these threats can have unclear origins. You don't necessarily know where the storm is coming from; you just know that you're in a storm, and the same way, you don't know where the attack is coming from, you just know that your site is down.

Okay, so why would states agree to this? Why would they agree to some sort of a duty to assist as they have in the maritime environment or in outer space or with respect to nuclear accidents? Remember, these are all areas where international law says "Hey, you're in trouble," you send out a call for help, and people who can help are required to do so.

I think one reason why you might think about an e-SOS system is functional necessity, right? To the extent information technology has become indispensable to modern society; we need to have regulations that allow it to function, right? Just as the SOS promotes a robust maritime environment where the laws of war and the laws of crime don't necessarily work properly; it's too big a space for us to individually police it. So, too, might we think about a duty to assist regime for cyberspace.

And second, cyberthreats do have a reciprocal aspect to them, at least in their most severe form, that might incentivize people to cooperate, because in cyberspace, everybody's at risk and everybody can help each other. Even an individual user can help a major state and a directed denial of service attack against it by, as Professor McNeal says, unplugging your computer, whether you're the victim or the attacker, right? We can individually and collectively provide assistance.

Now, assuming that you have followed me so far, states still need to actually construct an e-SOS system, and I've talked to some about how they might do so. We've got to elaborate what cyberthreats to cover under this e-SOS system. Presumably we're not going to regulate it when you lose you law

students lose your 1L outlines because your computers crash, but we might want it to cover protecting water filtration systems, hospitals, nuclear plants, and the like. We need to define what cyberthreats to cover, and which victims can invoke the duty, right? Can you and I "hit the red button" and put out an e-SOS call, or is that ability limited to Internet service providers - or some other set class? How does one call for help? Is there really going to be a button or some website you can go to and send out the flare?

Who has to provide the help? Obviously, the nature of the technology would allow an SOS to be heard by everybody, unlike the sea where you send out the SOS, and the folks who are most proximate to your danger are the ones most likely to provide assistance; that's not as true in cyberspace. So we might need to regulate who has to provide the help and what kind of help they have to provide.

But I do think it's something worth considering. However, this idea is not without costs. It certainly can cost something. And I think that what one thinks of those costs depends on what one thinks of the status quo, right? If you view the status quo as okay, and indeed, in the status quo sometimes when things go wrong, there is substantial informal assistance out there that's occurring among states, individuals, particularly among companies cooperating to combat certain cyberthreats. The Conficker Working Group is a prime example where public/private partnerships were formed to stop a particularly bad form of malware and get it off of our systems. However, regarding extreme threats, I just don't think that this assistance is adequate, right? Most cyberthreats, 80 percent by some estimates, go unreported, right? Where assistance occurs, moreover, nothing dictates who gets it, let alone what kind of assistance you get.

Now, I think an SOS system would respond to those deficiencies. Many victims stay silent because they think, "Well, if I admit that I'm vulnerable or that I've been attacked, it's going to hurt my brand, it's going to hurt my bottom line." Look what happened to Google when it had to admit that it had been hacked by China, right? There's a negative reputational effect, but there's no upside as it is. But if you have an SOS system, at least you know, "Okay, I've got to put myself out there as being under attack, but the law will impose on others a duty to assist me to remediate the threat or remove it. Motivate enough people to do that, you could get a cascading response where disclosure becomes more the norm than the current exception that it is.

I think that the duty to assist could improve the quality and quantity assistance victims receive, right? So when Estonia asked Russia in 2007 to cut off the directed denial of service attacks it said were coming from Russia, Russia said, "Oh, you know how spoofing works. That's probably somebody else using our systems to attack you. Sorry, we're not going to do anything." If Russia had a duty to assist, Russia would have had more difficulty doing nothing. It would have had to take steps to do something, perhaps cutting off that traffic that was causing the directed denial of service attack.

I even think that an e-SOS system could do that deterrence thing I was talking about earlier. Once the duty to assist is established, states need to consider the costs and benefits of complying with that duty as part of any decision to launch their own cyberattack. So either you make the attack openly and defend its legality, or you continue to do it anonymously, but then you may actually have to participate in cleaning up the mess you yourself made, and that cost of cleanup has to be included in part of the original calculation of whether it's worth attacking at all. So in that way, an SOS system could deter the - could do the very deterrent function I think is now lacking in rules on cybercrime and cyberwar.

But what if I'm wrong? Say that the e-deterrent system does not fully work. I do think it would increase the resiliency of our systems and networks, right? It would at least help victims mitigate the harm. Maybe we wouldn't catch the bad folks, but it would at least help them recover more quickly and get them back on their feet to return to tolerable operating conditions.

And finally, I guess that one last thing I'd say about all of what I'm proposing is that none of this is in conflict with existing law. In fact, it would complement rather than conflict with existing approaches. It leaves the prescriptive rules of cybercrime and the rules on cyberwar in place. Indeed, if attribution efforts bear fruit, criminals can be prosecuted or states be held accountable for their actions, and e-SOS could even help if that assistance assists in attribution in making those laws work better. All said, I recognize that it's an ambitious idea, but I also don't think the status quo is going to remain tolerable indefinitely. Indeed, today we have a U.N. group of governmental experts that's been meeting periodically, trying to figure out what a code of conduct for cyberspace would look like, and what the norms of behavior should be.

And maybe Professor McNeal was right at the end of the last session in saying, "We have to wait for the digital Pearl Harbor. Regulation will never come until there's been the crisis." I hope that's not the case. There are instances where law has stepped in, whether it's regulating blinding weapons or dealing with various rules in the law of cyber. In these instances, the law has affirmatively stepped in to correct the problem before it reaches the crisis point. It's my hope that we can think about cyberthreats and the law's relation to them, and work through the regulatory options and try and find those that will be more effective than where we are today.

So thanks for your time, especially while you're eating your lunch. I'm happy to take any questions you might have.

QUESTION: Thanks for your great remarks. My question is about a lack of attribution. And so you mentioned that victims don't know, A, whether they're being attacked, and B, who they can expect an attack from. How would an e-SOS system work towards fixing that? If they can't prepare or don't know what to look for, how would they be able to put out that warning that, "Oh, we were attacked by this?" And then also, in that e-SOS system, does that provide other companies, then, the ability to

look for certain attacks, maybe even predict them?

DUNCAN HOLLIS: So it's not a perfect solution, but neither are any of the existing rules. But what I think it does is it turns - and this you probably owe something to Professor Michael Schmitt - it turns on the effects. If you as a company are suffering a particularly severe cyberthreat, and I think this has to be done - there has to be a floor for what allows you to send the call for help. It can't be that the home computer's down; it has to be at a certain level of crisis. But if you're suffering, if the system is down, if the power grid is not working in the Northeast, the idea of the SOS is you don't have to wait to figure out is it an attack, or is it our system not working? If you can't figure out what's going wrong, you can ask for help, right? And maybe in the course of helping you, people will say "Actually, you just were running these two systems you shouldn't be running together, it's your own fault, here's the fix," or they might say "It looks like you've got malware here, and it looks like it came from over there, or this is a particular variation on some malware we already know about, here's help getting the patch," right?

So the idea is help people deal with the harm that's being imposed, as opposed to the law enforcement or the international law model concentrates on finding out who did this and then holding them responsible. It's a different way of thinking about regulating the problem. It's like how do you regulate hurricanes? You don't stop hurricanes, right? You just try and minimize or mitigate the harm they can cause, and they can cause a lot of harm. And so I'm not saying that this will stop all harm, but to me it seems to be one of the few ways we can have the law work in the current environment.

QUESTION: Hi, thanks so much for coming today and for speaking with us. I really loved your analogy of using an SOS system, like the maritime system. But it just seems so hard for me to comprehend how that would apply in the e-SOS context. Because in the maritime system there, as you said, you can literally pinpoint who would be best located to lend their aid and effort and help the ship that's in trouble. So I am curious if you could explain how that would play out in the e-SOS context. How would the government, or whatever international organization, regulate and decide which computer user system should address the issue?

DUNCAN HOLLIS: Right. So I think - let me take the second part first, right? Process-wise, how do you get from an academic paper to a reality? So I think there's a variety of ways that you see norms translate into international legal rules. I'm a treaty lawyer; I love treaties. You know, I'd love to see a global treaty that has an e-SOS system. That's my favorite dream; I don't know that it's a reality. I think it's actually really practically difficult. I think you're more likely to see it be adopted in steps, right? So you could see a particular community; the Council of Europe or NATO. I've actually had some conversations with NATO representatives about what it might look like in the NATO context. Where you would have a particular community where that community agrees in advance on what the thresholds are; like what's to be protected, who can call for help, right? You designate here are the people who can hit the button, and what kind of assistance would have to be provided, as it were?

So it could be done on a regional level, whether through a treaty or even some soft law - I don't love the term "soft law" - or political commitments. It could be done on a more global level. I think one of the things I've argued about is where we're in a world where the Russians and the Chinese insist information weapons - Facebook, Twitter - have to be regulated alongside to get regulations on stopping massive cyber-espionage and the like. This is kind of a more low-hanging can't-we-all-get-along sort of solution. Can we just agree schools, hospitals, and certain, you know, water filtration plants and dams, for example, should be protected, right? Can we get a collected group of things to protect?

The harder question I think you hit on with the first part of what you were asking me is, well, how do we decide who provides the assistance, and what kind of assistance shall they provide? You could do it territorially, like "Hey, I'm in trouble." Boom, I hit the button, and then it's my government or somebody closest to me that provides the aid - we could do it on a territorial basis – some people down the road here are taking me to task for that idea. I think there are a lot of problems with that idea, because the nature of the Internet is not geographic space; it's not geographical.

So we could do something I call technological proximity, which is look at the technology that is most proximate to the harm, right? So if the malware is a directed denial of service attack and it's coming through one or more Internet service providers, maybe they're the ones who have to provide the assistance as opposed to some other Internet service provider elsewhere.

You could work on some sort of system of graduated response, where you start with certain assistance and if they're unable to provide you can move broader. I mean there are these CERTs, these Computer Emergency Response Teams that exist out there, and they kind of cooperate, but they do so informally; there's no requirement to cooperate. And so on things like Stuxnet or things like Estonia, they break down. Part of what I'm suggesting is once you bring the law into it, there are costs and benefits. But one of the things it does is it forces behavior that right now certain companies say "It's costly for me to cooperate; I'm not going to do it."

So I think the answer, in short, to your question is it needs to be worked out. Nation states would have to get together either in small groups or bigger groups and say "Where are the thresholds we want," and exactly how we're going to do it. Because just to say "Oh, we're going to have an e-SOS generally is too simple a solution in much the same way you don't just say "Oh, you know, we have any SOS in the high seas." There are certain protocols you're supposed to follow. So that's it.

QUESTION: So, for example, when the previous speaker was talking about how when he was working in the army located in South Korea and that virus rolled out and basically shut down their entire system for I don't know how many hours or that entire day, and when it's the case that it is the government, it is a state that is under attack, how would you suggest that? Like who would be the ones to step up and to address the issue and assist the state?

DUNCAN HOLLIS: So as I understood his story, I think you could think of a couple of different ways to hit - if you hit the button. You know, I don't know that taking down the e-mail is the kind of thing that I'm necessarily talking about. But for purposes of your hypothetical, let's assume it is. I mean the obvious thing would be where is it coming from? Is it coming through only U.S. networks, or did it cross through foreign networks… Where was the last stopping point, you know? Can you get South Korea, for example, their ISPs, to make sure the virus stops, have them stop and halt the e-mails?

So now you've contained the problem and now you've just got to clean out your systems that you have. And then presumably I think you said Microsoft Outlook, right? You're picking up the phone and you're calling Microsoft and saying "Your software has allowed this thing to happen, you know, get to work and fix it," right?

Now, Microsoft is going to say, "Well, that's going to cost us money." Now, they might have a business interest in doing it anyways, but the idea of the duty to assist is that you're now obligating them to fix their software. So when it's not Microsoft and it's somebody else who might say, "Yeah, yeah, yeah, we're not responsible for our patches, it's on you," there's going to be an obligation for them or the state which exercises control over them to step in and help out. Yup, thank you.

QUESTION: To what extent do you see the cybersecurity bill in the Senate this past session providing a domestic analog to your duty to assist with the information-sharing provisions?

DUNCAN HOLLIS: So I will caveat that my cyber-expertise is largely international. I follow - you know, Businessweek is much better than I am where things are on the domestic front. I mean I think the idea, as I understand it, and it's been very controversial, is we're going to require people to participate in a framework, right?

So the hostility to this bill rests on the mandatory nature of "you've got to participate". And so I don't know if that it's an analogy, right? Because what I'm proposing as an e-SOS system where the victims decide, you opt in, victims could decide "I'm under an attack, but you know what? I don't want anybody's help; I'll go down with the ship," or so what to speak, and that's possible. I used work at the State Department; if the Embassy's on fire, it's the ambassador's prerogative to let the Embassy burn rather than accept assistance.

The controversy in the cyber security bill comes from the fact that it is the government telling industry what they have to do and how they have to do it. The idea of an e-SOS is saying, "Look, let's clarify. If certain bad things happen, you can ask for help and other people have to help you," and in that sense it's a little more libertarian, right? It's a little bit more, hey, the law is only triggered by the victim as opposed to some government weighing in and telling you how you have to do it. Thank

PANEL 2: CYBER WARFARE PROGRAM - IS DOMESTIC LEGISLATION A SUFFICIENT TOOL TO BATTLE FOREIGN ATTACKS?

MELANIE TEPLINSKY: So we're all delighted to be here today. My name is Melanie Teplinsky and I'm an adjunct professor here at AU and I teach information privacy law. This is a really exciting time in cyber security. You can tell that from what you saw this morning. I want to take a few minutes to set the stage for this afternoon's panel discussion, but before I want to do that, just a couple words of thanks first to the administration and faculty and the staff of WCL for supporting this event, and second to the leadership of the AU International Law Brief and the National Security Brief for deciding to take on this complex issue and inviting me to moderate this afternoon's panel on the efficacy of domestic cyber security legislation. We have an extensive biography for each of our panelists; it's available in the materials, so I'll just briefly introduce to you each of our expert panelists. Michelle Richardson at the end, Catherine Lotrianti in the middle and Jamil Jeffer right next to me, all of whom have so generously agreed to share their knowledge, expertise and their time with us today. I will introduce you in the order in which they'll speak, so first Michelle Richardson.

WCL is proud to welcome Michelle Richardson back. She's an alumnus of American University Washington College of Law. While she was here she was a Mussey-Gillett fellow and a member of the AU Law Review. She's legislative counsel in the ACLU Washington Legislative Office. She works on national security and government transparency issues there, and she's worked tirelessly on the recent cyber security legislation. Prior to joining the ACLU, she served as counsel to the House Judiciary Committee specializing in national security and constitutional issues for John Conyers of Michigan, the ranking Democrat. Ms. Richardson is a fellow at Stanford Law School Center for Internet in Society and she holds a B.A. from the University of Colorado at Bolder.

Next to speak will be Jamil Jeffer. He is Senior Counsel for the House Permanent Select Committee on Intelligence, and in that capacity he has an insider's perspective particularly on CISPA, the controversial cyber security legislation that passed the House last April. Prior to joining that committee, Mr. Jeffer was an attorney at…in Washington, D.C. He served in the White House as an Associate Counsel to the President, and he has had a number of other influential legal positions at the United States Department of Justice. He is a graduate of UCLA and the University of Chicago Law School, and he holds a Master's degree from the U.S. Naval War College.

And finally Dr. Lotrianti [will speak]. She's a well-recognized cyber expert. She directs Georgetown University's Institute for Law Science and Global Security. She directs the Cyber Security Research

Project in partnership with Lawrence Livermore National Lab. She's also had a distinguished record of public service as counsel to President Bush's Foreign Intelligence Advisory Board, as Assistant General Counsel of the CIA, as Legal Counsel to the Senate Select Committee on Intelligence Inquiry Committee, and at the U.S. Department as well. She holds a Ph.D. from Georgetown and [J.D.] (ph) from NYU and a B.A. from the University of Massachusetts at Amherst. Please join me in warmly welcoming our panelists.

So a word about me. For those who don't know me, and many of you do in this room do, cyber has been my own professional passion for about two decades. As many of you know, I started my career at the National Security Agency as an Analyst back in 1991, just as the Agency was coming to grips with the post-Cold War world, and in the years since, I've been privileged to hold a number of positions both in government and the private sector working on international law and policy issues. … [I]n the Executive Office and a number of years in private practice at Steptoe Johnson. I'm currently on the Board for Proud Strike—we were just talking about this—it's a big data technology company that's focused on identifying and preventing damage from targeted cyber attacks. And it's in that capacity that I've had the opportunity to think very deeply about some of the most interesting and difficult cyber law and policies that are facing us as a nation today. So I'm thrilled to have been asked to moderate today's panel. I'm going to spend a couple of minutes just setting the stage for our discussion.

Technology offers us tremendous opportunities, but we all know [that] the digital infrastructure is vulnerable to cyber crime—cyber spying and cyber war, whether perpetrated by script kiddies or hactivists or criminals or nation states or terrorists. And policymakers have long been concerned with the security of the privately-owned systems and networks that support our nation's critical infrastructures, like our power grid, our telecommunications, our IT and our banking system. The U.S. has traditionally relied on market forces to secure the networks that support our nation's critical infrastructure, or C.I. Years ago, legislation that was designed to regulate the cyber security of the nation's critical infrastructure was considered a non-starter, but today the future of cyber self-regulation is uncertain as congressional law makers and the Administration are considering the possibility of requiring critical infrastructure providers to satisfy minimum baseline cyber security standards.

So why, after so many years is the issue coming to a head now? It's because as a society we've come to understand that the cyber threat is, in the words of President Obama, one of the most serious economic and national security threats that we face as a nation. Cyber war. Well, we understand that the weaponization of cyber and the threat of cyber war have had significant implications for our national security. You've heard this all morning with the references to Stuxnet, to Saudi Aramco, the state-owned oil company that was the target of one of the most destructive attacks on the private sector that we've ever seen, involving destruction of 30,000 computers and the critical files that were on them. And in addition to the weaponization of cyber, which poses a threat to national security, there is cyber espionage, which poses a great threat to our economic security. The loss of industrial

information and IP through espionage is considered the greatest transfer of wealth in history, according to Keith Alexander, who as referenced earlier is the dual head and director of both the NSA and also the head of the U.S. Cyber Command. U.S. companies lose an estimated $250 billion a year to IP theft [and]$114 billion from cyber crime. A trillion dollars was spent in 2011 on remediation from both cyber espionage and cyber crime.

So the question that's facing our panel today is how should Congress respond to the new realities of cyber espionage and cyber war? As we think about that question I'd like to turn the program over to our first panelist.

MICHELLE RICHARDSON: Thank you very much, I'm very happy to be here. This is definitely one of the hottest issues right now in D.C. and it's very likely that there will be significant movement just in the next six weeks, at least on the domestic front and legal authorities, so this is a perfect time to be speaking about this. Now, the ACLU does recognize that cyber security is a problem and that government action is necessary. The difficult question though is: what should the government be doing? The devil is always in the details when you talk about these programs. There are a lot of cyber security programs represented in different bills already undertaken by different agencies that actually have nothing to do with privacy, and the ACLU would like the government to focus on those efforts. For example, the government itself will tell you that 85 percent of cyber security problems are hygiene issues, where people are not taking basic steps to protect their own systems or their own information. And information has come out over the last few years that major system controls are not even changing the passwords from 12345. These are really basic sorts of things, and 85 percent of cyber security problems could be fixed if these things were addressed. You also have the regulation of critical infrastructure, securing the supply chain, amending the government's authorities to control its own systems under the law called FISMA, money towards research and development, workforce training, and education of the public. Some of these things are already underway and it's possible that legislation could expand all of these efforts. The issue that the ACLU is tracking, though, is information sharing, which the Administration and the Hill all agree is one of the most important things that can be addressed legislatively or through Executive Order to make sure that more information is shared. The idea is that [the] current privacy laws prevent companies who are sitting on top of cyber data to share information with each other or with the government so that everyone can defend themselves better. The problem is that this has really not been defined. There hasn't been a good explanation about why current laws are blocking the sharing of this information. There have been no congressional hearings where members of let's say the telecommunications committee have come up and explained why the current law is insufficient and [what] changes that they would like to see. And people have been proceeding with the broadest approach possible. They have written legislation that says, notwithstanding any provision of law, entities can share cyber information. Most obviously this would be an exemption to [ECBA] (ph) and FISA, because mostly you're going to want the Internet data from the people who are actually trafficking in Internet. But that also means that it's an exception to HIPAA, and to the financial banking laws, and IRS

regulations on tax information, you know, gun records, anything you could possibly think of. It's an exemption to all privacy laws on the books anywhere, and so it allows, for cyber security purposes, information to be shared that could be incredibly sensitive. Even if you are looking at the information that is directly related to the Internet and communications, it's still sensitive. It's not that anyone has done anything illegal. You know, in your Internet life you have information about your financial situation, what you read, where you're a member, what you eat, what your health problems [are], and these are things that we all have a right to privacy in.

So the legislation has evolved to create an exemption to all privacy laws to allow entities to share information. The questions then become: who can it be shared with, what can be shared, and then what can be done with it? And these are very important questions and the legislation right now cannot be more different between the House and the Senate. As for who it should be shared with, it must go to civilian agencies if it is going to be shared directly with the government. These changes are necessary to deal with American information on U.S. soil, so that means it needs to go into [civilian agencies–] it could be DHS, it could be [INDIST] (ph), it could be any number of different agencies, but it should never go directly to the Department of Defense, especially the NSA.

As for what can be shared, it's important to write statutory limits that require companies and people who hold this various sensitive information to take efforts to minimize out content or personally-identifiable information that is not necessary to describe the cyber security threat. We do not want this to become a fire hose of information where companies just turn over more information because they don't want to go through the process of sorting it. And that's a facs-specific analysis we recognize, and sometimes PII, for example, may be involved in what is turned over. But a lot of times it doesn't have to be. You'll hear the Administration talk about how a lot of the information that they want is just a fact of notification. A fact [that] a certain IP address [is] active or the existence of a certain worm or other threats coming across their networks, and that's the type of information that we think is okay to share. But sadly that is not where the legislation has headed.

Finally, the use of the information. Since this is a backdoor through all privacy statutes and the Fourth Amendment, it is absolutely crucial that the information is only used for cyber security purposes. It's possible that the information that's turned over may reflect criminal activity or other things that are wholly unrelated to the cyber security effort, and we do not want this to be a way for the government to enforce immigration [laws] or prosecute minor unrelated crimes, and that this information, its dissemination and its use, needs to be targeted just in the cyber column.

Now, the two major competing bills now are CISPA, the House bill, and the Cyber Security Act, which is the Lieberman-Collins [bill] in the Senate. They've both gone under significant amendments over the last year but they ended up in completely different places. The Lieberman bill in the Senate is far superior as far as privacy is concerned. As far as who can receive the information, [it] [clarifies] that if the information goes to the government it has to go to a civilian agency. As for what can be

shared, that Lieberman bill says that only information that's necessary to identify the threat can be shared, and that the entities who are sharing it need to make reasonable efforts to protect PII. And it clarifies that the information can only be used for cyber security, not for unrelated and undefined national security purposes.

On the opposite side you have CISPA, which does allow the information to go the NSA or the DoD or the FBI. It allows the companies to decide what will be shared and doesn't put any onus on them to protect personal information, and it allows the information to be used for a number of different purposes, including an undefined national security purpose. And we know over the last ten years that definition is always growing broader and broader. And in fact CISPA did get a veto threat from the Administration, in part for the threat to privacy. And that's just so significant. This Administration has asked for the PATRIOT Act and the FISA Amendments Act and other laws to be reauthorized without amendment, so for them to say now this is a bridge too far is really significant.

So the question then is how this will be resolved. It seems as though [Majority Leader Reid] (ph) is dead serious when he says he's going to bring a bill back to the Senate and they're going to have another vote. It's not clear what that bill will look like, but there are a couple of hurdles they'll have to address, most importantly being what to do about Title 1 of that bill, which is the regulation of critical infrastructure. They could amend it further; they could take it out. It's not really clear where they're going to go on that, and it seems as though there was a hiatus in negotiations with the elections and the members being out of town, and so it sounds like that will pick up starting next week. You will have to see a resolution between the House and the Senate, even if you were, let's say, to break out information sharing as a separate issue. Because in the Senate bill you have something like nine or ten different titles addressing a whole sort of different issues on cyber security. Even if information sharing were to be broken out and moved separately, the bills could not be any more different. And I think the number one issue you're going to see to prevent some sort of compromise is the question of who's going to receive [information] and whether entities will be allowed to go directly to the NSA or whether the legislation will direct them to stay within the domestic sphere.

The last point I'll add is that we do fully expect that an Executive Order is coming and that it's near completion and will be out some time before the end of the year, by our best guess. That has now been leaked on the Internet. It's on the Lawfare blog I believe. So if you want to take a look at that [, feel free]. [The Executive Order] deals more with the regulatory issues than it does [with] information sharing. There is a small information sharing section that is privacy neutral, and we're very happy that it doesn't seem to have a significant negative impact on privacy. And what it does is increase information sharing in the opposite direction. Because the other half of the equation is what the government [will] share with companies. So they are taking steps to make it easier to get a clearance so that there will be someone at these companies able to even receive the information. You know, they're directing them to make more of the information unclassified in the first place so it can be distributed further, maybe even made public, and internally start the processes for information

sharing and setting up regulations, because right now it's happening quite piecemeal.

So the ACLU will continue to be involved with this. We certainly prefer the Senate bill over the House bill; we think it actually has pretty substantial privacy protections and we're happy with how it turned out, and so we'll be doing what we can to support that legislation in the coming weeks.

MELANIE TEPLINSKY: And with that let's turn to Jamil Jaffer who ….

JAMIL JAFFER: So maybe a little bit of background on sort of how we were in the Cyber Intelligence Sharing and Protection Act. So when I arrived at the Committee in May of 2011, Chairman Mike Rogers, along with many other chairmen in the House, was looking at the question of how [to] deal with cyber security. What can the government usefully do to help the private sector better protect itself? One thing that came through off the table right at the outset was: this isn't going to be the government going into private systems to defend the private sector. Rather, this is a question of can the government do anything useful to help the private sector protect itself better. And so we were looking at at our committee, the House Intelligence Committee was looking at it from the perspective of what can the intelligence community do to help the private sector better defend itself. And we didn't go in looking at it with, you know, there's going to be something there. We could have come back with there's nothing useful the intelligence community can do today. And what we found was when we talked to the intelligence community, what they told us was, look, we have a tremendous amount of information about the current threat to the government. Right? We monitor our own systems to protect ourselves, and we conduct espionage against foreign nations to collect information, both about their plans and intentions and about the threat they may pose to us. So we know a lot about what foreign nation- state actors might do to us, and we know a lot about what we're seeing against our systems both from a nation-state perspective as well [from] as other attackers. And they said, look, what would be really useful is if we could find a way to share what we know with the private sector. Today there's no mechanism in the law that permits the government to share both classified [and unclassified information]—largely classified, not really unclassified, because that happens at some level—but to share information directly to the private sector to help them better defend their own systems. So it would be helpful for us to have the ability to grant security clearances to the private sector outside of the sort of normal government contracting process, and then share at a very highly classified level some of this information, but [do so] in a way that is actionable and useable to defend unclassified private sector systems.

So that was number one. So we heard that from the government side. From the private sector we heard, you know, it would be really great to get that information. We know the government has some information. We don't know how valuable it is yet. We're skeptical; it may not be that valuable, because it's really about the threat to the government. We know that threat might be different than what we're seeing in our systems, but we'd love to get that information, at least [to] start learning from that and start protecting our own systems.

Second, we heard from the private sector: we have a real challenge sharing with other partners in the private sector. So we can't share with our colleagues in the private sector because we're concerned with the information antitrust laws. So, for example, if ATT and Verizon and Comcast want to sit in a room and have a joint net operations center their lawyers tell them, look that's going to be a real challenge for you because you might have to invite everybody else, every other potentially large or small telecommunication provider, for fear that the government might come after you for antitrust violations or you might be sued in a private lawsuit. So those laws present a challenge. Whether that challenge is real or perceived it's hard to say, but it's one that certainly companies feel. And [they] feel that they can't share the information effectively, and their lawyers are saying no. Don't get in a room and share that information, because it's going to be too hard for you to get out of the potential lawsuits you might face.

In addition, the private sector said, look, we'd really like to tell the government at times about the threats we're seeing on our systems and be able to get their insight and their assistance in protecting our own systems. And on a one-off basis they say, look, we can sometimes get clearance from our … counsel when the threat's really bad or there's been a really big IP theft; we can go to the government and say, hey, we need help, and we're not so worried about the [legal risk]—even though we're worried about the legal risk, we're willing to take that risk because the threat's so dangerous to us. But by and large we'd like to be able to do this on a regular basis. So the government said: well, what do you guys think about that? Would you be able to help the private sector better if the private sector were able to share its information with you? And what they said was, actually this is very interesting. So today we send people, both human spies and all the mechanisms of surveillance, to figure out what the foreign nations are doing to us. If we knew better what the threat to the American private sector was, we could use our methodologies, whether it's human spies or other, to collect information from those actors and pass that back in this classified mechanism to the private sector to better defend itself. So on Day 1 we're going to do this information sharing thing. You know, the protection might not be that great because the government's just providing what it sees on its own systems. But on [Day] 365 if there's robust information sharing from the private sector to the government, and then back from the government to the private sector, you'll have a much more improved picture for the private sector about what the threat is, particularly from high-end nation state actors.

Now, it's certainly true that information sharing doesn't solve the cyber security problem. In fact it doesn't take you a long way. As Michelle pointed out, 85 percent of the problem might be solvable, some have argued, by better hygiene. But from the intelligence community's perspective, from the Intelligence Committee's perspective, our goal is not to protect against the vast majority of cyber threats, our [goal] was to protect against the high-end really problematic cyber threat, which is the threat of sort of [a] major catastrophic attack by a nation-state actor that could take down large-scale systems and/or just [a] high-end IP theft fomented by nation-state actors. And so today it's no secret that the Chinese government is stealing terabytes of highly sensitive IP information from

the U.S. private sector. The heart of the American economy is literally going out the backdoor. And my boss likes to say—Chairman Mike Rogers likes to say—that there are two kinds of companies left in the American economy today, companies that have been hit and know it and had their IP taken and those who don't [know it]. Everyone's been hit. And now, with the now recently disclosed attacks on Saudi Aramco and Qatari RasGas, you can actually see what appear to be potentially nation-state actors going after these systems and taking them down, and then along the same time schedule a sustained DDoS attack against the U.S. financial sector. These are very worrisome things. We're finally seeing a real no-kidding threat that goes beyond just IP theft. So forget the billions of dollars that were walking out the backdoor, now we're talking about real potential takedowns or attempted takedowns of government systems, potentially by nation-state actors. And so there's significant pressure on the government to do something, and I think that no matter where you sit, whether you're in the Legislative branch, the Executive branch, the House, the Senate, Democrat, Republican, everyone agrees that you can at least move the ball forward by sharing information from the government to the private sector, the private sector to the government, and private to private. Every bill, including the Administration's legislative proposal and the ones that are in the House and Senate, all share some aspects of that. And they're different. But truth be told, actually I don't think I agree with Michelle that they're that different. In fact, I firmly believe that as between the House and Senate, the two Senate bills, there's a Republican Senate alternative called the Secure IT Act, there's the a Democratic alternative, some say a bipartisan alternative, the Lieberman-Collins bill, the Cyber Security Act of 2012, and in the House there's the bipartisan Roger Ruppersberger bill that passed the House by a substantial bipartisan margin—even in the face of a veto threat it got substantial bipartisan support in the House—called the Cyber Intelligence Sharing and Protection Act [CISPA]. And so the real question is: can the House and Senate find some middle ground on information sharing, and I think the answer is yes. I think there's substantial common attitudinals. There are important distinctions, but they're ones that I don't think are ones you can't get past. The real thing that's holding up the bill in Senate right now is the insistence on some need to take up a regulatory provision that would regulate critical infrastructure, and that's what caused the Cyber Security Act of 2012 to go down on a [cloture] (ph) vote during the last session. It's, I think, what's likely to hold up the Cyber Security Act if it's brought back in its current form during the lame duck session. If those provisions were stripped out it's a much more interesting question. If in fact the House and Senate can find a middle ground on information sharing, I think it's very possible in the lame duck session [that] you can see a bill going to the President's desk for signature. That's not to say there aren't challenges here, that there aren't hard questions, but I firmly believe that the bills aren't that far apart and that there is a middle ground to be had on the issues of private-to-government, government-to-private and private-to-private sharing, and liability protection and minimization, and all those hard questions. And so I think that we've been engaged over the long run since Day 1 of this in discussions with the ACLU, with CDT, with EFF, as well as with the business community, as well as between the House and the Senate. And those discussions continue to this day. I think we're very hopeful that, particularly given the now publically disclosed rising threat to the U.S. private sector, both of economic theft and no-kidding real takedown attacks, that we're at a point where we

can find a partisan, bicameral consensus on these issues and move the ball forward. To be sure, an information sharing bill won't address everything, but it moves the ball significantly forward in a way that I think we believe can better protect the nation without the government being directly involved in defending the private sector.

MELANIE TEPLINSKY: Thanks, Jamil. And we'll turn next to Catherine Lotrianti.

CATHERINE LOTRIANTI: Thank you for inviting me here today to talk to you about this topic, which [a serious topic], clearly from all the speakers here and probably from you because you came here today, you recognize how serious of a topic it is, and … a lot of people to look at the issues. I'm going to bridge the two topics from today. The first panel, if you were here for it, focused on the international aspect of cyber security, what legal regimes are effective—or not effective in some of the discussions—in dealing with cyber security, and [I want to] connect it with the discussion on the domestic legislation side of things. So as the question [that] was posed to us for this panel asked a very specific first question about whether the domestic legislation could be effective in battling the cyber threats, particularly against critical infrastructure. So I'm starting from there and we'll start with kind of a discussion of what domestically can the U.S. do, and then I'll move into the international aspect.

So from a domestic perspective, you can kind of divide the areas, as the legislation has, into two spaces: one, the securing of critical infrastructure, and [two,] the sharing of information, which could seek to enhance our protections broadly, even more broadly than just the critical infrastructure. I'm going to give you specific examples of what the U.S. has done in both of those categories and really how the laws, since we're discussing the laws, both domestically are affected by it and can have an affect upon it, and yet ultimately my bottom line is [that] the concern and threat from cyber security for the U.S. is not solvable only through U.S. legislation. This is truly a global issue, because of the nature of the system itself, the Internet and connectivity. You have to look domestically first, but what is ongoing—you heard some from the first panel, I'll talk a little more about that—we also have to connect that to the international. That means working with other nation-states. And that's why we have two panels, one talking about international law and one on domestic.

So on the security side of securing the critical infrastructure, the debate, as pointed out very clearly was: there is on the legislation [front,] a disagreement among the camps about how much the United States government should be involved in the business of the private sector. All the critical infrastructures are owned and operated by the private sector. As you've probably read many times, I think the percentage of the entire Internet is 80 percent—maybe that number's changed but last time I was reading it—owned and operated by [the private sector]. So clearly it's an issue of government interacting and regulating the private sector. It's a long-time debate on other issues, not cyber necessarily, in the United States, right? We have this divide where we have very strong companies that feel strongly that less government is better, better for the U.S.'s innovation, economy, profitability, [and

is] certainly better for these companies, they believe. All of the critical infrastructures that opposed any kind of regulation have articulated the current compliance process and regulatory regimes that already exist over them, all of these sectors are regulated in some fashion already, and they have already pointed out very clearly how costly that is in and of itself. And they have argued, sometimes convincingly, that the compliance and audit system is maybe not even effective. Costly, yes, but [it] might not even get to the core issues of security.

So we're talking about certain sectors, so let's specifically identify. The one most discussed is the financial sector. One, because it's probably the most advanced in taking it upon itself to put the dollars necessary to protect its networks, not shockingly because there's real dollars involved. But there [are] also other sectors which are important, [such as]the nuclear plant operators. The nuclear sector is very important. If we have a leak from a nuclear power plant, that is very detrimental to the U.S. population, and possibly other states as well. So that sector is one, but there are a number of them. I just mention one or two, but there's the power grid, there's the gas and oil facilities and pipelines, [and] there's the water supply. DHS lists eighteen. You know, not to offend any of them, but there are some of those eighteen that are more important and therefore that's typically why they're ranked. Not to offend people ranked at the bottom, but they are already identified. They've been identified because if something were to happen to any of these sectors, if they were unable to function [or] protect their systems, [or if they were to] lose data, it would have a very significant negative effect against the U.S. national security, [and] basically the social operation, the civil society of our country. So protecting those systems is important. The question which has been battling out on the Hill is that the private sector believes for the most part [that] it can protect [its] systems on its own effectively and it does not want the government in its business. The compromise in both of the drafts, both House and Senate, it wasn't as—one was a little more heavy-handed in the government side of things getting involved, but both the last versions that were out basically said [that] we the government will not tell you what type of technology you must use to protect yourself, but we will mandate and require you to be secure to a certain level. How you get there is up to your—and then the government often, the people in the Executive branch particularly, they know that there's great knowledge and capability in the private sector, and often if we get them alone and not in public, [they will] readily admit that there is probably more capability technically in the private [sector] than in the government. But irrespective, the law–[or the proposed legislation]– was a compromise about how to have the security of these systems up to a certain level but not have the government getting in their business of dictating which technologies, which vendors and how they were going to do it. I'm not sure why this couldn't be worked out. [T]here wasn't much difference between the legislation on this particular issue. Both versions had backed off some early—I mean a couple of years ago—discussions of the United States government actually mandating certain standards. This was we will work with you. I think it was basically a fear of, well, yes the U.S. government says they'll work with us, it is NSA and DHS, and what they're really going to do is take over our systems. That's a lack of trust in the government. I'm hoping that that can be worked out. These private sectors I asked, the financial sectors, I was at a forum with them a couple weeks ago, the banks, [and] I asked: in your worst case

scenario, worst case for you guys, what would the Hill do? Right? All these versions, what's the worse thing? They said: if they do anything it's the worst case scenario. Like anything. So they want nothing to change. Nothing. So we'll see what comes out of an Executive Order or the legislation.

So some of the things other than—and sharing of information, as we've heard from. [Information sharing is] clearly important to increasing the knowledge of the threat, our vulnerabilities, [and] how to fix that and how to defend ourselves. So some of the things that I wanted [included] the security of the systems and the sharing of information. There's also technical, there are other technical things we could do and mandate by domestic legislation. For instance, the earlier panel talked about identifying targets and distinguishing targets. That's a technical fix; that's we can change the domain name system, the DNS, and create a new top level domain name. And the East West Institute wrote a paper, as I think Chuck mentioned, that you could technically change the names where you could have hospitals that are identifiable. That is, in another way, protecting and securing some of our systems, [and is mostly being discussed] in [the context of] a time of conflict. Domestically, we could also look at what has not been [done, such as]concepts of self-defense for companies. We were talking just before the panel about private companies acting in their own self-defense to protect their networks, their information, and [their] data. [W]e don't have clear legislation on the books allowing them [to take these actions], but domestic legislation could go there. Right now, although it's being discussed, it's not at the front and center of legislation discussions. Maybe it will be once we get through the sharing of information and critical infrastructure regulation.

Agency authorities. Domestic law can do a lot in terms of creating new government agencies in cyber space with the authority to protect, and it has done [that]. [We] created DHS with the mandate to protect the .gov. We created Cyber Command with the mandate to protect the .mil. Now, there's a lot more discussion that needs to be going on as to, well, who really has the lead to protect the .com, and that really is the bigger part of the story. But domestic legislation has operated in that space, given authorities to agencies, and could do more.

Other areas. Amendments to laws. Michelle mentioned a couple, but I remember when they were first proposing the language within the cyber legislation, "notwithstanding any other statutes," I had a flashback back to when I was working in the General Counsel of the CIA. CIA's legislation has that language in it. It is very unusual in U.S. domestic legislation, highly unusual, very controversial. Because what you're saying is, we the lawmakers are going to take the easy road out here. It is so very difficult—and it is—to go through all of the pieces of legislation and make amendments. And so I was working at the time with Melissa Hathaway; we had been asked by DoD Cyber Policy to come up with a list of laws. So her not being a lawyer, me being a lawyer, us working together previously, we got together and we had over twenty different statutes that would have had to be amended in some way or another to get the authorities that the government [wanted in order] to take certain actions domestically in the cyber domain. ECBA, the Computer Fraud and Abuse Act, probably the top FISA. That would be a very difficult political challenge for anyone to start going down that list

one by one and seeking those amendments. So [to take the] easy road out, one way is to put that provision, "not withholding any other statutes." So based upon my knowledge of how difficult it was to get that in the CIA's legislation years ago, and how unusual it is, I anticipated that to get that through Congress would be very challenging. There would be many people from the outside [who didn't it want it], [for] privacy reasons; [there are] a lot of reasons why you would not want that.

How to work that out, though? My view is that you seek to amend those statutes. But we could do that in a number of ways. [With] the Economic Espionage Act, another statute that was on that list that we had, you can amend it [so] it becomes a stronger weapon to be used to protect cyber security. The concern is always with strengthening your government to protect us in national security areas. You don't want to give [it] too much authority, where you're then drawing down on and imposing constraints on freedoms. That is always, in making the law, what you need to contend with, and it [especially] comes up in privacy discussions. So domestic legislation, is it sufficient to battle foreign attacks? So I say not enough, but there are areas which are useful.

Some of the examples of securing the systems from attack. So we do have the discussion ongoing now on regulating the critical infrastructure. Under the Bush and continued through [the] Obama Administration, we had the CNCI, the Comprehensive Cyber Security Initiative. The goals, fifteen, sixteen different elements of that [initiative], were to do just that, to work with government agencies in securing our networks. The Cyber Command I mentioned, the creation of DHS. There was also the DIB program. That goes to the heart of information sharing: government to private, run out of DoD. They went to their defense contractors, those corporate entities that do a lot of business with the military, and they said, listen, [on a] voluntary basis, let's figure out how we share information, so we protect that information that you all have but is important for DoD and that's why we actually have contracts with you. That program has been a very effective program. There are limits to that program, though. The scalability of that to reach beyond the defense-industrial base is limited. It took, I don't know, close to eight or nine months for the lawyers to work out all the legal issues just for those companies that were in that small group of voluntary partners. But that is an information-sharing model. And I think [that] supply-chain issues are a big issue. [So is] ISP regulation. These are things the U.S. government [and]Congress can regulate on to improve. With SEC mandatory reporting rules, they did create a new rule. And when a company that's publically traded has a breach it now has to, by the SEC new rules, report that. That's important. If there's no reporting, or not enough reporting, the government doesn't know the extent of the threat.

The nuclear regulatory agencies, as I mentioned those plants, it's important also to secure their systems. And the IAEA, on an international scale–I've been working with them–[is] getting involved not just because the U.S. has these plants, [but] because there are a number of states with nuclear plants and their cyber security is critically important.

I'll speed up because I want to get to the international authorities to take action. So we did talk

about Cyber Command, but that's in [terms of] defensive and offensive [actions]. You can authorize the agencies to do certain things to protect, and the phrases like "active defense" have been talked about, and [that] includes offensive action. [One option is] allowing companies to do takedowns, right? [Allowing companies to] not just [use] criminal processes but to actually do the takedowns even before the attack occurs in real time.

As Duncan mentioned the criminalization [is another component of cyber defense]. Having criminal laws is very good and very impactful in many ways. It allows for a transnational jurisdictional investigation. It takes a lot of time. It might not be the only solution. It allows for some pretty good [prosecutions]—we've had some pretty good DoJ prosecutions recently. You can take down some organized crime organizations this way by having criminal laws in our country as a signatory to the Cyber Crime Convention. Of course policy statements also [play a role]. [This is] not real hard law, but the U.S., although some may disagree with whether we should do this, the U.S. has come out and stated, we will abide by the laws of war in cyber. So the policy statements in and of themselves, although not statutes, are also powerful, and to the extent that you believe compliance with those laws will create a more stable and secure cyber environment for both us domestically and internationally, [a good thing].

This is not enough, though. My main take is [that] just looking inside our borders is insufficient.] Because of] the nature and characteristic of the network itself, the efforts to protect that global network [are beneficial], as long as we [do not] balkanize our own Internet. Some have projected—Zitran (ph) at Harvard says let's all get over it, it's going to happen. Let's not shed too many tears, balkanization will happen. Most people in the U.S., analyzing the U.S. economy, assess that if [balkanization] does happen it is not going to be favorable for the U.S. economy. If we do cut off ourselves voluntarily, which I don't think we ever would, but if other states did it–cut us off–it would not be good and advantageous, so let's think about international actions tied to our domestic legal actions that could help on the cyber security issue. So international engagement and agreement. Shy of a treaty, which many predict may not be able to happen any time soon– I jump into that camp of finding it not very probable that a multinational treaty will take place like an arms control treaty–there are other aspects. So, for instance, take up economic espionage. You've got the one trillion dollars of IP theft causing a one trillion dollar loss to the U.S. What can we do about it? Well, you know, you have NCIX, who has officially called out China in the first U.S. government report saying it's China, but not only China. So we don't have to like talk about it secretly anymore. So China is stealing us blind in IP theft; what can we do about it? Internationally we have options. Amend our own domestic legislation, but use the WTO, and use other nation states to start calling them out.

Collective defense: we've heard about NATO as an organization. The principles under collective self-defense in international law need to be worked out with other states. Global networks, the issues of traffic. Duncan talked about a really interesting idea over lunch– hopefully you guys all heard it–about the e-SOS. It's very fascinating. And related to it, one of the areas that will be of great poten-

tial for dealing with protecting these global networks is looking to the ISPs. And not looking to them to mandate. Some have said, let's mandate the ISPs, let's put a duty of responsibility on them to do X, Y and Z. But I'm talking about an international consortium, on a voluntary basis. These companies are the ones that have a lot of power and a lot of equities because they own or they operate on these platforms.

MELANIE TEPLINSKY: I'm going to ask you to wrap it up.

CATHERINE LOTRIANTI: Okay. So we can go on about the international kind of ramifications, but kind of my main point is there's a lot we can do domestically. We'll sort out the disagreements on the Hill hopefully, [and] between the parties we'll get some progress. But that can't be where the story or the discussion stops. That's why we have the international folks, and that's why you connect[ed] the two ideas [in two great panels].

MELANIE TEPLINSKY: So let's start. There are a lot of ideas here, everybody can see that, and there's a lot of room for debate. What I'd like to do is take a few different items at a time and walk through them. Let's start with information sharing, since that's one of the main things on the table and it's one of the things that you've said might be able land on the President's desk in the form of a bill from Congress. My question here is, from the private sector perspective you often hear some concerns about information sharing. You hear concerns that if information is shared with the government, there might be leaks about the fact that a private company has been attacked. You hear concerns that if you share a private company's information with the government, that's great because the government can use the information but that the government doesn't necessarily provide any assistance. So we talked this morning about how the U.S. financial sector had the largest DDOS attack a few months ago, and in response the government didn't do anything, and the reason was not that that it wasn't a cyber attack necessarily, but there was no loss of life. And the government has really drawn the line there: where there isn't serious destruction to property or loss of life, there isn't going to be government action on behalf of the private sector. So the question here is, what is the benefit of information sharing, and what should the information sharing regime look like to address some of these concerns? Sure, it's open to all three.

JAMIL JAFFER: So I think from the perspective of the House, our view is, look, the private sector should do its own network defense. The government shouldn't be in the business of getting on private sector networks and putting up sort of a border fence around the nation. Rather, the private sector has every incentive to set up its own systems, because fundamentally its businesses depend on functioning computer systems and they're going to lose a lot of money if their computer systems go down. They're going to lose a lot of money in research and development dollars if their IP continues to be stolen out from under them. And our view was, look, if you can share the information about what the threat is they can (a) better defend themselves, and (b) make better economic decisions about how much to invest in cyber security. So today a lot of people say, look, there's a market

failure in cyber security; companies don't do enough to protect themselves. But the truth is it's not a market failure if there's not full information in the market. And we know today [that] the private sector doesn't know enough about what the threat to its systems are because it doesn't know the classified information that the government knows about what nation- state high-end actors are doing to private sector systems. They know at an abstract level that there's this threat going on, but they don't see what the government sees; they don't see quite how bad it is. I think that if we were able to share that information with the private sector they'd make better economic decisions and be able to better defend themselves. On the other end, [from the] private sector back to the government, part of our notion there was—and when we talked to the private sector and the government about this, what we realized was the government has a real capable system of obtaining information about what foreign nation-states are doing. When you're talking about human spies or other methodologies, the government's really good at getting that sort of information. The private sector simply doesn't have that capability. If you could give the private sector information from that mechanism and allow them to use that information and allow the government to be informed by what—so take the following example. You have Chinese adversaries going up against the United States government. You also have Chinese adversaries going up against the U.S. private sector. They may be in the same room, but they're two different sets of attacks, two different actors. The government sees the one going up against it; they don't see the other one. If the private sector were able to share information–we see this kind of thing happening to us, whether it's a technique, a tactical procedure or a specific IP address–the government could use its methodologies to find out about that person and provide information about that person or that methodology or whatever it is back to the private sector to better defend itself. So you allow the private sector to leverage the government's capabilities, not to have the government defend the private sector, but to allow the private sector to defend itself with the government's capabilities. And [that] was sort of the notion behind our bill, and frankly it's the notion that underlies the information sharing provisions of all the other bills out there, and that's why I think there's a lot of commonality between these bills. And there are important differences about how much and what and to whom and what liability protection you get, but these are differences that fundamentally aren't at the heart of the discussion. The heart of the discussion everyone agrees [on], right? If the information were better shared between the government and the private sector and private to private, the country's going to be better protected on its own.

MICHELLE RICHARDSON: It's not really clear if this will work, because there really isn't meaningful open information about how the law is actually preventing information sharing in the first place. And [as] I think Jamil said earlier, it's not clear if the law is really preventing information sharing or whether that is just perceived– the difference between real and perceived. The problem is you're writing a bill that is going to undo a half a century of privacy laws. You are going to revoke, as one DHS person estimated, over a hundred different statutes and allow corporations to decide what information about us and our Internet and communication habits can be given to the government. That is an astounding response for what could possibly be [only] a perceived problem

MELANIE TEPLINSKY: So let me just take one second and read the language of this so that everybody who's in the room can be on the same page. The provision we're talking about is the CISPO provision that says, "Notwithstanding any other provision of law companies may share information with any other entity including the Federal government." Is that the right?

JAMIL JAFFER: So there's actually—so it actually says "may share cyber threat information." And "cyber threat information" is a defined term in the bill that includes information directly related to a threat to a network or system. That was the original draft. That definition actually changed over time after we sat down with CDT [Center for Democracy and Technology] principally in the Constitution Project, and we worked [out] language that they were much more comfortable with that significantly narrowed the scope of information that could be shared pursuant to that "notwithstanding provisional law" provision. So the notion somehow that [a company] could take your gun records and share it with the government, I mean, that's just a red herring, right. I mean, we're all lawyers; you look at the law, the law's definition is in it. The definitions constrain what [can] be done, what the content—what the scope of the information is. Moreover, the bill provides that you can only share [information] for a cyber-security purpose, also a defined term, defined by the same notion of a threat to a network or system. And again, [that definition was] narrowed down by language that the Center for Democracy and Technology and the Constitution Project [agreed with]. I should note, by the way, the Administration's veto threat was directed at a bill that was not the operative bill in the House, or the bill that came out of committee, not the bill that was the negotiated version with CDT and the Constitution Project. So the notion somehow this is about gun records or tax records or [that] the private sector could just dump everything they have on the government, I mean that's just not reality. And Michelle and I actually had this conversation months and months back when we first came out with our bill. Michelle said hey, you know what? We're going to call your bill the biggest cyber spying bill in the history of the country. And I said: Michelle, you can go do that, but it's going to be wrong, and you're going to get laughed out of the room, and the truth of the matter is they made that effort. Right, EFS, CDT, ACLU [all] had a joint effort, "Stop Cyber Spying Week," and the bill passed the House floor by a substantial bipartisan margin. It just didn't catch because it's just not true.

MELANIE TEPLINSKY: So Michelle, let me ask you, are privacy and cyber security a zero sum game?

MICHELLE RICHARDSON: Absolutely not, absolutely not. There are ways to do information sharing that have protections built into it. And as our privacy laws have developed over the last half-century it has been very thoughtful. I mean, a lot of work has [gone] into developing ECBA and FISA and every little protection for records and content. And to do away with all of them and not build something in [their] place is a privacy disaster. Now, CTD and Constitution Project opposed CISPA, even with all the amendments. And in fact the entire advocacy community opposed CISPA. The Senate opposes it, the Administration issued a veto threat; there is not a huge amount

of disagreement. And there were 168 no votes in the House on that bill. So I think you're creating a solution where it's not even clear that that's a problem. People in the Administration will tell you that information sharing is already going on to some extent, and some companies choose not to [participate in that information sharing]. And there are other motivating factors here besides the privacy laws. Some [companies] just don't want to start this process with the government because they're afraid it will come back and result in the government mucking around in their systems, or asking for more information or causing other problems. Some are not going to want to share information with their competitors. If they get a leg up with better security or things like that what really do they want to give it to their competitors for? And these are things that cannot be addressed with changing the privacy laws.

JAMIL JAFFER: So there is a—I mean, I've never quite seen a consensus behind the bill that we saw with CISPA. Every major industry group, from the financial industry, telecommunications, the U.S. Chamber of Commerce, Facebook, Microsoft, Intel, IBM, AT&T, Verizon, Tech America [all supported CISPA]. I mean, you name it—and you can go on the website and look at all the letters of support. And I'm talking about complete [support]; the best thing that could happen to help the private sector protect itself is for the government to share information with the private sector and for the private sector to be authorized to share information with the government. [The companies supported] the notion that the laws don't prohibit it. There's a reason why all these companies wrote letters saying we need help, [saying,] we need to change the law to share information with the government and allow the government to share information with us. We can't do it on our own today. So there's a broad coalition, … laws don't prohibit it, it's just perceived. I said that with respect to anti-trust laws. And I said that cautious lawyers are going to say don't take [the] risk [of information sharing]. I didn't say that with respect to [ACBA] (ph) and all these other laws that do prohibit explicitly the sharing of certain types of information with the government. They do; they were designed to do that.

One last thing I'll note. You know, [there is] this notion that somehow the private sector should be forced to minimize information that it provides to the government. Even in the surveillance laws, which are much more intrusive, which are much more aggressive, and actually involve getting the content [of] information from individuals, right, your phone calls, the actual content of your phone calls, [w]e don't expect [that] the private sector [will] minimize; we have the government [do it]. When it comes to the government, the government does its minimization procedures. So the notion that somehow that the private sector's being charged or being forced to minimize, in a situation where we're trying to create voluntary information sharing, puts a burden on them where they're simply not going to share. It just doesn't make any sense. We don't do it in the surveillance context, why would you try to create a voluntary cyber threat sharing mechanism? It doesn't—it's just nonsensical.

MICHELLE RICHARDSON: Because under ECBA and FISA that information is protected by a

subpoena or warrant or has some other front-end review by a judge or high-level officials that says that it's actually connected to suspected wrong doing. That's different. There's a front-end protection on it.

JAMIL JAFFER: Here we're talking about—

MICHELLE RICHARDSON: You're ….

JAMIL JAFFER: We're talking about a very narrow category of information. Cyber threat information, if you look at how it's defined—

MICHELLE RICHARDSON: Including [content] (ph).

JAMIL JAFFER: And by the way, on the CDT Constitution Project issue, I would note that they actually came to an agreement with us on the definitions, they supported the bill, … [and it] went to the Rules Committee. The Rules Committee did not make an order and amendment to prevent the NSA from getting the information directly, and that's why they finally came out and opposed the bill. (A) The House… Committee doesn't control the Rules Committee, number one, and number two, they did agree under…they still support the definitions and say the definitions are narrow enough for [the bill] to pass the House and to pass the Senate. So [it's not true that] somehow that they pulled their support; …that's just a canard, [and] it's not true.

MICHELLE RICHARDSON: And also what my last [point] is, [that] actually there are minimization requirements and things like that in FISA and under Title 3 surveillance where it is—

JAMIL JAFFER: On the private sector? I don't think so. It's on the government.

MICHELLE RICHARDSON: Well that's a very interesting thing to find out about FISA and some of these other statutes.

MELANIE TEPLINSKY: So we can see [that] information sharing, which is the piece of the cyber security legislation that is most likely to get to the President's desk, is entirely non-controversial. [That's] part one. [In] part two, let's talk about standards. Let's change the topic here and talk a little bit about standards. So we've got a couple of different comments here and I want to try to try and tie them together a little bit by stepping back. So there's been a long-standing claim that companies have underinvested in security; that there's been chronic underinvestment. And one of the points Jamil makes, and it's a very important point, is that there's a reason for that. The reason for that—and one of the reasons at least—is that there is a lack of information about how much damage is done by cyber attacks and cyber espionage and other cyber incidents. And so in part it is true that there is a lack of investment because there is a lack of information. And you can see the develop-

ment of a body of law in this area to try and force information out. We've seen data breach reporting laws, SEC guidance that requires—or at least reiterates requirements that companies report any material cyber incidents to the SEC, and other reporting rules which are designed to get more information out. And for those of you who follow these things, you'll see that Senator Rockefeller has sent out a letter to the Fortune 500 companies in the United States asking them: what are your cyber security practices? Think for a minute if you were a lawyer about how you would respond to that. But the point here is that there's one problem, and that's a lack of information. There is a second problem, which has not been raised yet, and so I want to just toss it out and see how folks think about this. And I think it goes to the reason that there was a problem—that the Chamber of Congress had a problem with the Senate bill that would have imposed only voluntary standards on the private companies with respect to cyber security. And it is that once a set of standards is out there, those standards can become the basis for tort liability. And I think that's the unspoken concern here. So can you speak to whether there is any room for negotiation on the standards issue and what he likelihood is of getting minimum baseline standards through Executive Order and how that will impact the legislation that's coming down the pipe? Anyone?

JAMIL JAFFER: Yeah, I'm happy to take that. I mean, it think that today there are things that everyone in the House and the Senate—Democrat, Republican—agree on, and one of those is information sharing. Another one is [changing] the criminal laws [by] making the government better at securing its own systems through FISMA reform. There are four or five bills—four bills, I believe, that passed the House that contained those consensus measures. The Senate bills both contain parallel provisions along those lines. But there is not a consensus between the House and the Senate, [nor] even within the Senate. What held up the bill in the Senate the last time was the issue of regulation, or even voluntary standards, [or] whatever else you might call them, because as Professor Teplinsky points out, maybe the creation of even voluntary standards may be a basis for tort liability. It also is perceived as a…attempt for regulation. Right, so today it's voluntary standards, tomorrow you lay a regulatory framework on it, it's not that big [of] a deal to do and it causes all sorts of people concern. Given that there's consensus on these other things, I think the view of the House was, let's pass bills that everyone can agree on, let's let the Senate act on those same bills, let's get to a conference, [and] let's [create] a bill that will at least move cyber security forward in the immediate term. Rather than try to wait to get consensus on these really hard questions, let's move the ball as much forward as possible. So that I think is where the House was. And we'll see what the Senate does in the next few weeks with the Cyber Security Act, but I think a wise move would be to pass a consensus bill that the House and Senate can conference on and get something that can reach the President's desk.

MELANIE TEPLINSKY: Michelle?

MICHELLE RICHARDSON: You know, that's a good question, and that's actually part of the theory about how they're going to get some sort of Title 1 regulatory thing through the House and

the Senate. [The theory] is that this Executive Order is going to come out, [and] it's going to start a process for creating these standards. But you have to use legislation to get the liability protection for cooperating with those standards. So we'll see. But I think that's exactly what the theory is about how they're going to get some sort of regulatory thing written into the statute, if for no other reason [than] that the liability protection will only come with something like that.

MELANIE TEPLINSKY: So Dr. Lotrianti, this one's for you. We've talked a lot about the use of possible information sharing and cyber security standards and how those two things may help us to bolster our cyber security, but we're here because we're worried about foreign attacks, attacks by nation-states against critical infrastructure that is located in the United States. So now the question becomes: what is the role of government when the cyber security of privately owned critical infrastructure is at issue? And the real question here, as I understand it is: where are the swim lanes? And you started to address this a few minutes ago. Could you talk a little bit more about that question?

CATHERINE LOTRIANTI: So the foreign threats are the biggest concerns. I sometimes referred to [them] as the advanced persistent threats. So the first step, what we've already talked about, [is] making sure that you identify those companies, industries, [and] sectors that are most critical for our security and making sure that they are, first and foremost, as secure as they could possibly be. You've got to figure out how we get there. But that's part of the regulatory [issue]. So Dick Clark was talking about this in the Nineties when he was at the White House, [when] his position was, and still is, that we have to regulate the private companies, period. They're not going to do it. So there's this disagreement between the companies that own these sectors and the government. It may be that we need [regulation]—that some have suggested that it won't be until we have that equivalent [of a] cyber Pearl Harbor will the government force regulation on the companies. [The] companies are too strong, [they] have a strong voice on the Hill, [and] a lot of lobbying power; they'll be able to keep the government out of their business, right? We don't know what's going to happen, but if we have strong regulation that—now, we are making an assumption here; the government's making an assumption, those who advocate this–is that that which the government would regulate would make us the most secure. And that's part of the contention of the private sector, that that's a big assumption, that the government knows how to secure us, right? So end of the day, by securing those sectors, however we do it, to the best they can be, would protect us against the advanced persistent threat. Because after all, it's not the criminal offenders, it's the APTs against the banks that are really disconcerting, or economic espionage that…. So it is the foreign—so that's step one. Now, the first discussion on the earlier panel is where I think the next steps have to be, that you need to engage—and that was kind of the rest of my notes—with the states and international actors in order to come to an agreement on certain rules of behavior. And it might be through punishment of China, for instance, just on economic espionage. Not okay. We don't have a consensus on that. We could push for a consensus, [although] not through our domestic legislation; I'm talking about the international legal regime. You know, WTO is one venue for holding [international actors] accountable for things like that. [The] same thing [exists for], say, the nuclear power plant sectors. The IAEA, as

I mentioned, [has] created what's called Wins. It's basically [that] they are now looking to conduct their regulatory authorities in the IAEA, but with respect to not [the] physical security of nuclear plants but cyber security. They've come to look at the U.S. first because we're kind of ahead of the game compared to most countries [that] have nuclear plants, but they want this of course to be international, so [they are also] looking to international organizations [and]the law of armed conflict issues. A big important issue [is] to understand or get some agreement as to what would constitute an armed attack under international law. So states know, you know, another state, a foreign adversary knows, oop, we probably should not cross this line and target XYZ in the U.S. because they've already put us on notice that that will be an armed attack and they would call it such, act upon it as such, triggering Article 51, and responding to us either in a cyber or kinetic way that would be lethal. So that is the international aspect. So it starts [as a] domestic [effort], I think, with the security. I mean, the information is tied to that too, but you jump right to the security of these critical sectors. But those are all rules that depend on international–not agreements in the sense of treaties–but consensus; it could be bilateral. I think it's mostly going to be bilateral, but [there are] even smaller steps, like hot lines, which have been discussed and worked on. So a state can actually call another state when they have an incident originating, or at least [when the] last point of departure was their countries, so we can not have escalation. And that's a foreign battle.

MELANIE TEPLINSKY: With that let me turn it over. I want to open it up. And sorry, I've actually run a little bit late. But let me open it up for questions. There was such a good debate; you just hate to cut that off. But is there anyone who has any questions? Yes?

QUESTION: Good afternoon. I just want to say thank you all for being here, it was a very interesting discussion. My concern is: was any thought given to the fact that information sharing between the government and the private sector… security risk, given that you may kind of tip your hands to foreign nations as to what exactly it would mean that we're doing in this country?

JAMIL JAFFER: So absolutely, and that's a big concern. The way that the government's sort of baked that problem is to say, look, we're going to provide classified information about cyber threats to the private sector in a classified setting, but provide it in a way and using methodologies that allow the private sector to deploy information on [an] unclassified [level] in order to protect themselves, using techniques that prevent the fact of the classified information that's being used from being disclosed. So I can't get really further into detail about how that works, but there are methodologies [that exist] today [that allow] the government to protect its own unclassified systems using classified threat information. It can provide that same sort of methodology to the private sector, and it did pilot that. And so there are ways to use classified information to protect the private sector [using] unclassified networks.

QUESTION: Hi. Thanks for coming out. I don't know if I need to use the microphone. I just have a question for you guys about who …exactly are we fighting and is there a difference between do-

mestic hackers with a 14-year-old in a room, or the group Anonymous, or is it China, like the government of China trying to destroy our economy because that's…? You know, just kind of trying to get my head around what's actually happening.

MICHELLE RICHARDSON: Well, this is one of the problems with information sharing; it lumps all of those people together. And while we hear the examples about cyber 9/11 or cyber Pearl Harbor, that's not what the legislation is about. It's not targeted at those sorts of threats, it's [about] general cyber security, you know, infiltration, manipulation of information, so that it is broad enough to include a dumb kid trying to do something in his basement, and puts [him] on the same level as, you know, the Chinese government who is trying to steal military secrets. The same information can be turned over. And that's been part of the problem; this has all been lumped together. And I think you would see far less opposition from groups like mine if it were really targeted at, you know, foreign nations and high-level threats that are really directed towards CEI or government information But they're not. They are including sort of petty criminal activity in the information sharing legislation.

QUESTION: I guess the follow up would be how do we know then? Or how do we distinguish what is government and personal….?

MICHELLE RICHARDSON: Well, the attribution question, you know, really depends [on] what your response [is] going to be. Because you don't have to attribute to mitigate a cyber threat, right? If you're looking to prosecute, maybe [you do]. But it really depends. You don't always need attribution if what you're trying to do is just stop the attack or prevent it in the future. And so I think that's more complicated.

JAMIL JAFFER: I think Michelle just responded to her own point, which is that she said on one hand we'd be less opposed to legislation if you differentiate between who the attacker was when you're doing your defense, but that you really can't do a good job of attribution and you don't really need to attribute if you want to do defense. And that point is, let's suppose you said, okay, we're only going to make legislation about high-end threats. So much for how you like the legislation that way. But then you just encourage the nation-state actor to act like a low-end criminal, right, and just use low-end techniques. The truth of the matter is—and now that the Secretary of Defense has talked about it we can talk about it—the Chinese and the Russians have extremely advanced cyber capabilities. Iran is increasingly making its presence felt on the cyber networks. Those [comments] are basically where the Secretary of Defense has gone with it; I'll limit my remarks to that. But I can tell you, there is no lack of a serious, no B.S. nation-state threat to the American private sector—and the American government, but the American private sector [is more vulnerable]—both from IP theft and the potential for real no-kidding takedown attacks. It's real, it's happening, [and] it's a problem. And if you don't believe that, you know, I've got a bridge I want to sell you in Brooklyn.

CATHERINE LOTRIANTI: I wanted to add one thing on the attribution [issue]. So clearly, [in]

domestic criminal prosecutions, well, you need the defendant there so you definitely need attribution, right, and that's part of the evidence game in litigation. But internationally, we can't forget that if the U.S. or any country is going to take an act in self defense, U.S. policymakers now, I don't put a percentage on it, like United States President [says]: [w]e have 100 percent certainty. International law requires attribution of an illegal act before you actually respond to it. So we don't—you know, attribution's difficult, and we disagree about how difficult [it is], but it is required at certain levels in certain ways in both spheres, both to prosecute domestically and also [when] you're acting under international law, where presumably we want to act in compliance with international law. [To do that,] you need to have attribution of the offender.

MELANIE TEPLINSKY: So—go ahead.

MICHELLE RICHARDSON: One last thought. There's actually been a lot in the press recently about attribution, and I think it's been phrased as "closing the gap," in that the government has started doing something over the last year that is really honing their attribution, but they haven't discussed it in a lot of detail, so I'm not really sure what it is. So it's possible that attribution is getting easier. But just to answer Jamil's question, [the] first thing you could do [is] limit your bill to information about threats to critical infrastructure. That way you will keep it focused on systems that are absolutely critical for national security and will cut out all of the, you know, petty criminals and things like that.

JAMIL JAFFER: So we let the Chinese keep robbing the American private sector blind at the heart of our economy, [and] we protect the critical infrastructures? I mean, I guess you could do that, right. But if you're going to share information between the private sector and the government, why not pick the whole of the American economy? Today the [DIB] (ph) pilot takes one little sub…by protecting defense industrial-based companies. If you're going to protect them, what's the rational decision for you protecting defense industrial-based companies and protecting the power grid or protecting IBM and Microsoft? Why Boeing and Lockheed and not IBM and Microsoft? Do you really want the government making those choices? It seems like a bad idea and exactly the opposite of what you want the government doing.

MICHELLE RICHARDSON: Or maybe we can have classes of them, right. So maybe outside groups would be okay with critical infrastructure and say the DIB companies [deserve more protection] because of their significance, right. That's kind of an okay, no brainer. They'll fall out of the critical infrastructure, but we might want to capture them. It sounds good to me only to the extent [that] if you can get actually a bill passed because we do that. I think it would at least not lose everything. Protect critical infrastructure, people are happy, and then maybe get more than critical infrastructure. You say: oh, how 'bout the DIB companies because they're special? And maybe you get a few more like that. Where maybe IBM doesn't fall under there in any way, but you know, at least you get the legislation passed.

MELANIE TEPLINSKY: You guys are so good we got an extension to 2:45. So if there's another question let's take one more question and then we'll wrap up. So everybody gets a little last word.

MELANIE TEPLINSKY: Oh, two more questions.

QUESTION: So my question is to kind of go back to what Professor Hollis, who just stepped out, was talking about in terms of an e-SOS. So do you think a system like that should be built into a domestic response to these types of threats? Because it seems like that's something that the private sector would be interested in doing, because it would allow them to coordinate with each other. You know, they can decide who wants to respond to what depending on what their knowledge is. And I'm curious if you think that's something they would be open to, and also what do you think the drawbacks to that sort of system would be?

CATHERINE LOTRIANTI: I'd like to hear from folks with intimate knowledge on the Hill, but my opinion on this? So one, what I do know is the private sector is interested. So I've been working with the telecoms. I've kind of implied that before. But here's one thing I caution. And I was going to ask Duncan if that's where he was going. I do not think this should be mandated by the government. I think [it's] very complicated and I see lots of downsides. But what I see as a positive [thing], and I believe it will be done by [the] sector, with companies like the telecoms globally–where they have common concerns, common security problems, and the reciprocity of benefits would be greatest–[is that] it would probably be not truly global but based on sectors, and it would be voluntary based. And it's like the basis of international law. You know, we do this, we join this. You have a problem if one ISP has a problem. But [in reality,] the ISPs themselves are not being attacked. You know, they're not the victim per se, the pirate ship in the analogy, but it's that the information they're responsible for is being threatened. The threat is overseas in somebody else's jurisdiction. But if they have a consortium of ISP members, or telecommunication company membership, they would be committed to helping each other. That that member who is the target or who's got a problem calls the other member and says, "It's in your jurisdiction. It's on your cables; it's on your wires. Now you've committed, [so] take an act in your jurisdiction." [That would be] a lot easier and less problematic legally than an ISP or a telecom in this country taking an independent act in another jurisdiction. But I would caution about getting the state governments involved. Because one, even with the telecoms that I've been working with—and I'm talking four different major government agencies that should be interested in this—I'm not quite sure [that the U.S. government] really accept[s] the nature of the threat as I've seen the companies trying to explain to them. These are just the Americanized pieces. And I don't think it's the government's one high priority or main mission. So I think it's going to be company-driven, consortium voluntary basis. And that's it.

MELANIE TEPLINSKY: Others?

QUESTION: So the domestic law dangers. Is there some hope for the—I think you were asking, is there domestic legislation or—

JAMIL JAFFER: To be honest, I don't know enough about the topic to speak intelligently about it. And also I came a little late so I missed Duncan's speech. I apologize for that. But it's an interesting concept. I think I share a lot of the concerns and thoughts expressed by [Bachelor Chauney] (ph). I think at the end of the day, folks working together makes good sense if you can find a voluntary methodology for doing that. There is one thing I'd caution, and that is that there's been a lot of talk about the need for international law in this space, and the one major cyber security treaty that's been proposed has been proposed by, I believe, Russia, Uzbekistan and I think China. And literally what appears on its face to be a cyber security treaty is really a methodology for tamping down free speech on the Internet, and that is not the place you want to go. So what one man's cyber security threat may be in this international law dynamic may be another person's free speech and you want to watch out for tamping that down. So that's the one caution I'd put out there about that.

MELANIE TEPLINSKY: So let me take a minute to wrap up and then maybe we could each take one minute of final thoughts. So I think what we heard today is that there are a couple of approaches that are being followed for cyber security, both in the United States and frankly as a matter of international law. The first is that we are interested in vulnerability mitigation, making sure that we protect our networks, right. That we have basic hygiene so we're protected against the script kiddy attack, and also making sure that our critical infrastructure has the kind of strong security that will help it to survive against a concerted attack from a nation-state actor. We've also heard that there's a move, I think, towards threat deterrence. And this was I think Dr. Lotrianti's point about looking at ways to use [methods], whether it's the Economic Espionage Act or the WTO, or other mechanisms, to try to put pressure on those who would threaten us to not threaten us. So right now China, which is engaged in essentially wholesale economic espionage against the United States, has no reason to stop, right? They're heavily embroiled in our economy, we have a lot of debt to them, there's not a lot we can do to take action against China. There are lots of policy levers because we're heavily engaged, but we can't press them because we are heavily engaged. So one of the ways we can think about this is how to think about deterring the threat of cyber attack. And then the final point I'd make, and this really goes to a different perspective, is that we're hearing a lot about attribution, and I would suggest one important concept to think about there is that as attribution becomes an issue—and there's [an] argument as to whether or not it is a substantial issue, because there's a very limited number of folks with the resources to actually put on a concerted attack of the sort we're discussing from a foreign nation-state. But whether or not it becomes a substantial issue, attribution is about learning the identity of the actor. And one of the things we need to be very careful about when we're talking about this [is], as the government becomes more and more interested in following attribution, there will be pressure from governments to have authentication mechanisms built into the Internet. And there is of course a corresponding pressure from the other side to protect

the anonymity, the very anonymity that allows dissidents that Jamil was just referencing in Russia and China to act in ways that they couldn't before and to facilitate things like the Arab Spring. So I think those are the things we need to be thinking of as we address the foreign attack scenario.

JAMIL JAFFER: You know, I'll just very quickly [talk] just on information sharing. I'm very hopeful that there is a middle ground to be found between the House-passed bill and the Senate bills that are currently out there on the information sharing piece. And I think it's very doable. I think that on the questions of liability, minimization, structure for sharing, and the specifics of what is to be shared and the uses to which it can be put, there are certainly differences between these bills, but they're differences that can be overcome and a middle ground found and a bipartisan, bicameral consensus found on a bill that can go to the President's desk. The challenge I think is, even if you were to find that consensus, can the Senate take up a bill that's just information sharing only, or just the consensus provisions, or are the Administration and the leadership in the Senate going to assist on some…. provision as they have to date? And I hope that we don't let the perfect be the enemy of the good. I think that while it's not a panacea by any stretch of the imagination, a substantial benefit will be gained to both the American government and the private sector to pass information sharing legislation. I think we're hopeful that that can happen and happen here in the near future.

MICHELLE RICHARDSON: Thank you for having me. Come back and see me on Tuesday afternoon when I'll be talking about FISA and I get even more upset about FISA so it should be interesting. The WCL/ACLU chapter is having an event on warrantless wire tapping, so I'll be back on Tuesday, so come see me then. So from this discussion, you know, I hope it's clear that the ACLU doesn't oppose efforts to improve cyber security or even encourage information sharing. At a top level we don't, and we think there are smart ways to do it. And we just can't encourage Congress and the Administration to get it right enough, because once you write this law you're stuck with it. I could tell you, after ten years of working on the PATRIOT Act and FISA and dozens and dozens of committee hearings, amendments, [and] competing bills, you're not going to make substantial changes to it once it passes, to be honest. So it's incredibly important to make sure that when you're talking about undoing 50 years worth of privacy laws that were very carefully considered and passed that you make sure that you keep these programs civilian, limited to the information necessary to address a cyber threat, and then limit its use to only cyber security purposes.

MELANIE TEPLINSKY: Well, thank you to all of you for being here today and a warm round of applause for our panelists.