CARNEGIE COUNCIL *for Ethics in International Affairs*

The Ethics of Hacking Back: Cybersecurity and Active Network Defense

Carnegie New Leaders, Ethics Matter

Gregory Conti, Robert Clark, Chris Rouland, Jennifer Otterson Mollick

Transcript

JENNIFER OTTERSON MOLLICK: Good evening. My name is Jennifer Otterson Mollick, and I am the program coordinator for the Carnegie New Leaders Program here at the Carnegie Council. Welcome to tonight's event.

One of the core themes of the Council as we lead up to our Centennial in 2014 is technology and risk. So we are especially pleased to welcome Colonel Gregory Conti, Mr. Robert Clark, and Mr. Chris Rouland to participate in this joint Ethics Matter and Carnegie New Leaders event on "The Ethics of Hacking Back: Cyber Security and Active Network Defense."

Before we begin, I would like to introduce two people whose hard work has made this panel a reality. First is Miro Vassilev, the Carnegie New Leader who first suggested this event and has helped coordinate it. Miro is a fund manager focusing on global macro investments. He is a graduate of Oxford University, Harvard University, and the Wharton School of Business. Miro is also a Truman National Security Fellow and Military Business Cyber Fellow at the Madison Policy Forum.

I would also like to introduce Lieutenant Colonel Jon Brickey, and thank you for all of your hard work organizing the panel you see here before you today. Lieutenant Colonel Brickey is the Army Cyber Command Fellow at West Point, where he is an assistant professor and associate in the Army Cyber Center and the Combating Terrorism Center.

So thank you, Miro and Jon, for arranging such a knowledgeable panel and for joining us tonight.

Now I would like to introduce our moderator for this evening. Colonel Gregory Conti is an associate professor and director of the U.S. Army Cyber Center at West Point. Colonel Conti has served as a senior advisor in U.S. Cyber Command Commander's Action Group and is officer in charge of the deployed U.S. Cyber Command expeditionary cyber support element. He co-developed U.S. Cyber Command's joint advanced cyber warfare course. Colonel Conti is also the author of *Security Data Visualization* and *Googling Security*, as well as over 60 articles and papers covering cyber warfare, online privacy, usable security, and security data visualization. He has spoken at numerous security conferences, including Black Hat, DEF CON, VizSec, and the NATO Conference on Cyber Conflict.

Thank you, Mr. Rouland, Mr. Clark, and Colonel Conti for joining us this evening, and I will now turn the floor over to you.

GREGORY CONTI: Thank you very much.

Like any good discussion, this one must begin with a legal disclaimer. The views expressed in this

panel are those of the speakers and do not reflect the official policy or position of Endgame, Inc., the United States Military Academy, the United States Naval Academy, the Department of the Army, the Department of the Navy, or the United States government. Have we forgotten anything? Is this sufficient? Okay, I think it is. We are here as free citizens, and these are our personal opinions. So thank you.

I would like to take the next couple of minutes to frame the discussion, because we have this big topic of hacking back and active defense. What does that mean?

I thought it would be useful to provide one definition—there are many—on what hacking back is. This is provided by Dorothy Denning in 2009: "Hacking back is a form of active response that uses hacking to counter a cyber attack. There are two principal forms. The first involves using invasive tracebacks to locate the source of an attack. The second involves striking back at an attacking machine in order to shut it down, or at least cause it to stop attacking." Just to ground our discussion, that's one definition. Our panelists may or may not agree, and we will tease that out as we move forward in the evening.

The idea of hacking back, or the more broad active defense, is rife with ethical dilemmas and challenges. The driving factor behind all of this is, some would say, the largest transfer of wealth via intellectual property theft in the history of mankind. Technology is changing much faster than policy and legal frameworks can perhaps keep up, although some may argue that the ones we have today are still valid and able to be applied.

In our discussion today, we will be thinking in the context of hacking back and active defense in the context of the private sector, so not U.S. government or anything. I think we are taking primarily about a private sector approach.

There are many adversaries that we need to consider: Who are the adversaries attacking us, the private sector, and who we would want to then counterattack or do something bad against—such as there could be insiders in your own company that are doing some type of activity? There could be lone malicious hackers; there could be "hacktivists," groups of people out there that are self-organized; there could be online criminal groups involved. You can see we are increasing in capacity and potential resources as well.

Then you start getting to the nation-state level of organized cyber capabilities, from relatively small nation-states to very large and very powerful nation-states. So who are we attacking back against?

Physical location matters. Who owns the devices both being used to cause the attack, as the perpetrators of the attack? Are there any intermediaries involved? People will try to mask their identities often. They may try to pin it on neutral parties. So location, ownership, and control of these devices all matter. Geography drives the jurisdiction in many ways. And what legal framework applies?

How do we deter these attacks? If we do conduct a counterattack, do we risk escalation? Could that escalation transfer from cyberspace-only effects to something in the physical world? You can envision attack, counterattack, and then people with guns show up as a counter-counterattack.

Does private industry have the resources? At what level do they have the resources to mount a sufficient counterattack? Do they have sufficient information to do so, intelligence to determine who the adversary is? This is an incredibly difficult problem. Do we want a "Wild West," where companies without any sort of regulation are attacking back?

What are the international norms and agreements that are necessary if we were to support these types of activities? A norm in one location may be the exact opposite in another.

What about collateral damage? And all of this is in the context of attempting to preserve the privacy and civil liberties that make our country and other democracies around the world places that we want to live.

So, with that, I will introduce our panelists.

The first is Robert Clark. Robert Clark is the distinguished professor of law at the United States Naval Academy Center for Cyber Security Studies. A career military officer and attorney, Mr. Clark has over 20 years of experience within the Department of Defense (DoD), having served at its counterdrug command, as well as numerous other positions. He is the former operational attorney for the U.S. Army Cyber Command; cybersecurity information oversight & compliance officer for the office of assistant secretary of cybersecurity and communications, Department of Homeland Security; and legal advisor to the Navy chief information officer.

Clark is also an adjunct professor in the College of Professional Studies, University of Maryland, Baltimore campus, instructing on cybersecurity law and policy and cyber warfare. He is a past lecturer at Black Hat, DEF CON, Stanford Center for Internet and Society, and the Berkman Center for Internet & Society at Harvard University.

Chris Rouland is founder and founding CEO of cybersecurity firm Endgame, Inc. Mr. Rouland was previously chief technical officer (CTO) and distinguished engineer of IBM Internet Security Systems after IBM purchased Internet Security Systems, Inc. (ISS) in 2006. Prior to the IBM acquisition of ISS, Mr. Rouland was CTO of ISS. Before his executive roles at IBM and ISS, Mr. Rouland was the original director of the X-Force vulnerability research team, which was responsible for the discovery of hundreds of security vulnerabilities. He was also a vice president at Lehman Brothers.

With that, I would like to ask Mr. Rouland if he would provide his opening remarks.

CHRIS ROULAND: Thank you, Colonel Conti.

He neglected to mention that we enjoyed a little crossover in graduate school at Georgia Tech. I won't say who was first. But it's interesting that the guys in the military seem to finish their Ph.D.s exactly on time. [Laughter] Congratulations, Colonel Conti. It's good to see you again.

I've got a couple of General Hayden quotes in here. I had the opportunity to work with him when he joined Chertoff Group. He just has, I think, some fantastic metaphors for what's going on in cyberspace.

I think the one he used Saturday was "a global free fire zone," which is really what we're operating in today. Everyone is shooting everywhere. We've got attacks coming from within our own country, from machines that are co-opted, machines coming from outside the country.

You've got a situation where critical infrastructure, as defined by the government, is almost entirely owned by the private sector. So how do we deal with situations where our national critical infrastructure is owned and operated by civilians and unable to defend itself?

The first challenge is not necessarily technical, but it's clearly legal, and it's frankly illegal to attack back today, to attack back in a traditional information security sense of throwing a load of packets

back, or throwing an attack or a backdoor at an adversary, because the odds are it's going to be attributed incorrectly. It's a violation, I think, of Title 18.

But we've got to deal with this. I'm hopeful, as our new leadership, whether it's our legislators, our military leadership, and our government leadership becomes and emerges as more technically savvy, I think they are beginning to recognize we've got to not only deal with some of the privacy challenges, but the challenges of how to deal with the fact that most of our critical infrastructure and assets lie in the private sector, as well as the talent in cybersecurity.

It proves very difficult to retain the top cybersecurity talent in the world in government permanently because it's simply too lucrative in the private sector. I have immense respect for those who make the sacrifice to wear a blue badge or wear a uniform. They take a lot of risks. They take a massive pay cut as compared to working in the private sector, and they are granted special authorities to defend our country.

Conversely, my opinion is that the government should not necessarily be in the software business, and the private sector has shown and proven over the years that they are effective in the software business.

So I think we have a couple of options on how to gauge private sector and government cooperatively to deal with threats.

I did some history work, which is normally outside—I'm a techie—of my work. I looked at the nationalization of the railroads in 1917 by President Wilson. He basically said, "Look, I am taking over because you guys aren't doing a good enough job to support the war effort."

So we've got a history of either nationalization or conscription. Neither of those techniques, I think, would be entirely effective—conscripting, literally drafting, cybersecurity experts from Wall Street to go work at Cyber Command. But I think there's an intermediary concept of public and private partnership, whether it be a militia or a cyber National Guard, where the government can grant these authorities to vetted individuals to help them in case of cyber attack.

It's really a hybrid model. This is my personal view. But we've got to have some way to create risk and consequences for bad actors on the Internet, and we really have no capabilities, or very limited capabilities, today.

GREGORY CONTI: Very good. Thanks.

Mr. Clark?

ROBERT CLARK: Colonel Conti, thank you. Carnegie Council for Ethics in International Affairs, thank you for inviting me here today. I'm the lawyer, so by all means throw your barbs this way.

The aspect of active defense stems from a couple of things that from a legal perspective frame the issues on it.

As far as a self defense or a digital self defense, I'll quote Orin Kerr, who's the criminal law professor at George Washington University: "It doesn't exist." So there is no self-defense to the Computer Fraud and Abuse Act.

But the problem is active defense isn't going, just necessarily, only outside your network. There are a whole host of things that we can do as computer security and computer network defense that are

actions taken within your network. That's, I think, where we jump to "I've got to strike back" without doing all those things ahead of time.

The main aspect on that is, because there is no self-defense—I talk to folks. When you go to security conferences, it becomes: if you're going to do something like this, then you've got to apply the principles of self-defense.

Now, there is a case out of California, *Intel Corp. v. Hamidi*. Hamidi was sending a bunch of emails back to Intel when he got fired, causing problems for Intel. In that case, the amount of emails going in there didn't rise to the level of spam. The court was looking at it as what's called a "trespass to chattel." That's where I'm basically interfering with your property and I'm lowering the value of that property.

But the court said: "I haven't diminished your computer servers. Your computers are still up and running. Yeah, it's harassing your employees, it's taking away some of their time and productivity. But there's no trespass to chattel here. And, oh, by the way, the law favors prevention over post-trespass recovery."

Now, I'm a simpleton. So what I typically view that as: if my neighbor borrows my lawnmower and takes it and locks it in their shed and I walk over and kick down their shed door and get my lawnmower back, that's post-trespass recovery. They've taken my lawnmower and I'm going back and getting it back. But if I lock it in my shed, that's the preventative measures that we need to do.

So if you're going to go in this area and operate in this area and do these things, then you want to convince the Department of Justice (DoJ) not to prosecute you—or, worst-case scenario, a judge or a jury because you're being prosecuted—what were those steps that you did ahead of time that were necessary and reasonable to protect your property that got us to this point where we're at right now?

There's a whole host of things that you can do from technology, from red teaming and penetration testing your systems on things, to spear phishing your own people to make sure they're not clicking on the wrong thing, to business knowledge, which borders on—you've got to be careful on economic espionage aspects of it. So a whole host of things that you can do ahead of time before you reach out and go outside your network.

There are a lot of places, as far as self defense, if you want to go back and get your intellectual property that has been stolen. If you are in a place that you have a lawful place to be and you're doing what anybody else can do, then you can go get your property back. The challenge with technology is facts are king.

I've talked to Colonel Conti before about this. I'm trying to make Clark's Law famous: The first thing is you need to get your lawyers involved early and often. The next thing is you need to explain the technology to them at a third-grade level, because they've got to turn around and explain that technology at a first-grade level to a senior leader or a judge. As lawyers, we very much want to learn the technology, and we will painstakingly be with you as you're learning it.

The one thing I'm hoping, if you hire a good lawyer, which is on you to hire that good lawyer, we've been trained through law school to ask the right questions. So as you're explaining it, we are hopefully asking the correct questions to fully understand what it is you want to do. There's a lot of things out there that you can do, prior to actually melting somebody's hard drive, to retrieve your property.

GREGORY CONTI: First question: Is hacking back even necessary? If you're a nation-state, there are many levers of power available; or if you're a private company, you have other tools, such as lawsuits.

CHRIS ROULAND: I'll go out on a limb and I'll say I think it is.

Let's take a simple example, denial-of-service attacks. If you look at 2012, 19 percent of denial-of-service attacks from inside the United States came from inside the United States. So if you take that 19 percent out, half those denial-of-service attacks—this is the drones attacking, not just the command and control—came from China and Russia. So it's kind of a low-baller to (1) filter out those attacks technically at a primal level; but (2) is, I'll quote General Hayden again: "Good people don't let bad people do bad things." Another metaphor for good people not letting bad people do bad things would be good people don't let bad guys set up terrorist training camps in their backyard. When they do, typically something bad happens to them.

But we've got a situation where nation-states allow bad people to do bad things with no oversight and no downside. So there needs to be some consequence there. Now, whether it's the FS-ISAC (Financial Services-Information Sharing and Analysis Center), Cyber Command, or some other entity hitting them back, there needs to be some deterrent. My take is I think the legal process operates in months and years and we're talking about attacks in milliseconds that can be very destructive to an organization. It could be all over by the time you get to court.

GREGORY CONTI: How useful is embarrassment? There have been some embarrassing reports that have publicly outed various actors. It wasn't a fast response; it took months. But is that another tool in the spectrum of options that companies can use?

CHRIS ROULAND: I think, for instance, there have been finally some really good reports out of Mandiant and McAfee on some state actors, specifically China. It was not necessarily just embarrassment; it was these guys really did their research and published multiyear studies that just nailed it.

I think that's helpful at a policy level, because now it's on the table as a policy discussion. But at the end of the day I think one of the highest-level challenges is—this is debatable—I think from what I've seen we're the only major nation-state that doesn't use its national intelligence apparatus to advance its corporations. So if that's the playing field, where our adversaries use their national intelligence apparatus to advance their corporate entities or they're totally mixed together, then certainly we're different from them, and that makes us Americans. But this is the new normal.

ROBERT CLARK: So here's the government lawyer stepping up:

From what I understand, corporate espionage is not new. I'm a Chrysler kid. I'm from Detroit. My dad worked for Chrysler. There's a book out there, called *Beijing Jeep*, a great book. Basically, it was Chrysler's attempt to sell 1.2 billion Jeeps in China in the 1970s. They were going to just make a killing. Of course, what did China want? They wanted the transfer of technology and that was it, and that's what they got. Chrysler got left with egg on their face and it was a big fiasco for Chrysler. That was in the 1970s.

The challenge now in the public-private partnership: If there's a threat the government knows about, if it knows about training camps somewhere, yes, it should do something about it. If the government knows a specific threat is going towards a specific company, yes, they should share that information. If they know of a specific signature that should be put in place for a Snort box, they should share that

signature, absolutely.

Where it diverges—so let me make a lot of enemies right now—is: Why should government give private companies incentives or tax breaks to do security? I'm a taxpayer, and from what I understand, my brother-in-law and I are the only two people that pay taxes in the world, so I'm going to have to pay for this, because everyone else gets out of paying their taxes. I'm not smart. So for this, if I give incentives and tax breaks to companies to do your cybersecurity, as a taxpayer I am going to pay for it.

If you do your cybersecurity as a private company, you are going to pass that cost on to me as a cost of doing business with you. So I'm still going to pay for it.

I'm at a loss for why you should get tax breaks and incentives, as opposed to do-it-yourself, which is what you're supposed to do, because that's what we've done in the 1950s and the 1960s and the 1970s. Maybe not so much in the 1980s; we were all into ourselves. But that's what we expect business to do.

Again, this isn't saying, "Wait. You know stuff that I don't know." You're absolutely right. If there's something that I know that you don't know, then I should be sharing that. But, given all the companies that are out there that have very good products—the iDefense, iCyte, the Mandiant reports, the people that are doing these things—and providing business intelligence and cybersecurity intelligence to you, my question becomes: How much better is the government information over what these companies are doing and what they're providing at high cost to the companies, so they should be providing something worthwhile? So there's that aspect.

The interesting aspect on the denial-of-service attacks coming in is something that we hear a lot about. I've heard—again this is the aspect to explain the technology to me—I've heard arguments made by people saying, "Well, the problem with that is business invested in their pipes coming into their system and they chose only such a size of pipe because of costs, and they're capable of doubling or tripling the size of that, which adds cost. But if they have that, denial of services would be a blip on the radar."

Now, I'm not a techie, so I would defer to Chris on this aspect of it. But again, that's all of the cost of doing business and managing risk. The new PPD-21 (Presidential Policy Directive) just came out, and it says a great line: "The owners of critical infrastructure are best and uniquely situated to manage their risk."

Hey, if I'm critical infrastructure and the government says, "Hey, we want you to do something," I'm going to point to that line as their attorney and say, "You said in your document ‘We are uniquely positioned to manage our risk.' We'll do that. We've got it. Thank you very much."

Those are my two cents.

GREGORY CONTI: Do senior leaders have the background to assess risk? I know it's a challenge in the military and other places, that they're experts at their primary line of operations in the business arena, be it finance or something else. Cyberspace is sometimes really altogether different, and the laws of physics can be counterintuitive, and it's hard to assess risk. These senior leaders have a difficult time. So any opinions on how qualified senior leaders are to make cyberspace/cyberthreat-based risk assessments?

CHRIS ROULAND: The game has changed so much over the last 10 years. Ten years ago,

customers were worried about their web page getting effaced. Now they're worried about going out of business the next day because their mail spool got dumped or they were offline for three days.

I don't know that, say, the chief information officer of Bank of America should be prepared to deal with a state actor like Iran deciding they want to shut down B of A, JPMorgan, Wells Fargo, and Citi. I think the government has a responsibility to protect our borders in cyberspace just as they do in real space.

GREGORY CONTI: How well are they doing it?

CHRIS ROULAND: They're not. They're not protecting. It appears they may have good capability to inspect. But there are plenty of kinetic parallels. If a private charter from St. Petersburg showed up full of drugs and money at Kennedy, the response will be pretty straightforward, which would be to stop the packet. But a trillion packets come in from Russia attacking critical infrastructure and there is no response.

There are a lot of technical challenges, I think, in effectively creating a cyber border, but in doing so would allow law enforcement to prosecute threats inside the country. Certainly a lot is going to get through, and then I think could reduce some of this need to hack back.

ROBERT CLARK: An interesting aspect is the protecting-the-border part of this. Back in the day a decade ago, when there was a MAE-East and a MAE-West (Metropolitan Area Exchange)—and that has clearly changed—

GREGORY CONTI: You need to define MAE-East and MAE-West.

ROBERT CLARK: MAE-East and MAE-West: so it would be the Internet exhcange point? It was the two pipes coming into the United States. I've got to go to the techies on this, because again I know the acronyms but I don't know what's behind them. It's the two pipes coming in.

They said, "Okay, hey, the two pipes come into the United States, we put a big old sensor on that thing and we can monitor that, put rules on that." And we thought, "Okay, civil liberties and privacy. Is everybody really going to want"—10 years ago—"everything being monitored coming in and out of the United States?" Of course we backed down. Now we know, but hell no on that.

The other challenge on this is there is the National Cyber Incident Response Plan. It was drafted in September 2010. It's the only plan the government uses right now if there's a significant cyber incident. And of course, it's a gobbledygook of governmental policy thrown together to define what is a "significant" cyber incident. The Department of Homeland Security (DHS) is in the lead for that, until such time as the president wants to say, "This is an attack. DoD (Department of Defense), you're now the lead. DHS, you have a supporting role now."

And here's the aspect of being a lawyer, and I apologize for this. Under the requests for comments, Section 4949 is the glossary, and that's definitions. In there it has the definition for events, incidents, intrusions, and attacks. Now, being the government, we're also very wonderful at coming up with a lot of definitions, and we have definitions for events, incidents, intrusions, and attacks.

"Attack" is a very specific word, not only for a lawyer but for a government lawyer, in terms of who's going to take over, be it DoD over DHS. So from my aspect—and I got in trouble and I'll say it again—I get to see an attack. Thomas Rid, our good friend, has also recently just published an article where he says he has not seen an attack.

Now, the reason why that wasn't an attack was because the president of Iran did not complain to an international body and point-blank say, "I have suffered a violation of the law of armed conflict, international law, and it was done by X and Y." That was the only part that missed on that. Everything else was a use of force. But it wasn't complained about, so it wasn't completed, or it would have been a "cyber attack."

I know I'm totally being a lawyer here mincing words. But that's the challenge here in this. The government is in the job to provide security for the United States and its people on that. Private businesses are in a job to protect their own intellectual property and make sure their pipes are running.

Saudi Aramco—at a briefing I was at, someone said, "What was the damage to Saudi Aramco? It's like they lost $30 million."

Then the staffer said, "Yes, but they're still up and running, aren't they?"

Yeah, they are. Nobody wants to lose $30 million. And I agree with that, that's not a great answer. But the fact of the matter is they're still up and running, and—I go back to it—if the government has knowledge on a specific threat, yes, absolutely we should be sharing information and working together. It's that aspect of finding that balance between—again, it's businesses' responsibility to defend their intellectual property.

From a lot of folks I hear, they're not even air-gapping off their research and development sectors, their crown jewels. I mean if you're not going to take the steps to protect your big thing you're working on, it's hard to step up and say, "Government, do this for me."

GREGORY CONTI: So the government likes its acronyms. One of them is a tongue-in-cheek acronym called RUMINT, or rumor intelligence. This is an audience participation question, in addition to the panel. Are companies—have you heard rumor—and this is by no means stating that you are doing this or that you have any real substantial knowledge that can be used in a court of law or something—a better disclaimer Bob could come up with—have you heard rumor of companies offshoring hacking-back activities?

PARTICIPANT: Why only offshore?

ROBERT CLARK: In other words, companies actually hacking back and not using just offshore entities, but maybe someone within the continental United States.

GREGORY CONTI: Okay, a couple certainly had some hands raised. And I think we've all heard certain rumors in that space. But did you have any comments that you'd like to make?

ROBERT CLARK: When I go to security conferences, this is a hot topic. Rumor intelligence is you talk to people and they say point-blank, "Yes, U.S. companies are using offshore entities or folks to hack back." You never find out what that means.

Today there was an article in the American version of Al Jazeera on hacking back, which quoted a Phoenix company. The Phoenix company won't tell you who their clients are—"that's confidential" —which is what you get when you talk to all these companies who are doing this.

"What are you doing?"

"Providing services to our clients."

"Who are your clients?"

"That's confidential."

Interestingly enough, one of the scenarios they were talking about is where they're being blackmailed. They say, "Okay, we're going to take them down the rogue path here. Tell them we're going to communicate with them. We're going to do it securely, so they need to load this code onto their system so we can communicate securely." We say there's no self-respecting hacker or blackmailer who's going to sit there and download that code. But, sure enough, you'll always catch somebody who's going to do it.

A colleague of mine who works for a law firm out in Colorado, called Titan, Dave Wilson, said, "We're not sure that if someone's being blackmailed when they download code that's lawful without their consent."

I called them, coming here today, and we of course clarified. He's like, "Yeah, no, I wasn't quite quoted on that, because if I send something to you and we're communicating and I say, 'Hey, let's communicate, please download this code so we can communicate,' and you download it, you've consented to doing that. You put it on your box. So as far as the legal aspect, you've consented. The fact that I'm going to get your Mac address and your IP address, that's consent from my aspect."

So again, that's an active response. I have no problem legally from that aspect of it. I talk to the programmers, my techies, and say, "Okay, that code, exactly what's it going to do? What information are you going to get as you do that?"

PARTICIPANT: I work with a lot of law enforcement on similar stuff. The concern I have is—and I brought this up as a very creative look at active response—is Java Script. If we have a technical adversary and they know how to use Firefox or turn it off or everything like that, we say, "We've got their fingerprint, we've got them."

A good example, years ago there was a heap overflow with Java Script that you could actually get all the bookmarks from them. Well, it's a great maneuver from a counterintelligence perspective.

That process was: "Well, they are accepting the use of Java Script and the code that they went to deciding to go to this page." Do we say that that's totally legal, because what's the limits of us saying, "Okay, well, I put that code on there and now I might use it to inject further code and things on that?" What is their point that they say, "I didn't consent to this whatsoever"? So you can kind of get into that little tricky play there too, because now that it's all about intent and consent. Does that make sense?

GREGORY CONTI: Terms of service, would that cover it?

ROBERT CLARK: The terms of service, you've got to love that aspect because Skype just went through that, as a matter of fact, hit the press with them, went for a blackout in terms of the aspect of their terms of service, and people were complaining. They said, "Oh no, you agreed to this in your terms of service."

So again, your point being—again, I've got to do it whenever I can—Clark's Law: Get your attorney involved early and often and break it down and explain what it is you're going to do. They need to understand.

"Okay, you're getting a Mac address."

"What's a Mac address?"

"Now we're going to get the IP address."

"Okay, what's an IP address?"

What you are going to get and what is it that you want to do has to be broken out in painstaking detail.

Now, once you do that—you've got to remember one aspect about attorneys. It's what I call "the steak dinner." At the end of the day, I'm going to go home and have a steak dinner.

Now, if this is my client, they're going to make the decision, because they do the risk management aspect of it. So if he's my client and he decides to do this and it's illegal and the cops come and put handcuffs on somebody, it's him. I go home and I have the steak dinner, and I'd go look for another client. Now I've got less of a client. I may be liable for malpractice and negligence.

So from that aspect of it, you've got to break it down, get them involved early and often. And what you're going to do, as far as that continuum, that's up to the risk managers.

PARTICIPANT: Jerry Spivack, Columbia University, Knowledge, Technology, and Social Systems Seminar.

The thing I'm concerned about is the way you've been using the term "critical infrastructure." Now, in the past, critical infrastructure meant railroads, it meant things like the highway system. It seems to me the critical infrastructure that's developing is computers all over the world. That's the critical infrastructure. And what's happening is that the critical infrastructure is moving from the West to the East, because there are more people in China than there are here. And as a matter of fact, we're going to try to sell tons of computers there. Pretty soon the Internet, which has to read all of those computers in order to look at the addresses and everything else, will be basically primarily in China, as opposed to, let's say, here.

So to me that's an easy way to hack. You just become the largest possessor of infrastructure and you're all set. So I don't know how one can even approach what's about to happen.

ROBERT CLARK: Again, PPD-21 identifies 16 critical sector-specific agencies. Ironically enough, in the introduction it says the two most critical that go over all of them are energy and communications, which I think is what you're talking about.

PARTICIPANT: Absolutely.

ROBERT CLARK: And then I've had some of my students say, "Okay. Wait a second. DHS seems to have a lot of power over this. But a lot of it's international."

I had to clarify that: "You've got to understand, DHS is for leading and coordinating the cybersecurity for the executive Branch, the dot.gov, of the United States. There are a lot of international things out there. Yes, we talk about the Budapest Convention from that aspect."

So the critical infrastructure, obviously, is in the United States. But when you start moving it—this is part of Eric Schmidt and Jared Cohen's book, *The New Digital Age*, where there's several countries

that are going to leap over different levels of technology and move right to the handheld aspects of life. They don't even know what a dial-up modem is. Yes, that's going to be a huge challenge moving forward.

CHRIS ROULAND: The flip side of that is specifically the United States certainly is the hub of the big-I Internet, and I think will be for some time.

The challenge of it moving to a country that imposes significant restrictions on the Internet's content—censorship is a performance problem. You can't move big-I Internet to China because they can't scan it fast enough to make sure the citizens are not reading materials that are against the regime.

So if you look at other countries that are very picky about what they let in, where their citizens don't have freedoms on the Internet, it also creates a huge performance drag, more so than just defending against attacks.

GREGORY CONTI: Could that ultimately be automated away so they could have it at machine speed?

CHRIS ROULAND: I think it's always moving faster, and there are a few vendors out there that make these technologies that allow oppressive regimes to restrict what their citizens can read. But it's always going to be content inspection and it's going to slow things down.

PARTICIPANT: Lance James.

Are you guys familiar with ITAR (International Traffic in Arms Regulation), the compliance for crypto and what you can send out to the rej8 [phonetic] and the different countries and stuff? When we're talking about hacking back, and we talked about weaponization of tools for this, if we even talk about companies that come along and decide to build weaponizations—we even talked about zero days that are being sold supposedly to the government, things like that. So obviously we're in an era where this is being addressed more frequently.

Where is the line where it's ITAR-classified, in the sense of "Hey, my decision, even if I had a lawyer in front of me—why can't they say, 'Well, that's a weapon'? Why are you suddenly allowed to do that as an industry and not have that ITAR-classified?" Does that come up much in these conversations?

ROBERT CLARK: Again, you're asking challenging questions where facts are king and facts are very specific. There's a lot of research going in right now in terms of—you're spot-on point—cyber weapons. What is a cyber weapon per se?

We have, at least what I've seen a lot in—this is not going to help you—in the legal community, we've gone to "what is the intent or the purpose?" because the same tool I use to gain access to a box, which would be espionage, not causing any damage whatsoever and not illegal under international law—domestic law it's illegal, but not illegal under international law. So now it's espionage. But of course it's got a payload in there which comes back the next day and it says, "Okay, now I've got to execute the attack."

So again, we look to the intent and the purpose for what that code and tool is made into. When you're working in private corporations, in corporation settings, you better have a darn good technology lawyer in your hip pocket.

GREGORY CONTI: And that's one of my personal fears, is that tools that legitimate security

researchers and system administrators and others use to perform their jobs think, "backtrack and metasplit. Will this one day become illegal and then we'll shut down the ability to use those tools to make systems more secure?"

PARTICIPANT: Bob Perlman.

A quick question. You had mentioned FS-ISAC. The SIP process (System Idle Process?**)** for various key industry verticals has government/public/private partnerships, such as FS-ISAC, the Chemistry Council, so forth and so on. Why aren't those being strengthened so that we can provide defense mechanisms, shared intel, et al, against the symmetrical and asymmetrical threats?

ROBERT CLARK: The National Cybersecurity and Communications Integration Center (NCCIC), which has subsumed the US-CERT (United States Computer Emergency Readiness Team), has on the floor all the definitive ISACs that are supposed to be working for the sharing of information.

Again, the public/private sharing of information is the largest complaint that I hear. And strengthening it? I hate to answer a question with a question, but you're right. How? Is it going to be more private folks coming in? Who's going to pay for that? Will there be more government resources going towards that?

I do greatly apologize. I don't have a good answer for that one.

CHRIS ROULAND: It seems to me, looking at FS-ISAC and national defense, that there should be a big red button that FS-ISAC can push and say, "Shields up, guys. We need National Security Agency or Cyber Command help. We got an inbound from this bad-guy country. Block everything until we figure it out, because we're hosed." If they can't, then call our friends in Phoenix, who will probably call a company in Tunisia—you know, the fixer—and they'll take care of it.

But no, really, I think there should be some kind of time response, hit a big red button, just like your alarm system, and help is called, at least for macro-level issues, especially what we saw with the Iranians, the denial-of-service attacks on key financial services. I think it's a good case study where you can say you should really have a 911 for that kind of event.

ROBERT CLARK: Now, again, the aspect is the report. Here's the challenge: According to the NTAC (National Threat Assessment Center) and the US-CERT, it's voluntary. In companies, it's not mandatory. And oh, by the way, when that was kicking off, they were reporting and the banks were calling in. So then it becomes the aspect of how much information are private entities sharing this way for it.

So it wasn't like this was a surprise. Everyone who was working there—there was kind of the red-button aspect of it. Again, the National Cyber Incident Response Plan is supposed to be the big red button that calls in all the folks from the United States government who are supposed to be senior leaders who are supposed to be able to say, "You need to make decisions back to your entity."

So if, Department of Interior, you need someone to disconnect, you've got to be able to say, "Okay, we've got to shut down, kill that"—nah, it's government. I don't know if I have that level of confidence in the government that they're going to send that senior leader that's going to say "shut it down, disconnect."

And again, I will confess, and maybe agree with Chris. Does it work at the speed that it has to work for the Internet? I actually have more confidence in the business sector, kind of a Conficker Working

Group. When the cabal was put together to resolve that aspect of it, that was done first by private folks moving forward on it.

If this goes up, again, we all know each other in this industry, and you'll have your senior leaders up talking about what we're doing. But you're going to have a lot of people in back channels talking to the different cyber centers, different companies: "What have you got? What are you working on? What have you figured out? Here's what we've figured out."

Fortunately, I have enough confidence in our techies, that they've got a big enough chip on their shoulder that says "not to me, not today," that they'll keep things up and running.

GREGORY CONTI: If you'll give me a minute, I'll ask the audience a question. You may have heard of an obscure news story involving Mr. Snowden. In a post-Snowden era, I'd like your thoughts on public/private partnership.

With a show of hands, is public/private partnership more likely?

Is it the same as pre-Snowden? Has there been no impact?

Is it less likely?

Of the people that responded, everyone said less likely.

Anyway, I think that's a backdrop now, that there is a pre-Snowden/post-Snowden look at this public/private partnership.

PARTICIPANT: Gadi Evron. I have many titles. I'm not sure which hat I should use right now. But I have been working in this area for a while now.

I would like to actually connect the last two things you guys have said. You mentioned the Conficker Working Group, and, Colonel, you mentioned confidence in techies. It's my view that over the past couple of decades, it has been the private community, rather than the private industry or public sector, that have done a lot to protect the Internet itself, as an infrastructure, a global infrastructure, which is one thing we keep ignoring in a way. It's not just one country.

My view has been that people get things done and then new people come on the block and they use two terminologies: number one, more cooperation; number two, information sharing. That's how you know they're new. [Laughter] Sorry. Am I being rude? I'm Israeli. I apologize. And then they basically start over and try to ruin what the private community versus industry got started and say, "Let's do it." Then it takes us a while to get started again. So that's just throwing it out there.

But my actual question is on the idea of the panel itself, attacking back, let's call it that way. Looking at attacking back, first of all, I was In Estonia in 2007, when one of the major events occurred that led to where we are today, I believe. I was there and I helped write the post mortem on all those attacks. There are many, many things that became clear back then.

The two things that became clear are: number one, the Internet is global. I know it sounds so simple—the Internet is global. But it is, and it has an infrastructure of its own. As much as we try to define critical infrastructure, in Estonia, when communication to the banks was blocked from outside, it wasn't actually blocked. Communication was allowed only from within Estonia to reach the banks—then bots located inside Estonia started attacking, only then.

So blocking parts of the Internet, trying to do something on the policy level—that's not how the Internet works. You can always reach places. You can always do things. That doesn't really work out.

Now, if we are to connect this with three things: number one, the infrastructure is global; number two, on the policy level we may encounter laws, such as data protection and privacy—if we try to hack back and we get some information on a private citizen of Germany, oh my God, that will be incredibly difficult for us. And if we try to hack back and we have the wrong person, are we seriously talking about deterrence? We hack the wrong person and they actually do go to a court of law to get us. These are all policy questions that we have no answers for. And we need our lawyers to tell us no and then do it anyway. You keep saying "ask the lawyers early," and they will tell us no, and then we'll do it anyway. That's a risk management issue.

Connecting this to the technical question, how do we actually do this? Because people are not waiting for ethics; people are hacking back. That has been going on for a while and we can say, "No, that's wrong and we'll not stand for it," and then two years later we'll say, "Yes, we want to help you." What do we actually do today technically that will enable us to hack back, if we even should?

GREGORY CONTI: As background, Gadi is an internationally recognized researcher in this space. He is brought in to troubleshoot major problems. It's a pleasure to have you here.

CHRIS ROULAND: Gadi, first of all, I'm a big fan of your work, and I am glad you're here and asking hard questions.

At the end of the day, in this country it's illegal to hack back. But, technically, we are starting to see a new brand of startups bridge the gap of active defense. So let's make things sticky. Let's collect some intel and some attribution data so we can track these guys. I think there are some search engine companies that are doing a good job at this, and other innovative startups that are saying, "Hey, let's put out some fake data, let's put out data with tags in it, let it phone home"—not necessarily dropping zero days on targets that may or may not be correct. This sticky factor in between of a next-gen honey pot, if you will, I think will be the first legitimate active defense technology.

Going forward, though, I do think eventually we need to enable corporations in this country to be able to fight back at some level. My high-level take on that from a policy perspective is that when I hit the big red button, nothing happens.

So let's take your metaphor of your lawn mower. But let's say it's $10 million in gold bullion of yours, and you call 911 and they don't call you back for a week. When do you go get it? For me it's probably that night. Maybe, after they turn the lights off and go to sleep, I'd probably go get it, if the police won't call me back. That's, I think, a realistic metaphor to where corporations are today, which is they're losing and bleeding out millions of dollars. Maybe it's their fault; maybe it's not. However, it's so challenging for law enforcement and government to help with that. I think we've got to enable them themselves.

ROBERT CLARK: So Chris comes to me and he says, "My research and development has been hit. In the logs, we saw our information go out. It's on an FTP server over here that belongs to—we all know who, wiseguys.com. We don't know what their aspect is.

I say, "Is it an anonymous FTP server?"

He goes, "Yes, it's an anonymous FTP server."

"Okay, self defense, a place I have a right to be. Can you log into it as anybody in the world?"

"Yes, I can."

"All right, go log into it, because if anybody can do it and your data's on there and anybody can do that, you haven't broken any laws. You're where you're supposed to be."

So I ask Chris, "Okay, how is that set up?"

He goes, "Well, there's a file tree in here and it's in this file right here."

I'm like, "Okay, great. That's our data, right? You can download it?"

"Yeah, I can download it."

"Okay, great. Can you upload something?"

"Yeah, I can upload something."

"All right, so you download it. Can you delete that file?"

"No. On an anonymous FTP server do you typically have rights to delete data that's on there?"

"No."

Now, at that point in time this is the most asinine thing I can think of. It's my data, it's there, I should be able to delete it.

Now, on the argument, I haven't even damaged their server. I've created more space for them to put more on the FTP. So actually he's improving the system. [Laughter] As his lawyer, that's what I'm going to say, as they're leading him off in handcuffs. And I get my steak dinner.

So if you're in a place you have to be—now, the next part. It's not an anonymous FTP server.

"Well, how do you know what the log-in is on it?"

"It was in my logs. I saw it come in."

Now, under the third party doctrine that the government is so famous for using—*Smith v. Maryland* is the case—in which phone numbers were exposed to a third party, the telephone company, that information was exposed to me. I'm a third party. Arguably, I could use that to log in and go get my data.

So from that part I'm not damaging their system. I'm getting my stuff back, my gold bullion that was stolen from that aspect of it. I don't see huge harm there.

But I'm not going to sit here as a lawyer and say, "Technically, when you delete that data, again you are doing something that you don't have authority to do. You're exceeding your authority, which under the Computer Fraud and Abuse Act is technically a crime." But that's an aspect of being able to go and get your data back. So that's an active defense part of it.

Now, if it's an innocent third party, yeah, you can always pick up the phone and say, "Hey, do you know your FTP server is being used as everybody's intellectual property?" They might say, "No." You

might coordinate with them to actually put a monitor on there to see who's doing what and where and run your own self.

But you've got to remember what the DoJ wants. For a necessity defense, you must exhaust all remedies; which means law enforcement, you've called them, coordinate with them; and lawsuits, you do a civilian lawsuit, which again is back to your point. Seriously, I'm going to watch my gold bullion go away and I'm going to be in court five years from now and I'm not going to see dollar one on it.

CHRIS ROULAND: I think that's a good working example, caveated by the new normal, which is someone just posted var/spool/mail, your entire corporation's email spool, on Twitter and it's on BitTorrent. This means now there are 1,000 copies of it out there and now 100 million people know where to get it.

A couple years ago, yeah, it might be dropped on an FTP server here and here. Now it's, boom, Tweet, Torrent link, 100,000 copies of it. You're never getting it back. And this came up.

GREGORY CONTI: And the company may not be a company anymore.

CHRIS ROULAND: Your company may be gone.

ROBERT CLARK: But, real fast, when we're talking about the other aspect of tagging and sending beacons, DoJ's position still on that is putting beacons in your documents, believe it or not, is still illegal for you to do. It's a stupid technicality.

GREGORY CONTI: Can you explain beaconing?

ROBERT CLARK: The beacon is I put a tag in my document so that when it gets stolen and, if you're dumb enough to open it on the Internet, it will come back and tell me where it was opened.

But the other thing that people are saying is, "Okay, I'm going to set up a honey pot with a bunch of fake documents, deceptions on here." My favorite part of being in New York is the SEC, Security and Exchange Commission. Because what if my documents that are on there are fake mergers and acquisitions with real third parties? If I put crap on there no one's going to steal it, so I've got to make it look real. It gets stolen and then it gets leaked.

Now, I didn't disclose it, I didn't put it out there. But when that hits the media, who do you think is going to be knocking on my door? It's going to be the SEC: "Hey, we're here to investigate you."

"But that's not mine."

But I'm telling you right now, you go talk to your lawyers about that one. They're going to say, "No, don't think so" on that. So that's one aspect of this active defense and deception and the whole thing.

JENNIFER OTTERSON MOLLICK: Chris, earlier you mentioned that companies need to be enabled to hack back. So I'd like to ask a very general question of the panel.

First, do you believe the law is outdated? Are we dealing with laws and precedents that have not caught up with technology?

Secondly, if the legislation does need to be updated, if you believe so, what will cause that to happen? Are we talking about a catastrophic event, or are there going to be these losses every day

that finally build up to enough to cause a change in policy?

CHRIS ROULAND: I'm not an attorney, but I'm actually the first person in my family in about two centuries who's not, so I have a little bit of experience with them. But I do love to rip them a little bit. So I'll say if you're paying by the hour you can get someone to interpret a law from 1899 and make it applicable today.

But, realistically, I think that the technology has moved too much since the law of armed conflict. We have some old legislation on the books and old concepts that we're trying to apply to radically new technology and privacy issues that we just need to take a fresh look at.

I think you actually have to deal with the privacy and the network defense and active defense all at once, because they really fall into the same bucket. You can't ask your government to defend you but then complain that they're monitoring the traffic. Today, my understanding of those laws is they might not be entirely incompatible, but Bob is an expert on that.

ROBERT CLARK: So yes, no, and maybe.

Now, an interesting aspect. The private aspect we're all looking at is the Computer Fraud and Abuse Act. I am on the record as being the maverick in the international community, because the law of armed conflict, as far as I'm concerned, is as clear as it's going to get for the kinetic world and for the cyber world. The quote is, "there is no precise definition of an armed attack or use of force in the kinetic world and there's not one in the cyber world."

So we've been applying these same international law principles—the Lieber Code, from 1863. It goes back that far. So we have done that. Now, from the Computer Fraud and Abuse Act, statutes are written very generally because we don't want to make them so specific that when new technology comes along it's now obsolete and I can't apply it. We allow implementing regulations and court judicial decisions to interpret those things.

With that said, yes, the heavy lifting has to be put in place for a digital self-defense amendment to the Computer Fraud and Abuse Act. I may be in so much trouble now that I just said that.

You said, "What's going to take that? Where's the lobbying group that's going to invest the money to do the heavy lifting to get that written from that aspect?"

Now, why doesn't legislation come out? There's 19 separate committees in the House alone that have their hands in anything with the word "cyber" in it. The Intelligence Committee just passed a modification because they wrote it so narrowly. Theirs was the only committee that had anything to do. No markups with any of the committees. It was pigeonholed right in that one committee.

With 19 committees in there, what do you think is the odds that legislation is going to move forward, with the wonderful, swell Congress that we have working so swimmingly together? [Laughter]

CHRIS ROULAND: I would add that what you're describing brings to mind the military concept —actually, it emerged from the fighter pilot community of OODA loops (observe, orient, decide, and act). So the two pilots, they're both going through these loops trying to observe, orient, decide, and act. The one that does it faster can disrupt the other one.

So we've got adversaries, in my opinion, who are very agile. They're not constrained by things like laws in many ways, and they're able to evolve the technology and their techniques, tactics, and

procedures very rapidly. And then we have the law and policy and large bureaucracies trying to keep up with that. So it's definitely a challenge.

PARTICIPANT: Eric Joyce, Madison Policy Forum.

Chris, this question's for you, and then it gets into some things that I'd like to hear Bob's thoughts on it. And please, Greg, feel free to chip in as well.

You talked a lot today about increasing risk to the attacker. Could you explain the concept of increasing digital risk? Who should do it, how should they do it, when should they do it, and what is the risk of actually then increasing the risk?

And then, Bob, this is for you. How do you increase the digital risk but ensure proportionality, so given the concept of law of armed conflict?

CHRIS ROULAND: I use that in the concept of creating risk and consequences for an attacker. So the consequence could be to go to jail.

Increasing risk could be if we know a specific nation-state is advocating launching denial-of-service attacks against Estonia or Wall Street, we cut their cable, or put a denial-of-service back on them and create a deterrent in cyberspace, which I don't think there is today.

In the traditional Cold War, there was deterrence, right? Someone fielded a missile, then a bomber came out of a bunker in Poland. When the bomber went back in that bunker in Poland, then the missiles came down.

There is no concept of deterrence today, really, in cyber that I'm aware of, because it's this global free fire zone.

PARTICIPANT: Who should be the driver of that deterrence?

CHRIS ROULAND: I'm a simple government guy. I think the government should control lethality, taxation, and legislation. This falls under lethality in cyberspace, if you will. So the government needs to either call the ball on that or, as I talked about the concept of some kind of cyber guard, have individuals that are enabled in the private sector to do so. But the concept of deterrence in cyber space, I think, needs to at least be approved by the government.

PARTICIPANT: What does that look like from a digital perspective?

CHRIS ROULAND: It could be cutting a cable into a country or a corporation. It could be a denial-of-service attack. It could be some other economic impact.

PARTICIPANT: Would that, Bob, have to be proportional?

ROBERT CLARK: Let me start with the cyber deterrence piece. The MAD aspect, or the mutual assured destruction, that's kind of where my brain went to also. It's that aspect of, "If you're going to hit me with cyber, I'm going to hit you, and we're all going to be back with that mutual assured destruction."

But the smart minds that are writing on this are saying, "No, no, no, that's not good. It won't work." The stuff that they're writing—I'll be honest, I'm a kind of monosyllabic guy, which is that's the largest word that I will use; I really like small words. The stuff that they write on this, I'm going to sleep on it

immediately. So I haven't read a really good cyber deterrent.

In Sanger's book, *Confront and Conceal*, when he was talking about Stuxnet when it became public, he says there were discussions that were saying, "What's wrong with it becoming public?" What if the United States signed Sanger's book, saying "Dear Iran; Love, the United States"? What's bad about that? It's a deterrence aspect.

You're spot on as far as both the self defense for a private company and law of armed conflict. Distinction, targeting, proportionality—you can't cause superfluous injury, and you can't use an indiscriminate weapon.

So as far as shooting back, Colonel Brown, who was the Air Force staff judge advocate of its Cyber Command when Stuxnet came out, called that thing, in a personal capacity, a model of responsibility. Clearly, lawyers were involved, because that thing was surgically specific, looking for Siemens with two specific PLC drivers on there. You can't get more specific than that. That's better than dropping a 2,000-pound bomb on it. That's a deterrent piece.

Hey, our international strategy has simply said, "We will respond to a cyber attack using any means and methods necessary—diplomatically, kinetically, or with cyber." We put that policy out there that we will stand there.

What is it? How is it going to be done? Fortunately, from what I understand, we haven't got there yet on that. But you're spot-on that it's got to be proportional.

If you're an active defense kind of thing, what do you need to do? Do I just need to get my documents back and delete them off the FTP server, which is an old scenario that I can't do now because copies have been made? Or do I know who the company is that took that, and now I'm going to go to my offshore guys?

PARTICIPANT: Simply given how hard it is to attribute and the timing it takes, if you're the government, you're a lot better at it.

ROBERT CLARK: I don't know. I love my techies. That's the part where we go to conferences and we talk to them. It's like, "What can you do?" No one's going to come forward and say, "Hey, we've got a great attribution. We're going after—" But I've got to believe—I'm hoping—these guys and gals are good and that they can get some attribution.

PARTICIPANT: I think there are a lot of fields in which there is some difficulty understanding people who are specialists in the field and there's a lot of specialized vocabulary. But it seems to me that cybersecurity is one that is especially difficult to have an open discourse about with a broad community.

As we are trying to develop new policy and new legislature and have an open, wide discussion about the ethics that surrounds these new tools that we have and these new ways that we can be attacking other nations, so it deals with both private sector and national security, where do you think the responsibility lies? Do you talk to people like me, who may not have very much background in this field, and say, "I wish you were better educated on these concepts"? Or do you think, "Well, we could be doing a better job at having public education around them so that we can have this open debate about public/private partnerships and hacking back"?

And how do we get there as a society so that we're having these open conversations and deciding

where our values are in this space?

CHRIS ROULAND: I think from a cybersecurity perspective that, as an inside cybersecurity guy, these guys kind of look at it as the techies in cybersecurity and then the kind of civilians out there. We could have a conversation all day long not using a single word in the English language, just using acronyms, and it would seem natural.

So I don't know that education is necessary, more than you need to know how a specific medication kills a specific disease, how deep you go into that, other than the fact that the medication is tested, it works, and it's approved. I think there needs to be continuing education of threats against individuals and consumers. But I don't think there's a massive education initiative that needs to take place.

PARTICIPANT: I'd argue a little on that because I think that there has been a lot of civilian education around animal testing and other biological research issues. So maybe just to go with your analogy, there is something that could happen.

CHRIS ROULAND: On the flip side, one thing I was excited about are programs like Colonel Conti's and at the Naval Academy, where cybersecurity is mandatory in obtaining a degree from those institutions. And perhaps cybersecurity needs to be on every undergraduate program to some extent, to operate as an informed citizen on the network. So from that perspective I can see where you're coming from.

ROBERT CLARK: That's part of it. They say, "When are we going to get there?" and they say, "It's going to take a generation," because the generation that's behind us, they're going to grow up with it, and so they're going to be more technologically aware and need to secure it.

So I think that's part of it where, yes, we need to continue having these discussions and explain what it is and what the responsibilities are.

We always used to say in the Army that we had to qualify with our rifle two times a year, but we did five-minute information security training on a computer and that was it. So there's that part.

The part that really has me surprised is the Snowden thing. In the podcasts I listen to, everybody says when they bring up one of these stories, "Okay, there's another one." Are we just kind of getting immune to it?

You know, back in the 1970s when this happened, we had the Church Committee, chaired by Senator Frank Church, that looked into our intelligence things. Congress held committees on this. I'm not hearing anything of that.

So you want to talk about an education piece? I'm kind of shocked that the public is not crying for congressional hearings into that aspect of it. We're just kind of going over the privacy and civil liberties from that part of it.

So I think there's a lot that education can move forward on that. But I think it's going to be a generational shift. Hopefully, our kids coming forward, who have the iPhone in their hands, immediately start getting into the aspect of, "I've got to secure these things a lot better and understand—not the ones and the zeroes, but the steps I need to take so I'm not clicking on a cute little kitty and letting viruses come into my box."

GREGORY CONTI: I'm a teacher by day. We have 1,000 students a year we graduate from West

Point. Every one of them has to take two information technology classes. So we look at the context of all, every graduate. We're trying to, across the disciplines—from psychology, to history, to mathematics—to include enough cybersecurity to provide every graduate with a foundation.

And then, for the people who specialize in it, one of our core underlying principles is the ability to communicate technical subjects to a nontechnical audience. That is one of five of our core principles. So it's something that we and other technology programs across the country are trying to do.

With that, we are in the final glide path here. In a moment, I'll be asking our two panelists for about a concluding remark.

What I took away is that the Internet is a global free fire zone and that we need to conduct due diligence in protecting our assets first before we even consider things like hacking back.

That hacking back is happening today, both in the United States and offshore.

That policy, technology, and other approaches to attack the incentives of the attackers themselves, the adversaries, that increase the risk, increase the cost, can help defer the problem.There was mixed feedback from the audience on whether this was a good thing or not.

So that's my takeaways.

Mr. Clark, you're on.

ROBERT CLARK: It's a challenging topic, one we need to continue discussing.

Years ago, one of my first bosses, a staff judge advocate, gave me a Constitution. I keep it right on my desk.

The nice thing about being a government lawyer is I get to do the right thing. The Constitution and you are my client from that aspect. So at the end of the day, they say, "Make sure you're doing the right thing."

The Constitution is great. We have laws on the books for what we can and cannot do. When those laws are hampering what we are trying to do, then somebody's got to do the heavy lifting to get the modifications, to say, "We need to change this so we can do this." In the active defense realm, that's where we're at. That's where the heavy lifting has to be done, to put in a provision for a digital self-defense.

We ask: Is it going to take some kind of a large event to have that happen? Yes, I think so. I think it's going to require a very large event where everyone is going to say, "If I could have called Chris in and we could have stopped this—but I wasn't legally capable to do that." I think that's kind of the status for where we're at today.

CHRIS ROULAND: I found this a thoughtful, educational panel for myself, and it was interesting preparing for it. I enjoyed your remarks, Bob, and the good audience questions.

My takeaway is that—this is another Hayden quote; he just used it recently—"it is the Wild West and everyone has a gun, and there is no sheriff and there is no cavalry coming." Those are all appropriate metaphors for the situation we're in today.

However, we don't want everybody just making up the law as they go along and shooting each other.

So I think, from a technology perspective, investment in innovation and active defense and attribution, without actually crossing that line of the Computer Crimes Act and breaking the law, but while collecting as much information and to encourage government and commercial partnership in a post-leaks era—because I kind of put Snowden and Manning in a bucket together—the new normal is leaks. Once you're compromised, look on BitTorrent for all your secrets.

But I think the technology community has a ways to go to innovate and succeed in helping provide new tools to commercial customers to help defend themselves in a more active fashion.

GREGORY CONTI: With that, I'd like to thank everyone for coming and turn it over to Jennifer.

JENNIFER OTTERSON MOLLICK: I'd like to thank Colonel Conti, for providing an excellent moderating job; and Mr. Clark and Mr. Rouland, for joining us today. I'd also like to thank Lieutenant Colonel John Brickey and our CNL Miro Vassilev for putting together today's panel.

Thank you.

Audio

The Internet is "a global free fire zone," yet it is illegal for companies to hack back against cyber attacks--although rumor has it that many are doing so. How much of the responsibility to protect their assets should rest with the private sector and how much with the government? This expert panel explores these difficult legal and ethical questions.

Video Clip

The Internet is "a global free fire zone," yet it is illegal for companies to hack back against cyber attacks--although rumor has it that many are doing so. How much of the responsibility to protect their assets should rest with the private sector and how much with the government? This expert panel explores these difficult legal and ethical questions.

Read More: Corporations, Justice, Business, Collective Security, Global Governance, International Law, New Media, Private Sector Development/Corporate, Technology, Global, China, Iran, United States