American University National Security Law Brief

Volume 3 | Issue 1 Article 5

2012

Fall Cyberwar Symposium Panel 1: When Is a Virus a War Crime - Targetability and Collateral Damage Under The Law of Armed Conflict

American University National Security Law Brief

FALL CYBERWAR SYMPOSIUM PANEL 1: WHEN IS A VIRUS A WAR CRIME - TARGETABILITY AND COLLATERAL DAMAGE UNDER THE LAW OF ARMED CONFLICT

BEKA FEATHERS (American University International Law Review Symposium Editor): It is my pleasure to introduce our introductory remarks by Professor Kenneth Anderson. As you all know, he is a professor of law here at the Washington College of Law. He writes extensively for Law Fair on various issues in international law and national security and is also on the advisory board for the National Security Law Brief. We're very happy to have him, and so, without further adieu, Professor Anderson.

PROFESSOR ANDERSON: Thank you and I'm going to also be very brief in order to get us on to the panel. I think actually most of you know me here, if you are students, as a corporate law professor. And in fact, I look across the room and I see various people in my business law classes.
I actually have a very split personality between this sort of national security side and the corporate side. And in general, I guess, I would say that I'm interested in money and violence.

This particular conference I would like, first of all, to welcome everybody and I would like to thank the two student organizations that have put this together because when I looked at the lineup for this and had been invited just to deliver these brief opening remarks, it caused me to actually go and change a talk that I was supposed to give someplace else until next week because I thought these are absolutely just fabulous panels.

Let me say why I think the organization of this conference is exactly spot on for how we need to start addressing the cyber issues. This is the first of really three points that I just want to make substantively by way of introduction to the day. The first is that the two panels this morning address the international law side. And in the afternoon, ask, I think – and under "ask," questioned in all of this – whether and to what extent it's possible for domestic law to be able to address these questions. And I think that that's actually an under-discussed aspect of this when it comes to the questions, not only of the sort of all the domestic issues that we've been talking about – privacy and surveillance and other kinds of stuff in the cyber area – but including the questions of thresholds of war, other kinds of responses, the way in which one has to see an array of responses, some of which are essentially driven by concerns out of international law, but others of which, perhaps, are really driven by paradigms of domestic law.

So I think that that actually frames the question in a very important way, and I would stress that I think that it's actually under-asked in a lot of the circles here.

The second point that I want to make about these things is to locate cyber warfare, or let's say cyber operations because I don't want to actually suggest that everything is war. I mean we do it that way colloquially and I think that it's fine, but to be more precise, we just want to say cyber operations that may be characterized legally in one way or another.

Cyber is not the only emerging new military technology out there. So, as we think about the emerging technologies, we think about cyber, but we also wind up thinking, of course, about drones and remotely piloted vehicles as we are aware of them, but also the next couple of generations of what this technology will look like. This is going to wind up ranging from the things that get smaller and smaller in this kind of technological development. Meanwhile, some things get bigger, so you can have things that are fairly gigantic circling around doing surveillance at a very large level. Other aspects of the way in which these technologies wind up developing are still rooted around some notion of being remotely piloted.

And then finally, this technology will become more diffuse because it runs across different kinds of actual weapons in the general trend of military affairs but also because it's in everything else in terms of innovation and the economy and technology. This general trend is towards automation: the automating of systems, perhaps even leading to something that we would describe as fully autonomous systems. Systems that are able to, in effect, go beyond a set programming in order to actually make decisions that are not themselves fully predictable in advance, according to a rigid machine programming.

That's the direction that an awful lot of stuff is headed at this point, and it will have impacts on lots of different things in the military because it's going to have impacts on, for example, weapons systems. Should we ever wind up reaching the point of fully automating the decision to fire a weapon? It will wind up impacting not just the weapons themselves but also the platforms used in drones or other kinds of weapons systems.

We normally think about things that fly around, but remember the driverless cars that Google is driving all over San Francisco for hundreds of thousands of hours at this point - without a crash, by the way? First of all, the engineers and the basis for that driverless car get going in military research and development programs. We tend to assume that because it's Google, it can't possibly be evil or frankly ever raise any sort of ethical questions, but the reality is that many of the technologies involved in driverless cars have enormously important applications in military technologies, as well. And the driverless cars themselves, they're actually grounded in DARPA research. That is going to obviously transform civilian transportation. Drones are going to transform civilian aviation, if not general aviation, and in that process of automation, these things are going to be actually relatively small parts – i.e., the military parts will relatively small parts of much larger transformations towards automation but are just part of the way the world is going to work. We eventually will be replaced by robots; get used to it.

Now, these three different trends – the trend towards automation, perhaps even autonomy in military affairs and specific technologies in drones, and specific technologies in the area of cyber – these things wind up having enormous differences between them. So, for example, cyber can be extraordinarily targeted, but when we talk about many of the fears, concerns, and risks – the things that cause governments to draw red lines in the sand and to say we will consider this an act of war, they are very often based not on account of the fact that cyber is discreetly targeted towards some very particular, narrow thing. On the contrary, it's because we're worried about massively indiscriminant effects on the civilian infrastructure. What's striking is those possibilities, and the fears of these possibilities tend to be one of the drivers for why we wind up talking about whether this might be considered an act of war.

Drone technology, on the other hand, is really very much about precision. The whole point about drone technology is to narrow the focus of the kinetic strike down to getting it as precise as possible. That would be a difference between these areas.

But one of the things that I think that is shared between these things, and again, looking sort of the larger picture and not just at cyber, is the extent to which these kinds of technologies enable, in the first place, remoteness, or the ability to attack from a distance, which itself is actually not new. I mean from the moment that somebody picked up a spear and went whoosh or somebody invented a bow and arrow and got behind a rock and said, "Hurray, I can kill you but you can't get close enough to me." From the moment that happened a long long time ago, we've been looking at ways in order to strike from remote distance, and these technologies, in a certain sense, are just carrying that to a sort of logical further extreme.

But they also, to some degree, greater or lesser, wind up making it more difficult to identify who's launching the attack. So it's not just a question of remoteness, it's also a question of the ability to attribute attacks to a particular party. And that has the possibility, at least depending on how true that is, of using the drone, and maybe obliterating it or flying it out of the zone or doing something with it that gets rid of it, and simply blandly denying that you had anything to do with the killing that took place. And can that possibility be very destabilizing in terms of international relations in regard to war and peace because you can't so definitively say who did the killing? Who do you attribute the attack to? Who do you retaliate against? Who do you hold responsible?
Cyber has also, and if anything, been seen as the most scary in the lack of attribution problem although – and I think the panelists will perhaps address this – it is perhaps less of one than might have been thought.

Those are areas in which one looks across different kinds of military applications of emerging technologies to see commonalities. And my only point here is to wind up locating cyber within this sort of larger picture, [as a type of emerging military technology]. Again, I want to congratulate our student organizations for putting on a spectacular panel, and also to thank the panelists today and in the afternoon for being here for that.

So I'm going to turn it over to the panel and thank you all for being here.

DAN SCHNEIDER: Thank you Ken. My name is Dan Schneider. I'm a Professor at the School of International Service at AU and Director of our Center on Non-Traditional Threats and Corruption. What's a non-traditional threat? Well, what we're going to be talking about today is a perfect example of a non-traditional threat.

I'm essentially going to get out of the way. How we'll proceed today is each of the panelists will speak for about ten minutes, and then we're going to open up to questions. Let me introduce each of the panelists. I won't go through all of their accomplishments because then that wouldn't leave any time for them to talk, but we have a really incredible panel here today. So let me just give you some of their highlights.

Starting with Chuck Barry in the middle here. He's a Senior Fellow at the Center for Technology and National Security Policy at the National Defense University here in Washington. He has conducted research on defense related network integration and security for the past ten years with a special emphasis on NATO network defense against cyber attacks. He was a visiting fellow at the Woodrow Wilson Center from 2004 – 2006. He's also a retired career soldier with combat experience both as an infantry soldier and as a helicopter pilot. I would love to hear about that in another forum. He served for 12 years overseas – Africa, Central America, Asia, and Europe.

To my immediate left, Greg McNeil, from Pepperdine. Greg is Associate Professor of Law at Pepperdine where he specifically focuses on national security issues, transnational crime and international affairs. He has recently testified before Congress regarding cyber terrorism. He's advised members of Congress during the development of cyber security legislation, and recently served as an expert commentator and assisted the military in their development of two manuals aimed at preventing harm to civilians in warfare. Previously, he was co-director of a transnational counterterrorism program for the U. S. Department of Justice, my former employer. He's also a contributor to Forbes magazine. His current research includes an article entitled, "Kill-Lists and Accountability," and a book about the investigation and prosecution of national security related crimes, which will be published by Oxford University Press. Professor McNeil also served as an officer in the United States Army.

Last, but not least, is Paul Rosenzweig, who is a Professorial Lecturer at George Washington University School of Law. He's also the founder of Red Ranch Law and Consulting. He formerly served as the Deputy Assistant Secretary for Policy in the Department of Homeland Security just down the road. And twice he was Acting Assistant Secretary for International Affairs at DHS. In these positions, he was responsible for developing policy, strategic plans, and international approaches – the entire gamut of Homeland Security activities. He's a graduate of the University of Chicago Law School and is co-author of the book, *Winning the Law on War: Lessons from the Cold War for Defeating Terrorism and Preserving Freedom*, and author of the forthcoming book, *Cyber Warfare, How Conflicts in Cyber Space are Challenging America and Changing the World*.

DAN SCHNEIDER: The topic of this morning's panel is When is a Virus a War Crime? Targetability and Collateral Damage Under the Law of Armed Conflict. Very briefly, the laws of armed conflict, as they develop may be over the past, since the 1860's or so, were designed when war was kinetic, energy driven; things blow up. Not designed because no one could have even conceived not only back in the 1860's, but even maybe 30 years ago about cyber warfare. These laws were designed during a very different era. But some of the main principles of the laws of war, think about them, are things like proportionality. You do not deliberately target.

One interesting provision of laws of conducting war is that soldiers wear uniforms so they can be identified and separate themselves from civilians so the other side knows who to target, who to attack. Well, the attribution problem is not nearly as severe as it used to be, to the surprise of many, but still the people initiating attacks are not wearing uniforms. So that's just some of the many things to be considered in the talk today.

We're going to proceed in alphabetical order. Each speaker will speak for about ten minutes. And then we're going to devote the rest of the time to questions from the audience. So we will start with Chuck. Chuck just realized he has to go first.

CHUCK BARRY: Thank you very much Dan and thank you to the Washington College of Law for inviting me here today. As you know from my bio, I'm not a legal expert and I'm also not a technician in cyber weapons or a user of cyber weapons. But I have spent a number of years, ten years about over at the National University as a student of the application of cyber in armed conflict, and that's kind of what I bring to you today, that experience. And also working, since 2009, in an international forum with the East-West Institute where we've been talking specifically to our Russian counterparts at the Moscow State University. And also counterparts in other countries, to include China, on how you might render the laws of armed conflict in cyber space.

And in the context of that, we've been wrestling with our counterparts in these various countries with how you might define things such as offensive capability, defensive capability, cyber attack, and things of that nature. And we have actually come to some agreement realizing that this is just a couple of groups of Americans and interested Russians. At the same time, we realize that our counterparts are very closely connected in the Kremlin and we ourselves are wholly owned subsidiary of the Department of Defense. So there is some inside or a possibility that this is the beginnings of discussion.

The other thing that's encouraging I think about this idea of cyber warfare being subject to the laws of armed conflicts is that the laws themselves, as Dan was pointing out, began about a century and a half ago. They started out with land warfare. They migrated in to the naval environment. Later on there was the arrival of air power and much more recently space and now finding cyber space. So they have been able to adapt over this long period of time to the point where you have a rather large body of law.

A caution is that even those laws that we have today are not so precise or cut and dry, for example, the idea of proportionality basically says that there can be some incidental civilian loss of life or injury or damage to civilian objects, but it cannot be excesses to the military purpose. Well those types of things, particularly here in the law school, I'm sure you can realize that there is room for a lot of interpretation there. So we have both some encouraging things and some things to keep in mind.

The groups that I've been working with include combat veterans, not only on our American side, but also in some of these other countries, including Russia. So the bias of our group, I would suggest, is probably more towards the pragmatic application realizing that in some complex and sometimes extreme circumstances, it's very hard for practitioners to apply this. But there's a lot of technology that's working in this direction.

Some officials, most recently perhaps Secretary Panetta, have pointed out that indeed there could be a cyber Pearl Harbor. Madeline Albright pointed out in 2010, in leading the group of government experts in the discussion of the future of the NATO Alliance, that indeed some Article 5, that is to say, justification for a response against a territorial threat, could emanate from cyberspace. So we can foresee that in the future this might happen.

At the same time, pragmatically speaking, nothing has risen to this level to date to include, for example, the attack in Estonia, which was actually very harmful to them, but was very limited. Over a few weeks, a few very important websites, I believe in those attacks, were attacked in not a continuous, but rather a sporadic manner.

We have to understand things like Titan Rain, the attack against our own major defense contractors for secrets and things like the most significant attack in 2008 against the Department of Defense known as Buckshot Yankee. It is important to understand things of this nature and to not allow them to cause us to say, "Well we're in an armed conflict." We also need to understand the recent issue of Stuxnet in Iran as well as the more recent Shamoon Virus attack against energy companies, which have not triggered armed conflicts.

So what are the events that we might foresee that would trigger the application of the laws of armed conflict - *Jus ad bellum?* what would constitute a response in self-defense? Well, we have to theorize about this just yet, and we would suggest that if a cyber event resulted in significant losses of life, the same principles that apply to other attacks – destruction of property, extensive destruction of the way of life of a country or its ability to maintain its prosperity – apply. These are the kinds of things that we can look for, and I would suggest to you that we probably will not see. As for its future, we won't know. But we probably would not expect to see a purely cyber war because what that would suggest is that I will leave on the table all my other capabilities in the other domains. And if my national interests are truly at risk, then that is not really the definition of a war.

We would expect to see cyber conducted in context of a broader kinetic war. And this is not unusual. If someone attacks from the land, then we might respond in the air already. So this kind of cross-domain kind of conflict is there.

The other thing to realize is there's a – and over at the National Defense University we talk about this a lot because we have our military students there – close relationship between the electronic warfare and the cyber domain, which is clearly distinct today. But electronic warfare goes back to the days of cutting telegraph wires in the civil war. And we've had electronic warfare measures and countermeasures for many decades. They're a major component of any military plan.

And at the same time, today's weapons, almost every single weapon, every missile hanging out on the wing of an aircraft, virtually almost every weapon that even a soldier wears has a cyber component; something that can be disturbed in cyberspace. So these things will migrate together. The important piece as we talk about targetability is to target the military objects and not the civilian objects.

Attribution is – and it was mentioned already by Ken, but I'll just touch on it briefly – becoming easier. And I would submit to you that even on the day of December 7, 1941 when the Japanese fleet attacked Pearl Harbor, we didn't need perfect intelligence to know that this was not some renegade Admiral. We immediately knew that Japan was behind the attacks.

The attribution is never perfect. It need not be beyond a reasonable doubt. Part of the issues in cyberspace is who could be the attacker, who stands to benefit, who has the wherewithal to do these things? But once you get to this situation and you have an armed conflict, probably more evident in the other domains, then you become subject to these rules of *jus in bello*, and we have to think about three major pieces of that. One is the distinction we cannot attack civilian targets, but the other is that we can attack military targets. This is why we have things such as red crosses on ambulances and Medi-Vac helicopters and hospitals.

The next point is that we cannot be indiscriminate and this is a particular issue in cyberspace because you cannot use a weapon that you do not have good reasonable possibilities of directing it against a military target. You can't go indiscriminately to everything. This is an issue with viruses. We talked earlier about the issue of proportionality with incidental or how much civilian casualty might be inappropriate. This is particularly true today. We see this in the issue of drones. We can talk about that because there are a lot of other robotics on the battlefield to include autonomous undersea systems. In fact, a typical brigade in the field has some 300 robots now.

I'll just mention a problem here in tagging cyber, for example, on a medical database for a hospital that's conducting an operation, is how do you put that red cross on a database?

In our discussions with Russian colleagues in rendering of the laws of armed conflict, we made five recommendations. (These documents are available on the EastWest Institute's website.) We recommended that further international work be done on detangling protected entities, civilian entities, from military entities. Right now, the NATO headquarters is on the same power grids and servers and routers and switches as the local hospital and the airport and so forth. So we need to try and look at detanglement.

We suggested we look at getting the distinctive Geneva Convention's emblems rendered in cyberspace in some way – tagging on top-level domain names or things of this nature. We talked about recognizing both the rights and responsibilities of new non-state actors such as multi-national corporations or non-governmental organizations, and considered what are their responsibilities in cyber space. We talked about developing the Geneva Convention protocols further about cyber weapons. Some weapons, conventional weapons are prohibited, such as gas and certain types of projectiles, because they inflict undue suffering. So what cyber weapons fall in that category? And finally we talked about the possibility of another mode out here. Maybe because of this extensive espionage and so forth, we're not talking anymore about peace and war, but there's something in between that needs to be articulated.

Let me stop there and I look forward to your questions and the others.

DAN SCHNEIDER: Thank you Chuck.

GREG MCNEIL: Good morning everyone. So I'm thinking back now to one of my first experiences as an Army Officer. So I was actually a Signal Officer. I did communications when I was in the Army, and I was stationed in Korea. My first assignment as a 2LT Platoon Leader, I'm put in charge of 46 soldiers and 16 civilians who were responsible for basically all of the communications from a base called Camp Red Cloud north to the demilitarized zone. We had 10,000 military customers in 2nd Infantry Division, and my responsibility was to make sure that the secure network and the nonsecure network continued to function so that the war fighter could continue to be able to communicate.

At the time, I'm dating this girl. Her name was Melissa. And I get an e-mail in my inbox. Those of you who are tech geeks probably know where I'm taking this story. And the e-mail comes in my inbox and the subject line is – it's from Melissa – and the subject line is "I love you." And I'm thinking this is great. I miss you. I love you. She's home. She's in Pennsylvania, I'm in Korea. I can't wait to open this e-mail. So I open it and it immediately starts populating through my Outlook address book. The virus was the Melissa virus that was contained in the e-mail.

Now, not only is this like a stupid mistake for me, infrastructure-wise, it was pretty stupid that some 2LT straight out of the Officer Basic Course right out of college, 23-years old has an Outlook address book that has every single officer and civilian and NCO in Korea from the 4-Star General on down to the PFC who worked for me.

But in any case I opened it up and out starts flying 10,000 e-mails from my computer. So what I do…unplug my computer and sit and think for a second about how I'm going to fix my computer. And then I realize, holy crap; I'm responsible for all of these computers. Obviously I have a Company Commander, a bunch of people up the line above me whose head would roll before mine did.

What I do is I take off out of my office, which used to be an arms locker. So it was just a windowless safe, I've run out of my safe. I run to our bunker in the side of a mountain that wouldn't stop a bomb if it hit it, but it was cool because it was a bunker. Get in to the facility and I'm telling my NCOs, just unplug the computers because there was nothing else you could do. And so we did. We unplugged, I mean this is an hour and a half, two hours into this, and we unplugged the network. Effectively, an "I love you" virus shut down the NPR net and the SPR net for the northern third of the South Korean portion of the Korean Peninsula. That would be the way that we would send secure communication, and it was all through Microsoft Outlook e-mail, which we didn't have.

And so, now it was go back on phones and go back on radio communication until we could get the network back up and figure out then how to go through individual accounts cleaning out this virus so it wouldn't keep reperpetuating itself.

I mean imagine: you could still send e-mail. It wouldn't have been shut down if we hadn't unplugged it. Imagine you're the general and you have to sort through 10,000 e-mails from 10,000 people. Do that math and see how it keeps populating. How are you going to find the important message in there?

So it was a big deal for us. It was sort of emblematic of how some things small and silly can take advantage of [vulnerabilities] – and I don't think this was attributed to any nation state, I think it was just some, probably some 14-year old who was playing around on their computer and figured out how to make a really great virus that would mess with people and found this vulnerability and exploited it. But it shows how you can disrupt military operations.

Now would that be characterized as a cyber attack? You might be thinking, "Yeah. Definitely. I think that's probably a cyber attack. It disabled the military forces." That's one way of looking at it. Or you can just look at it as being annoying and all it required us to do was unplug this, get the new fix patch from Norton, and install it on our systems. I mean the military didn't figure out the fix. Norton Antivirus techs figured it out and posted it to the Symantec website.

Let me walk through a little bit of my sense of the law on this and in particular the law of targeting and how it helps to inform us of something about that type of attack and other types of cyber attacks; that type of operation and cyber attacks.

The question is whether the law of armed conflict provides sufficient guidance here. I'd say yes; Additional Protocol I, Article 49-1 defines an attack as "Acts of violence against the adversary whether in offense or defense." So the key issue in analyzing this provision, I think most scholars agree and most practitioners too, is the effect or the violent consequences directed at the target. And so we're looking at what the particular effect is and how we measure this or identify it as an attack, as an effect on persons, death or injury, and damage or destruction of property. So that's our threshold issue that we're looking for. Did cyber activity cause death, injury, damage or destruction to the adversary? That adversary could be a party to the conflict, their military forces. It could be civilians or civilian objects or civilian infrastructure. If we satisfy those criteria we can say that this maybe an attack under international law.

Now this is a little bit of a departure from what the current military doctrine is where that doctrine identifies cyber attacks as efforts to disrupt, deny, degrade or destroy an operation as a matter of military doctrine. That's an okay way to characterize this, but I don't think those two overlap completely. There are some areas in which they certainly do overlap. Thus, one of the immediate challenges associated with applying the law of armed conflict here. It's characterizing what is meant by "damage."

You might think that Melissa Virus I described caused damage, but I think there's a lot of room for us to disagree about whether or not there was some actual damage there. If you recall, you suggest that we look to death, injury, damage or destruction. The most difficult of these, then is to assess this damage. So cyber attack might merely change a line of code. It might start populating itself through the Outlook address book as I mentioned. And if one were to take a narrow view, we might look at this and only see the immediate effect of changing that code and perhaps causing a system to reset, a program to crash, an Outlook address book to start populating messages out. And so in the same way that one might foresee, let's say firing a bullet in to an electrical substation, will only take out that substation, we also have to assess what the cascading effects of that particular attack was. So if I only take a narrow view and look at that e-mail example I gave you, then it was a big hassle for the e-mail chain. But if that somehow caused other systems to shut down but then caused damage, then we might be able to characterize this as an attack and we might say that the cyber operator would be held to account for the reasonable foreseeable consequences and damage of their targeting decision.

The cascading effects are probably the easier effect. What if we're just going to look at the type of damage that we don't normally associate with armed conflict? Let's go back to my e-mail example or let's say that there's a cyber operation that just temporarily disables an enemy system. Could this be considered an armed attack? Let's think of a denial of service attack on a military web site.

On the one hand, Article 52 of the Additional Protocol tells us that only those objects would make an effective contribution to military action and whose total or partial destruction capture or neutralization offers a definite military advantage and only those targets may be attacked. And so if we're looking for neutralization we can read this broadly and say well neutralization of the web servers even temporarily could constitute an armed attack. In the denial of service attack on the defense website, assuming the website satisfied the effective contribution criteria, which we could have a big debate about. The fact that the DDS attack merely neutralized the web page probably doesn't fall outside the scope of armed conflict. That's one view.

On the other hand, as Professor Mike Schmidt of Naval War Colleges played it out, such an attack would merely be an inconvenience, and armed conflict is frequently inconvenient. The issue we have here is this [reasoning] skips part of the analysis.

Our threshold question is whether an attack is actually being conducted. Article 52-2 speaks to military objects. Defines them as "Those which may be attacked," and those are the objectives that only may be attacked in armed conflict. So looking at 52-2 to try and define for us whether an attack is going, skips our threshold question with regards to the damage provision.

In reality, our focus has to be what's being damaged and that will define for us whether or not this cyber operation rises to the level of an armed conflict. It doesn't mean that it doesn't further some other national goals, but if we want to trigger the law of armed conflict, we have to do so by looking to the scope of the damage that's occurred.

What we can do is start to lay down some clear markers. Operations causing damage to software that require repairs, damage to computer hardware, or other physical damage seem to rise to the level or a cyber attack. That's on one side. However, operations that merely cause inconvenience –the need to reboot, something that might delete nonessential information such as the server logs or history – doesn't make that deletion of that information rise to the level of a cyber attack. In other words, inconvenience doesn't count as an attack.

You can see the areas where this gets muddy. Professor Anderson alluded to some of the drone context. One of the things that anti-drone activists now are arguing is that we can also count as victims of drone strikes and drone surveillance those individuals who are experiential victims of the drones flying overhead. That is, I woke up every day, I saw a drone, and that emotionally traumatizes me. It's a stretch, and I think you can start to see some people trying to stretch the domain of cyber attacks for a variety of intergovernmental reasons. The more things are characterized as cyber attacks, the more money flows to cyber command to handle those issues and the less money flows out of DHS pockets. This is why a lot of this stuff is, I'd say, puffery on the parts of different agencies seeking to maximize their budgets and take control of certain issues. So we have to be careful to define cyber attacks appropriately here.

Now it's possible that you might have a denial of service attack that somehow takes out an anti-aircraft system. I'm not sure how that would happen, but if we thought about how we might have a cascading effect, it took out some computer systems or prevented those systems from operating, then – because there would be some clear damage to something that would contribute to the armed forces of the defender, the target being attacked – we might have crossed the line. But you can kind of see the boundaries that I'm hoping that will throw down.

This means that snooping and other types of intrusions, data theft, the type of stuff that you see frequently being talked about on the Homeland Security side and on the private side, denial of service attacks, many of these are not matters governed by the law of armed conflict and do not constitute cyber attacks. While those operations which cause death injury or destruction, I would say, do rise to the level of cyber attack.

Now merely characterizing these issues doesn't fully get us through the law of armed conflict analysis. We also have to apply the laws governing the targeting to the cyber context. And so some of this has already been mentioned, but obviously only combatants, civilians directly participating in hostilities, or military objectives may be targeted. This is the principle of distinction.

Now, it's possible that civilians will be impacted by cyber operations, particularly cyber operations designed to influence the population. We think of these as psychological operations or information operations in military terms. If those operations cross the line to threats meant to terrorize the civilian population, then we might have a law of armed conflict issue violation of Article 51-2. But the fact that this was a cyber operation doesn't change the analysis. We're looking at whether or not the operation was intended to terrorize the population.

Then we also have another step in our analysis, which is to take into account the cascading effects that I alluded to earlier because cyber operations generally have multiple orders of effect. [For instance,] an operation was conducted to take out a particular line of code in a computer system. The cyber attacker also has to take in to account the fact that there may be cascading effects from that.

Step 1. I might look at the attack whether or not the attack on the computer system itself was lawful. But then if I also want to implement my obligations with regard to the principle of proportionality, I also have to ask whether the second order effects – the incidental or collateral effects – will have impacted civilian objects.

Maybe I take out a computer system, which then shuts down a military electrical grid. Well if that military electrical grid is now somehow connected to the civilian electrical grid or connected to something else, which is then connected to the civilian electrical grid, I have to take steps to be sure that I'm accounting for those collateral effects in the conduct of my targeting. If there is any third, or fourth, or even tenth order effect, is that something that was reasonably knowable on the part of the attacker in that context? That's something that is going to require substantial effort on the part of the attacking party to make those types of determinations. Presuming there is such a third or fourth or even tenth order effect, it doesn't mean that I can't go forward with the cyber operation; I just have to weigh whether the damage is disproportionate when weighed against the concrete military advantage to be achieved.

The practical challenge here will be using all available information for the United States, all available information in the hands of the United States Government to determine the cascading effects. Just think of the 2002 blackout that took out Ohio, Pennsylvania, and New York City for five or six days in the summer time. It was caused by a branch that took out an electrical line somewhere in Ohio on a day of high capacity, and it shut down systems across the northeast for five days. Well if a branch can do that, then you similarly would expect that some shut down or overloading of a substation might do that and therefore you might have to take care to ensure that you're weighing all of those cascading effects in terms of analyzing the proportionality of your particular attack.

The law of [armed] conflict also deals with dual use objects. It defines those as, "those whose nature, location, and purpose reviews make an effective contribution to military action in the destruction of which offers a definite military advantage." Those are objects irrespective of the additional civilian uses which maybe attacked. The big problem here that we're going to start to see is that we have many networks and computer facilities, which host both civilian and military traffic. In the United States, more than half of the military traffic transmits commercial networks. Actually, it might be higher than that. I imagine Paul would know better than I would. And a substantial amount of storage is done on commercial servers.

Take Amazon Cloud services. A substantial portion of their business is to house military servers, even secure servers. An attack on that server facility is an attack on Amazon but also an attack on a military facility. This actually highlights part of the inner bureaucratic fight.

If I'm DHS I say, "It's Amazon. We own that. It's inside the United States. It's our area of responsibility and we need 10 million line items in the budget to be able to effectively respond to and deal with this." And if I'm DoD I say, "Yeah, okay, it's Amazon Cloud Services, but my SPRnet runs on that or my intelligence databases run on that." Therefore, all these targeting issues require a substantial intelligence effort for us to assess where attackers are going, whether or not we're dealing with a civilian object, a dual use object, or a purely military object meant to analyze the cascading effects.

PAUL ROSENZWEIG: HoneyCloud.net. has a map in real time of attacks that are happening right now in the world. It's but a small sample of what is happening because the Honey Cloud program is just a few reporters; not everybody. All the red [dots] are attacks. And the yellow ones are Honey Nets and Honey Pots where the malware is being captured.

So here's the question. Is that war? It's certainly a whole lot of activity. But what I would suggest to you is definitions of warfare are inadequate to the current state of affairs. I want to emphasize at the beginning that we're stuck with them because we're not going to build a whole new set of definitions, but we are in the process of pouring new wine into old bottles with limited success I would submit.

To just jump off of what Greg said in talking about an attack as being one that causes damage and destruction, the United States has attacked Iran, yet we're not at war. I would submit that we have not seen a cyber war. We will not see a standalone cyber war, and what we should be talking about is the use of cyber weaponry, cyber operations, and cyber tactics and whether or not they conform to acceptable rules of conduct.

Now again, I think that the existing sets of rules are ones that we're sort of stuck with, but in a lot of ways, they don't fit very well at all and eventually – I mean to put it in the legal terms that international law students will – we're going to develop another set of customary international practice that is completely different. We're going to try for the next five years to fit it in to the Geneva Conventions and the additional protocols and all that, and the international IHL and even International Human Rights Law, but we won't succeed.

So for example, this panel begins with the question can a virus be a war crime? I suppose I fight the question somewhat, but the answer is obvious. Of course it can be. But like almost any other weapon, it really is going to depend completely on the context in which it's used, how it's used, who it's used against, and when and why it's used for. My basic answer is in general, it's probably a lot less likely to ever be a war crime. Use of cyber weapons is less likely to ever be a war crime than a whole host of other kinetic weapons because they are inherently generally capable of greater precision and target-ability and therefore better able to meet current principles of distinction and proportionality.

That doesn't mean that bad actors won't use them in malevolent ways that are broad spectrum anymore that it doesn't mean that some bad actor might carpet bomb and entire country just because they're angry about a single intrusion. Or use them to commit genocide or anything like that. But cyber viruses are inherently program specific.

You think about Stuxnet. It's one that's in the public domain. That was a very precisely targeted virus. It wound up infecting a lot of computers, about 100,000 servers and hosts around the globe. But in so far as the public knows, and we can only go on that, only in one single system, in one single place, did it actually turn on and have adverse malicious effects. So that's a pretty good targetability. In fact, one of the questions that will come that is sort of inherent both in viruses and in drones is whether or not our increasing ability to do targetability more narrowly imposes on us greater obligations to avoid collateral damages and whether or not you get punished for being smarter because you have to start using more smarter narrowly targeted weapons. That's the type of discussion that we probably will have, but it isn't a discussion grounded in, in my judgment, the existing laws of armed conflict so much as in the inherent capabilities of the cyber domain.

Another area that is worth talking about where the laws of our conflict are, to my mind, sort of inadequate or failed to recognize the reality of where we are: it's the question of attribution. Both Chuck and Greg have mentioned that. I think that increasingly we're going to come to see two different types of attribution issues here. The way I think of it and the way I analogize for the law students is the difference between general deterrence and specific deterrence. We know of a certainty that China is hacking us beyond belief. There are dozens of hackers around. It is so much so that in any reasonable judgment, the Chinese denials of state responsibility are but the barest fig leaf.

Now there diplomatic reasons why we may want to continue to accept that fig leaf but that's another question altogether. If the question is can we conclusively attribute the ongoing espionage program to China, the answer, by any reasonable, beyond a reasonable doubt has to be "yes." The more specific narrower question is can we pick out five people or ten people who are responsible. Up until a couple of years ago, the answer was probably, but that's really hard. Increasingly, that too is becoming less difficult. Public reports suggest that the NSA has, through its magical means, identified 12 specific hacker groups within China who have responsibility for 90 percent of the economic espionage. Almost all of them have associated with Szechuan University, which has an information security program that is supposed to be or is likely to be a covert arm of the PLA. Thus, we know the groups, and we even know some of the people.

The New York Times actually called one of them up the other day and said, "Hello, are you the hacker, Scuhkr"…S-c-u-h-k-r was his name for Szechuan University Hacker and he was smart enough to notice a "No comment." So at least he knew a little bit about that.

The Georgians recently counterhacked a Russian. The Georgians actually identified a single hacker and downloaded the contents of his computer by counteracting. They larded a document with Honey Pot Document containing a malicious program that opened up his own browser. We got a screen shot capture of him looking quite surprised, and they downloaded the contents of his computer which gave evidence that he was taking directions from his local GRU – that's the Russian equivalent of MI 5 or MI6 – on what to hack for in Georgia.

We can attribute him. Now that leads to the next question. Which is all these people, everybody, they don't wear uniforms. This guy didn't. We're going to need a new category of combatants. That's the cyber combatant because they're not wearing uniforms. They're not playing the game by the Geneva Convention rules of carrying arms openly and that sort of stuff. But they aren't traditional civilians. The current traditional rules say the civilian is targetable only when he's actively engaged in the warlike activity. But as soon as he downs arms and goes home to his house, he no longer becomes a target. If he downs arms and goes home, he is immune from attack.

That maybe made sense when a guerrilla picked up arms, went to fight against the invading army and then went home to his house to his wife and kids. Now he fights from his home sitting at the computer next to his wife and kids. We need a new set of rules. Again, it seems to me kind of sterile to talk about existing categories of conflict when the right answers are that there are different rules.

I will end with two other examples that I think are perfectly good examples of why the old rules need to be re-thought. One is the principle of neutrality. World War I to a large degree was exacerbated by German invasion of Belgium and the violation of their neutrality. Yet, there is no way to conduct an effective cyber attack today without, in some sense, violating the principle of neutrality. Nobody in his or her right mind hops directly from the United States to China to conduct an attack. We always go through Malaysia or India, or Japan, or Belarus. So wherever it is we want to go through in order to try and mask our activity. All of those are probably, under current law, violations of the sovereign integrity of the country involved.

Now, we could try and reconfigure that and say, "No, it's more like radio waves going across the air waves. So it is not a violation." However, the truth of the matter is that Air Force and Justice Department attorneys actually think that we can't do that right now because the laws of armed conflict limit our activity. I think that that's probably the fair interpretation of the Geneva Convention rules to which I say okay; those rules don't fit anymore. We should be going about thinking about things.

DAN SCHNEIDER: Thank you. Let's line up for questions, and we'll take a couple at a time. While you're doing that since this is law school audience, I want to give a slight hypothetical; just like on a final exam where you walk us through the analysis. Let's take Stuxnet. You have an attribution issue – Israel and/or United States – but also the target, if you believe they're any, was a civilian target because they are maintaining that they are nuclear program. It's a civilian program being developed for peaceful, lawful purposes.

Under current laws of war, is that a war crime to deliberately target a civilian facility? Does anyone want to take a crack at that?

GREG MCNEIL: So if I start from the presumption that it's purely a civilian facility then yes, the attack on civilian on the facility, any civilian facilities, would be unlawful. If it's a military facility we don't have an issue. The question becomes the dual use facility and the nature of the dual use, and in which case we'd have to assess the proportionality.

If you tell me that millions of Iranians are without power and people are dying, it's like Staten Island a week ago but 100 times worse. Or even just Staten Island a week ago. And there's a causal connection between that action the attacker took and the resultant deaths. I have to balance that damage as against the concrete military advantage they anticipate to gain. The judge of that under Geneva Law is the reasonable commander in the circumstances or the reasonable attacker in the circumstances based on the information that they have available to them. And the only circumstance under which we'd see some form of accountability through like a war crimes tribunal would then force us in to the box of assessing whether or not the host state took reasonable efforts to discipline those individuals who acted despite some knowledge that these cascading effects will take place.

As for the United States, we're a country that takes pretty seriously disciplining individuals who violate the law, at least in our view. The war crimes accountability process would end if there was some evidence that we knew this was going to happen ahead of time and it was disproportionate. If it were a military member, there would be UCMJ process. That might not satisfy the international community who would look at this and say, "Well you know, you're violating your obligation to actually investigate and prosecute individuals," in which case they would want that an international tribunal exercise jurisdiction. But who that international tribunal would be, would be interesting because in the United States, there is not an intention to be party to the Rome statute. Then you would need a Security Council referral, and we would exercise a veto on the Security Council. In the end, the United States would be effectively unaccountable assuming that it knew this cascading effect was going to happen and that the attack would have disproportionate impact on the civilian population.

CHUCK BARRY: I take everything that Greg has said, but I would add maybe another point here and that is that the laws of armed conflict presume that there is an armed conflict. And the question would be was the attack in response to some violation of or something that would trigger self- defense. An issue of self defense might be much more approximate, for example, for Israel than the United States. Also this goes along a little bit towards the idea of preemptive action, which traditionally has been something that is very approximate to the presence of a threat whereas this seems to look out some longer period of time.

The main point I wanted to underscore here is that the idea of attacking a civilian target falling under the laws of armed conflict. There is this initial attack much like the idea of Pearl Harbor although the target there was military. This initiates a war if it's actually a bonafide attack.

PAUL ROSENZWEIG: I'm going to change the question because that's what law professors do when they get law questions that they don't like, but I'll change; I was struck by agreeing with the analysis that Greg gave. If you're inside the box of laws of armed conflict, its clearly depends on the hypos of how far down you are. I agree completely with Chuck that the main question is did we start the war. I think within the laws of armed conflict we probably started it. We probably attacked, and it doesn't necessarily lead to to war in the same way that every time the North Koreans shoot a single bullet across the DMZ constitutes an armed attack. But the South Koreans and the United States through our own grace, decide to refrain from response. But it's only by grace.

But I'll take it to the next level and ask you this question, which actually comes from a war game I did with some Israelis. What if Israel seeds the Iranian oil production facilities with cyber logic bombs but doesn't turn them off at all and says, "If you ever ever launch a missile of any form at us, we're going to destroy your entire oil production capability." They then do one little demo just to make sure that everybody knows that they're not bluffing. Is seeding, is that like mining a harbor? See *Nicaragua vs. United States*. Or is it a legitimate preemptive threat? These are questions that, again, I tend to think that the existing laws don't give us good answers to. So it's more a question to my mind of what is going to become acceptable state behavior in this domain, and we're driving ahead without anybody kind of giving thought to the long-term consequences.

If you were to ask me, I would think that the biggest strategic mistake that the United States has made in recent years is in Stuxnet choice, even more so than the war in Iraq because we've unleashed the Genie.

GREG MCNEIL: Just to respond to your hypo while people think of their questions. The example you gave, sort of the seeding – the Trojan horse waiting to be unleashed. So taking the doctrinal approach I outlined on the law of armed conflict, there's no damage yet other than the damage in the demonstration in which case that may have risen to the level of an armed attack.

The seeding of the Trojan horse amongst all these facilities under a damage-based analysis doesn't rise to the level of an armed attack until the damage occurs. Now, if I put on a different hat and I say what if the Cubans were secretly placing troops inside the United States and the Soviet Union was moving troops in to the United States in anticipation of an attack on Montana (where Red Dawn took place), what would I think about the placement of troops on territory?

Well there's a sovereignty violation there that clearly amounts to an armed attack even if the damage hasn't been done yet because it's effectively taking terrain. Could I then liken the existence of the software on servers owned by the other government as an attack akin to placing troops or amassing troops within another nation state, even if they got it – i.e., they just walked in without firing a shot. It's like a French server.

In any case, so I agree with you that that would be an area where the law of armed conflict analysis that I outlined doesn't address that.

DAN SCHNEIDER: Do you have any questions from our audience?

QUESTION: In the face of a cyber attack on critical infrastructure, would we be allowed to go back to the server from which it's coming and try to stop the attack there? This is kind of the hot pursuit question. Can you do hot pursuit in cyber space and what are the limits?

CHUCK BARRY: Let me just counter that there was an interesting scenario very much like you just described on a webinar just last week done over at CSIS where role players were people like General Cartwright and Peter Devlin and so forth. The scenario was essentially an attack on an American oil company.

They role-played very seriously in that as part of it, they shut down communications with rigs. Everything was going haywire worldwide, the pressure valves on oil pipelines, stock prices were dropping and the multinational corporation had the wherewithal to go into Venezuela and shut down the servers. They said we're going to do this. And the United States said, "No, we can't have you do that." And they said, "We don't care, we're going." This is your hot pursuit issue.

Then the question would be: what is the standing of this corporation in armed conflict if it were to be such?

The interesting thing here is that it's a role-play, so we don't know what might have happened there, but so far, the Iranians have not thrown down the gauntlet and neither have we or others in subsequent attacks like Shamoon. Even though these attacks continued to mount, and there is damage, no one has decided to take this into the realm of armed conflict other then reciprocal, perhaps, cyber activity which continues to go on at a noise level. This cyber activity begins to create the thought that maybe there is something in between kinetic war and peace where this build-up of cyber activity gets more and more serious and we throw more and more eight figure budgets into defense.

If I can right now, I'd like to make the additional point we talk often about the offense being dominant in cyber activity, and I have to say I wonder about that. The Defense Department says it's attacked millions of times a day, but it doesn't go down even a few times a day and maybe even after one or two significant attacks. It would seem to me that Defense is doing a pretty good job. Except for the website here, the lights are not off here and the power grids, the issues that we face in cyber have not demonstrated that the offense is particularly dominant. So maybe we're willing to put up with these kinds of hot pursuit actions, be it on a multi-national corporation or simply Melissa.

GREG MCNEIL: My sense would be that the attribution problem would probably be the first, but your hypo sort of addressed that by saying that maybe we don't know who's launching the attack, but we know it's coming from that server.

Analytically, we'd have to resolve whether the server located in country Hypothetica, is the attack being directed by the country of Hypothetica? Are they even aware of the fact? Then the next step of the analysis would be are they aware of the fact that the attack is being launched from within their territory? I think that, absent that awareness, we would violate the principle of neutrality to attack them, even though the attack is coming from their territory. We wouldn't like this operationally because we would have to slow the process down to contact the President of Hypothetica to ask them to intervene to stop this.

That's like neutrality law going back about 100 years; that's what I would be required to do in that circumstance. Whether we would actually do it, of course, because of the reverse attribution is another question. Or, if you tried to characterize the counter operation as an intelligence operation for domestic law purposes, it might allow you to make an end run around the requirement of notification. This is the central challenge that we're defining here. The attribution issue becomes one that [is complicated]; there could be operations where an attacker intentionally makes it appear that the neutral is the party that's attacking in the hopes of bringing out one party to attack another and drawing others in to a potential conflict. I think on the straight analysis with the hypothetical you gave, the law as it stands would require notification to the host state government prior to attacking. I imagine that's the position of the United States on that, or at least some agencies inside the United States.

PAUL ROSENZWEIG: It is indeed and that's why the law is wrong. Imagine a hypothetical. This extreme is a little bit of the imagination, but imagine if the Cubans had not known that there were Russian missiles on their territory. It's possible that there's a secret Russian base and the Russians give enough money to Fidel that Fidel doesn't ask what's inside the bases. Would we actually be obliged to go an ask Cuba before responding to missile launches from that territory?

Now under the laws of armed conflict, if you indulge my hypothetical and you believe in Fidel's honesty; yes and wouldn't. We just wouldn't. We wouldn't wait and we won't in cyberspace and in the end, there'll come to be a set of customary norms that will probably, for example, limit the destructiveness with which we may respond.

We were all at the same thing; we might freeze the server; encrypt it so it can't do any more damage. Take it off line. Those would be acceptable. But the customary international norm would be that you can't go in and fry it so that it's taken offline permanently and you have a major hardware damage and you have to go back and buy a new one.

That's Rosenzweig's corollary to the lack of law because I've just developed it now. But that's where we'll wind up; somewhere in that range. I am 100 percent confident in predicting in the event of such a real attack that had significant damage on an American electric grid of that sort, the niceties of existing international laws of armed conflict would matter for naught. 100 percent confident.

GREG MCNEIL: So just the thought of some feasible precautions came to mind here that would it necessarily be an attack, a responsive attack, or could there be some way that you could almost cyber embargo that state. So the lesser response measure might be because we control like 94 percent of the servers are like in Herndon, Virginia. Figure out a way to shut off communications from entirely in to or out of that nation state until such time as you could try and resolve the issue with the nation state. There might be some interim measures that are technologically capable, but I think Paul's right.

DAN SCHNEIDER: Last question.

QUESTION: [inaudible]

PAUL ROSENZWEIG: Well, there are two reasons. The first is that cyber is so comprehensive a domain that essentially it's the treaty of everything. Cyber infects every one of the 18 critical infrastructures. So any regulations we have will have the largest pan global effect. There are more than 2 ½ billion people on the network today, so that kind of universal agreement that poses a huge governance issue.

The other is really that, at least so far, we're in a fundamental disagreement about what cyber warfare is. We've all been talking about it as if it were an adjunct kinetic war with structure damage, whatever. You ask the Chinese, they don't look at Washington as the threat; they look at Silicon Valley as the threat and they think that Twitter is a tool of American warfare.

In fact, I've had talks with the people in China and have told them that Twitter is not a government sponsored thing and they laugh at me because they don't believe me. And Greg's on Twitter, I'm on Twitter. I don't know; who's on Twitter? How many of you tweet? Yeah, okay. Does the government ever tell you what to tweet? No. Of course not. But if I go and tell the Chinese that they don't believe me. They think Facebook is an American conspiracy to destabilize the regime. They see, and most of the world outside of the West sees, information and social media as a warfare domain. They see us as trying to destabilize their countries and we're never going to agree on a treaty-limiting vat; at least I hope we won't ever.

DAN SCHNEIDER: Chuck.

CHUCK BARRY: Well, we have a fundamental disagreement, I think, with China and Russia in that they would love to have a treaty on arms control. They would call it an Arms Control Treaty in Cyberspace to try and reign in and catch up, perhaps, with the United States.

So what the U. S. policy has been is to work through the rendering or the extension of existing treaties. This is largely a reflection of what Paul has just said and that is we don't have our arms around this yet. There are so many unanswered questions and usually we don't start with treaties. If you look back at the Hague and Geneva Conventions and all the other customary laws that have come about and case laws that evolve, this is, I mean the formal modern part extends back 150 years. I think that the treaties will come once the international consensus comes, but you think about how long it took us until 1949 before we agreed on how to treat prisoners of war.

You know, I don't think treaties are where you start, it's kind of where you get to after you've had experience and I think we all just kind of agree that there has not been an armed conflict generated in cyberspace. There's been no, not been, or probably will never be a purely cyber war. And the point I made about this kind of being an extension of electronic warfare. It's not the same. We understand that, but it has a paternity there. So we can move from the known to the unknown in that way and feel comfortable that we're at least staying abreast of the issues in cyber space.

Ken's comment up front has a very close relationship to cyber robotic warfare. Seems to me to be much more fraught with potential problems because we are getting in it to the point of significant robotic warfare in all domains. We talk about drones, but they're in all domains.

DAN SCHNEIDER: I think that's a good time to conclude with that remark because it brings us back to where we started.

Chuck your last remark was sobering because if you look at when the laws of war began and were extended in the 1860's and 1870's after the atrocities of the Crimean War. Laws banning poison gas were after the use of poison gas in World War I and of course, World War II. Then to war years, you also had the laws about POWs and of course, after World War II you had the Genocide Treaties. That's a sobering thought that it's only after massive damage and death has occurred that treaties begin to emerge and hopefully that's not what is going to happen in this instance.

One comment; Paul, what you were saying about the Chinese reaction [viewing] Twitter as part of the U. S. government. I wouldn't just say that's China. Much of the rest of the world, for instance in Egypt, when we had that short video that was produced, most Egyptians believe that the United States government was behind that or even if we weren't why couldn't we just stop it. Most of the rest of the world doesn't understand the public/private distinction that's made that's largely a western idea, and that leaves tremendous conspiracy theories also in much of the rest of the world that whatever happens, someone at the Pentagon or someone in the White House is pushing the button. So that's what happens.

Final food for thought (I teach a course on terrorism), is whether cyber warfare is a tool of the weak. After all, all you need is an Internet connection and some computer genius. It doesn't take a lot of money to do a lot of damage. Just like terrorism is a tool; people don't owe a lot of money, but they can maximize their impact.

MALE VOICE: Does anyone have final comments?

CHUCK BARRY: This is just two fingers, but it goes back to the point about robotic warfare. Just think about the fact that all the modern armies of the world have moved in the last 30 or 40 years away from conscription [with] the separation of the professional forces from the population.

In a certain sense we're moving towards robotic warfare in that we have a separate force that we could just send out there that is increasingly robotic itself. So the push button, the idea of democracies going to war, not fighting each other, stems in part from the fact that if they decide to do that they'd have to actually be the ones to go do that. That is increasingly less the case across all western forces.

And so the decision to send your armed forces is oftentimes a money decision; it's our team, and we support our forces, but we don't know them. We're increasingly not knowing them and we'll know them even less when they're more and more robotic. And then we will get to the point where it's sending our respective robots to do this work.

DAN SCHNEIDER: Well I would like to thank the International Law Review and the National Security Law Brief for organizing, at least, this session. The afternoon session promises to be as interesting and stimulating as this session.

I particularly want to thank our three incredible speakers who you've been privileged to hear from some of the true experts in the world on these issues.