Case Western Reserve Journal of International Law

Volume 47 | Issue 1 Article 22

2015

Talking Foreign Policy

Michael P. Scharf

TALKING FOREIGN POLICY:

A DISCUSSION ON CYBER WARFARE[1]

Talking Foreign Policy *is a production of Case Western Reserve University and is produced in partnership with 90.3 FM WCPN ideastream, Cleveland's NPR affiliate. Produced quarterly, the program is hosted by Case Western Reserve University School of Law Interim Dean Michael Scharf, and focuses on the most relevant foreign policy issues of the day.*[2] The January 30, 2014 broadcast covered the constantly evolving field of cyber warfare, and featured the following guests:

- *Peter Singer, Director of the Center for 21st Century Security and Intelligence, Brookings Institution;*
- *Michael Newton, Professor of Law, Vanderbilt University;*
- *Milena Sterio, Associate Professor of Law, Cleveland-Marshall College of Law; and*
- *Shannon French, Professor of Philosophy and Director of the Inamori Center for Ethics and Excellence, Case Western Reserve University*
- *Archived broadcasts of* Talking Foreign Policy *in both audio and video format are available at http:// law.case.edu/ Talkin Foreign Policy.*

TALKING FOREIGN POLICY

Cyber Warfare—January 30, 2014 Broadcast

MICHAEL SCHARF: Welcome back to Talking Foreign Policy. I'm your host, Michael Scharf, Interim Dean of Case Western Reserve University School of Law. In today's broadcast, we'll be discussing the topic of cyberwar.[3] We'll begin our discussion with Peter Singer, Director of the Center for 21st Century Security and Intelligence at

1. Special Thanks to Kristine Moore, Cox Center Fellow at Case Western Reserve University School of Law, for editing this transcript and providing background research.

2. *See Talking Foreign Policy*, CASE W. RES. U., http://law. case.edu/ OurSchool/FacultyStaff/MeetOurFaculty/FacultyDetail/TalkingForeign Policy.aspx (last visited Mar. 3, 2015).

3. *See* Quora, *How Does Cyber Warfare Work?,* FORBES (Jul. 18, 2013), http://www.forbes.com/sites/quora/2013/07/18/how-does-cyber-warfare-work/.

the Brookings Institution.[4] Oxford University recently published Peter's new book on cyberwar and cybersecurity. I just finished reading it and it's an eye opener. Peter, thanks for being with us today.

PETER SINGER: Thank you.

MICHAEL SCHARF: So, Peter, we hear so much about cyber threats and cyberwar in the news. Where do we stand now?

PETER SINGER: It's interesting, this topic of cybersecurity and cyberwar. It connects issues that are as personal as your privacy or your bank account to as weighty as reach of world politics. Where we stand is that we are definitely in an age of huge cyber dependence—everything from our communications to our commerce, infrastructure, and, yes, conflict. Ninety-eight percent of military communication runs over the civilian owned and operated internet, so we all depend on this cyber world. We live in a digital world, and yet we're also in an era of cyber insecurity. You can see it in everything from the 97% of Fortune 500 companies that have been hacked,[5] and the 3% who just don't know it yet, to— there have been created over 100 cyber military command equivalents around the world. There was a poll taken—the first poll of 2014 by PEW—found that Americans are more afraid of a cyber-attack than they are of Iranian or North Korean nuclear weapons, the rise of China or authoritarian Russia, or climate change.[6] So, we've got this combination of massive use of the online world and its rippling effect into the real world via the Internet of Things.[7] But also, we're not in a good place, in terms of our discomfort and, frankly, our lack of awareness on just the basics of this topic and that was the point of the book—to try to connect those two together.

---

4. *About the Center for 21st Century Security and Intelligence*, BROOKINGS INST. (2014), http://www.brookings.edu/about/centers/security-and-intelligence/about.

5. *All Fortune 500 Companies Have Been Hacked: 97% Know It, The Other 3% Don't.* HOMELAND SEC. NEWS WIRE (Jan. 8, 2014), http://www.homelandsecuritynewswire.com/srcybersecurity20140108-all-fortune-500-companies-have-been-hacked-97-know-it-the-other-3-don-t.

6. *Public Sees U.S. Power Declining as Support for Global Engagement Slips,* PEW RES. CTR. FOR PEOPLE & PRESS (Dec. 3, 2013), http://www.people-press.org/2013/12/03/public-sees-u-s-power-declining-as-support-for-global-engagement-slips/#top-threats.

7. *See* Jacob Morgan, *A Simple Definition of "The Internet of Things*," FORBES (Mar. 13, 2014, 12:05 AM), http://www.forbes.com/sites/jacobmorgan/2014/05/13/simple-explanation-internet-things-that-anyone-can-understand/ ("[T]his is the concept of basically connecting any device with an on and off switch to the Internet (and/or to each other).").

MICHAEL SCHARF: I suppose there's a spectrum. On one side, we've got the hacking like we were talking about and then maybe surveillance, but on the other side is this concept of cyberwar, which you also devote several chapters to. How is this cyber warfare different from conventional war?

PETER SINGER: You hit it exactly. Part of the problem with how we've approached it is we lump together so many things simply because they take place in the realm of zeroes and ones. A good illustration of this would be General Alexander, who is in charge of *both* Cyber Command and the National Security Agency.[8] You would never see that with other military commands and intelligence agencies, but because it's in this we do. But, he testified to Congress that each day, in his quote "the US military faces millions of cyber-attacks,"[9] but to get that number of millions he was combining everything from political protests and pranks to data theft and espionage. But, none of what happened, in terms of these millions of attacks, was actually what people think of when they think of cyberwar and what they should think of cyberwar, which is a state of armed conflict politically motivated with violent means— with violence, just like with regular conflict, with regular war itself. You can see this in the phraseologies of a *cyber-9/11* or a *cyber-Pearl Harbor*. So, we mush lots of things together. I make the parallel that it's a lot like saying that a group of teenagers with firecrackers, a group of political protestors in the street with a smoke bomb, a James bond spy with his pistol, a terrorist with a roadside bomb, and a military with a cruise missile and saying, "Well, these are all the same because they involve the chemistry of gunpowder." Well, no, they're not. And we wouldn't treat them that way, but we do hear so in cyber warfare. It's definitely— part of why it's important to distinguish what we mean when we say war is that it also allows you to get to the true reality of it. When you're talking about how the military actually uses this technology and the nature of the beast, when you're exploring things like computer operations and the like.

MICHAEL SCHARF: And you mentioned, the US, now has a cyber-command as part of its armed services. It's not just the sea, land, air,

8. *See US May Split Cyber Command and NSA,* RT (Nov. 9, 2013, 11:25 AM), http://rt.com/usa/alexander-retire-nsa-cybercom-438/ ("[General Alexander can c]urrently… both direct offensive operations against the computers of foreign military targets while also administering campaigns to collect intelligence on those entities.").

9. *See U.S. Military Goes on Cyber Offensive*, DEFENSENEWS (Mar. 24, 2012, 11:09AM) http:// www. defensenews. com/ article/ 20120324/ DEFREG02/ 303240001/ U-S-Military-Goes-Cyber-Offensive; Nominations Before the Senate Armed Services Committee: Hearing Before the Comm. on Armed Services, 111th Cong. 233 (2010) (statement of Ltn. Gen. Keith B. Alexander).

or the outer space anymore. We also have an entire military apparatus for cyberspace. But, surely, Peter, they're not looking at the firecrackers and the little teeny things. They're preparing for all-out war, right?

PETER SINGER: That question of mission and responsibility has been one of the areas that's bedeviled the approach to this space because of how when you talk about jurisdictions when you talk about national borders, it gets very fuzzy when you move into the online world. You also have an issue of scale. It'd be surprising to a lot of people, but there are actually more folks working in the Fort Meade complex—which is where Cyber Commandand NSA are—there are more people working in that than there are in the Pentagon itself.[10] This is a huge growth area and again—

MICHAEL SCHARF: How much money are we spending on that?

PETER SINGER: There are a lot of different ways to cut it. To me, what stands out is not the exact amount that you're spending but how you're dividing up your resources. And in the US, we spend about four times as much in the governmental side on Defense Department cyber operations as we do in the Department of Homeland Security on the civilian side.[11] Also, if you want to know what we are spending on internally, research and development, we're spending—again depending on how you're categorizing it— we're roughly spending two-and-a-half times to four times as much on cyber *offense* research and development as we are on cyber *defense* research and development.[12] I don't think—I argue that that's not that most strategic approach. It's a lot like, you talked about those teenagers along, if you're using a metaphor, it's a lot like being worried about

10. In fewer than ten years, Ft. Meade has expanded from 33,500 employees to approximately 57,000 employees, more than twice the number of Department of Defense employees at the Pentagon. *See* Marjorie Censer, *Fort Meade Transforming From Army Base to Cyber City,* WASH. POST (Oct. 10, 2013), http:// www. washingtonpost.com/ business/ capitalbusiness/fort-meade-transforming-from-army-base-to-cyber-city/ 2013/10/09/b319a3a0-2792-11e3-ad0d-b7c8d2a594b9_story.html.

11. *See* Liz Gormisky, *Cybersecurity Spending Up at DOD and DHS in FY15 Budget Requests,* DEF. DAILY NETWORK, Mar. 12 2014, http://www.defensedaily.com/cybersecurity-spending-up-at-dod-and-dhs-in-fy15-budget-requests-2/. *Ed. note*: Mr. Singer originally quoted the cybersecurity budget differential between DoD and DHS as a factor of ten. This transcript has been edited to reflect the actual FY 2015 numbers.

12. For FY 2014, Congress allocated $68 for central Cyber Command and $14 million for the Air Force's cyber offensive program, while only allocating $5.8 million for cyber defense. *See Cyberwar, High-Tech Weapons Take Center Stage in Defense Budget,* FOX NEWS (Dec. 27, 2013), http://www.foxnews.com/tech/2013/12/27/cyberwar-high-tech-weapons-take-center-stage-in-defense-budget/.

gangs of roving teenagers in your neighborhood, and you're standing there in your glass house and say "You know what? I ought to go buy a stone-sharpening kit."

MICHAEL SCHARF: Well, some people do say that a good defense is a strong offense, but I want to go back—

PETER SINGER: No, actually, in both sports and in warfare the best defense is a good defense.

MICHAEL SCHARF: Certainly with the Super Bowl coming up that's true. Let me ask you this: so, you mentioned that people are talking about a cyber-Pearl Harbor or a cyber-9/11. What are the possible major consequences that we could see from a cyber-attack? What's the worst case scenario that you can imagine?

PETER SINGER: First, let's caveat all of this by staying within the reality of the real world of what's happening right now before we get to the potentiality. So, the fact that there have been over a half million references in the media and in academic journals to a cyber-9/11 or a cyber-Pearl Harbor or the fact that there have been 31,000 magazine and academic journal articles about the phenomena of cyber terrorism, let's be fundamentally clear that no person has been hurt or killed ever so far by cyber terrorism by the FBI definition of it.[13] If we want to talk about the power-grid-going-down scenario, squirrels have taken down the power grid more times than in the zero times that hackers have. That's where we are right now. If we want to talk about the actual, now playing out, big national security issues, to me the real world one to worry about is the massive campaign of intellectual property theft that's emanating from primarily China.[14] It's the largest theft in all of human history that's going on and has huge consequences not just for the economy, but for national security in the end. Now, if you want to go to the what-ifs of what could be there in terms of danger, in the last part the book we explore the key trends that are moving forward. And it's the combination of one thing that's happening with the internet more broadly and one that's happening within cyber warfare. With the internet more broadly, it's the shift to the Internet of Things where we're not just using internet-

13. *See* Sue Marquette Poremba, *Cyber Terrorist Threats Loom 10 Years After 9/11,* NBC NEWS (Sept. 6, 2011), http://www.nbcnews.com/ id/ 44415109/ns/ technology_and_science-security/ t/cyber-terrorist-threats-loom-years-after/ ("According to the FBI, cyber terrorism is any 'premeditated, politically motivated attack against information, computer systems, computer programs and data which results in violence against non-combatant targets by sub-national groups or clandestine agents.'").

14. *See* Emma Wollacott, *US Should Get Tough on Chinese IP Theft, Committee Warns,* FORBES (May 23, 2013), http://www.forbes.com/ sites/emmawoollacott/2013/05/23/us-should-get-tough-on-chinese-ip-theft-committee-warns/.

enabled devices to communicate with one another. I email you or whatnot, but it's devices that range from our cars to our thermostats to our power grid to our refrigerators all being looped in.[15] So, now you've got the real world being connected. And we're doing that for reasons of efficiency, for gains in the environment, there are all sorts of good things out of it, but it also means that there are vulnerabilities there that can be tapped with greater consequence. We've already seen car hacking, we've already seen refrigerator hacking.[16] But, then the second is the development of new cyber weapons, and Stuxnet[17] is the game changer here where it's weapon that in one hand is like at every other weapon in history. It causes a physical change in the world like a stone did or a drone does, but the difference is its native zeroes and ones.

MICHAEL SCHARF: This is what the United States and Israel used against the Iranian nuclear reactors right?

PETER SINGER: It went after Iranian nuclear research. In particular, they were operating under a SCADA system[18] to control things like the centrifuges and the like. It damaged both what they were working on and also the systems themselves. And it's a fascinating story that we cover in the book in a lot of different ways. One, showing that this new kind of weapon was causing physical damage to digital means. It's interesting in that it's a weapon that was here, there, and everywhere. It was in 25,000 plus different computers around the world.[19] On the other hand, it might have been

15. *See* Morgan, *supra* note 6.

16. Julie Bort, *For the First Time, Hackers Have Used a Refrigerator to Attack Businesses,* BUS. INSIDER (Jan. 16, 2014), http://www.businessinsider.com/hackers-use-a-refridgerator-to-attack-businesses-2014-1.

17. Stuxnet was a combined attack from the U.S. and Israel on Iran's nuclear program. It targeted the main system in the plant through a USB drive carried by a worker. There were two attacks, and the first gave hackers an "electrical map" of the Natanz plant. The intended goal was to reduce the "lifetime of Iran's centrifuges… making the…systems appear beyond their understanding." However, the result was that many of the centrifuges were destroyed, delaying Iran's nuclear development. *See* David Kushner, *The Real Story of Stuxnet*, IEEE INSIDER (Feb. 26, 2013, 2:00 PM), http://spectrum.ieee.org/telecom/security/the-real-story-of-stuxnet.

18. *See* Anshul Thakur, *SCADA Systems*, ENGINEER'S GARAGE, http://www.engineersgarage.com/articles/scada-systems (last visited Nov. 1, 2014) (describing, *inter alia*, how SCADA systems monitor and control the main operating systems of a factory or plant).

19. *Iran's Bomb Experts: Israel Used Cyber Weapon to Disrupt Iran's Nuclear Reactor*, HOMELAND SEC. NEWS WIRE (Sept. 23, 2010), http://www.homelandsecuritynewswire.com/experts-israel-used-cyber-weapon-disrupt-irans-nuclear-reactor; *see also* Atika Shubert, *Cyber Warfare: A Different Way to Attack Iran's Reactors*, CNN (Nov. 8,

the first ethical weapon ever created in that it could— it may have been in all these different computers, but it could only cause damage to the one target that it was intended to. So, even if you had the very same brand centrifuges in your basement aligned in the exact same way, it still wouldn't have worked on those. It's fascinating in a lot of different ways, but it's also—one person we interview in the book describes this as Pandora's Box. It opened up a whole new set. So, that combination, to answer your question, now cannot just cause physical damage, but you now have more targets of greater consequence that systems like that can go after.

MICHAEL SCHARF: And, theoretically, that could be used against satellites, it could be used against our aviation, it could really cause physical damage by shutting down—

PETER SINGER: SCADA is used in everything from Nuclear Research-SCADA, the system that it was going after-everything from nuclear research to traffic signals to factories that make anything from jet fighters to cupcake wrappers. So, the issue here again is all the gains we've got now to digitize systems, but that brings with it vulnerabilities. The key, though, is you can't delude yourself into thinking that you can protect yourself somehow by disconnecting. Some people say "Oh, I may be using this digital system, but it's not linked to the internet." Sometimes it's called air gapping.[20]

MICHAEL SCHARF: So, that's not the solution. So, what exactly is the United States, this new Cyber Command, doing to try to protect us from this threat?

PETER SINGER: So, Cyber Command—one of the other things it's playing out right now is this question: what exactly are its responsibilities? Originally, when it was created, Defense Department officials talked about how it would just be responsible for defending Defense Department networks.[21] Like any other organization, again, whether you're talking about militaries or the March of Dimes, it slowly but surely, actually in this case quickly, took on a wide variety

---

2011, 12:13 PM), http://www.cnn.com/2011/11/08/tech/iran-stuxnet/index.html.

20. Air gapping is when malware travels via sound waves to physically attack nearby machines. After disconnecting from the Internet, a computer can still be infected by air gap malware. *See* Dylan Love, *Hackers Can Infect Your Computer Even if It's Not Connected to the Internet*, BUS. INSIDER (Mar. 5, 2014), http://www. businessinsider. com/what-is-air-gap-malware-2014-.

21. Meg Mirshak, *Recruitment, Retention Focus of Fort Gordon's New Cyber Command*, AUGUSTA CHRON. (Ga.) (Oct. 14, 2014), http://chronicle.augusta.com/latest-news/2014-10-13/recruitment-retention-focus-fort-gordons-new-cyber-command; *see also* Cheryl Pellerin, *Rogers: Cybercom Defending Networks, Nation*, U.S. DEF. DEP'T (Aug. 18, 2014), http://www.defense.gov/news/newsarticle.aspx?id=122949.

of different roles. So, it's both protecting Defense Department systems—it has set up a series of units that are designed to basically be operative in cyberwar. They're able to be tasked out to the regional commands and the like.[22] Then, there's another part that's about national protection. And there are units that are basically designed to aid in the defensive (not exclusively Defense Department networks but other critical infrastructure out there and the like). This is when you get into the interesting things of legal authorities, budgets, and responsibilities. One of my concerns is that it's quite natural, when you're talking about threats, to say, "Well, why shouldn't the military be responsible for defending us?" But, the problem here is that it causes a shift in and causes a sort of sense of complacency. It takes away what responsibility should have. So, think about it this way: you'll sometimes see here people site incidents where a group might have done a denial of service on banks. There was an incident where a general talked about that that is why we needed more funding for Cyber Command. If there was a bank that was moving cash to another bank in an armored van, and a bunch of protesters stood in the street, blocking it for two hours and then dissipated, no one would say "Oh, my goodness, where was the US military?" But, change that bank and that money to zeroes and ones, and that's the narrative that we have right now. No, it's also the responsibility of the banks and the like—

MICHAEL SCHARF: That's an interesting insight, and we'll discuss this in greater detail when we come back from a short break. We've been talking to Peter Singer, bestselling author of the book *Cybersecurity and Cyberwar*.[23] When we come back we're going to bring three leading experts into the discussion to look at the practical, ethical, and legal aspects of cyber warfare. Stay with us.

MICHAEL SCHARF: Welcome back to "Talking Foreign Policy" brought to you by Case Western Reserve University and WCPN 90.3 ideastream. I'm Michael Scharf, Acting Dean at Case Western Reserve University School of Law. We're talking today about cyberwar with Peter Singer of the Brookings institute, Colonel Mike Newton of Vanderbilt, Professor Milena Sterio of Cleveland Marshall College of Law, and Doctor Shannon French from Case Western's

22. *See generally Organization*, U.S. ARMY CYBER COMM., http://www.arcyber.army.mil/org-uscc.html (last visited Mar. 16, 2015) (describing the enumerated responsibilities of U.S. Army Cyber Command).

23. *Cybersecurity and Cyberwar: What Everyone Needs to Know…and How to Talk About It*, BROOKINGS INST. (Jan. 6, 2014), http://www.brookings.edu/events/2014/01/06-cybersecurity-cyberwar-what-everyone-needs-to-know.

Inamori Center.[24] Just before the break, Peter Singer was telling us about the US approach to cyberwar. There were some offensive and perhaps not enough defense components, but let's now begin this segment with our military expert, Vanderbilt professor and former JAG, Colonel Mike Newton. Mike, is it fair to characterize the situation that's going on between countries in the world of cyber weapons as a kind of arms race?

MICHAEL NEWTON: I guess, in a sense it is. But, it's a different kind of arm. It's really a race for technological supremacy, so the real challenge is the same thing we've had since the invention of the crossbow. How does the law respond? How does national policy respond? The challenges are classic conceptions of what we really mean by war and what it means to wage war, and this represents a whole new set of actors that are involved in that. Peter quite correctly points out there's this incredibly vast combination of private actors, public actors, government infrastructure, and persons acting under government influence or, in their minds, to help achieve government purposes. So, it's a very difficult legal conceptual fit to simply take the established law of war and cram it down onto the context of cyberwar.

MICHAEL SCHARF: Now, Mike, you mention that it's really about technology evolving. That evolution happens all the time, but this reminds me of more of a technological leap like the nuclear age. Let me bring in Shannon, an ethicist, into the conversation. Policy makers didn't really understand nuclear weapons, so they let the scientists and the military specialists do all sorts of *Doctor Strangelove*[25]-like experiments, some of which I think brought us very close to losing the ozone layer. Do you see any parallels to what's going on with the exploration of new weapons and means of warfare in cyberspace?

SHANNON FRENCH: Well, I will first say something I hope to be reassuring. I think we do have better communication going on now in terms of policymakers actually seeking out genuine experts and getting input from them. I would also say that although it is a little bit confusing to many of us, a lot of the world that is this new cyber realm can be translated better than a lot of the nuclear science, in terms of again speaking directly to policymakers. But, I actually think what's interesting is that there are some strong parallels to what we saw in the Cold War with the arms race and the so-called MAD

24. *Shannon E. French, Ph.D., Director of the Inamori Center for Ethics and Excellence*, CASE W. RES. UNIV., http://www.case.edu/provost/inamori/about/meet.html (last visited Mar. 16, 2015).

25. *See* Eric Schlosser, *Almost Everything in "Dr. Strangelove" Was True*, NEW YORKER (Jan. 17, 2014), http://www.newyorker.com/news/news-desk/almost-everything-in-dr-strangelove-was-true (describing, *inter alia*, some of the more improbable plot elements of the film and the analogous similarities in the 1960s).

strategy, which was Mutual Assured Destruction. [26] In the same way that major powers decided "Well, we really can't nuke one another because everybody loses," there is now the same kind of implicit restraint going on with the major powers using large cyber-attacks. We're too interconnected, especially economically, for us to attack one another. It is parallel in that, just like in that era, we have now the greater worry being rogue groups. It isn't that we're worried about the major powers attacking one another with their strengths, but we're worried about it more on the level of asymmetric threats.

MICHAEL SCHARF: But, what about China? I read in the news that it's China that's pouring all the money in, other than us, into this area. Peter, can you tell us what your take is on that?

PETER SINGER: There are a of couple things. First, you asked about arms races. One of the other attributes of every arms race in history is that you're a driving forward force, for very good reason, for your security. That's why they're investing in these technologies. They're worried about real adversaries out there, and that's what drives the sides in an arms race. The other hallmark of every single arms race is that the more you spend, the less secure you end up feeling in the end. That's whether you're talking about the arms races of battleships back prior to World War I, the nuclear arms race, or what we're seeing today on the cyber side. The other thing, and this is where I may disagree a little bit, is that there are some parallels to the Doctor Strangelove-ian thinking that's out there, and you can see that. One, and some of the kind of hucksterism—people who understand just a little bit about it or even more so stand to benefit from hyping a threat or some kind of silver bullet solution to it. A lot of the discourse in Washington DC, I joke, has the attributes of Spinal Tap and turning the volume up to 11.[27] You can see that there, and that's of concern to me. Yet another example would be to say that the solution is to create a new, more secure Internet. Well, no, that is not going to happen. To your point about China, I'm not saying this is purely a threat hyping problem. There are real issues at play here, and there are real capabilities being built. We talked about the US side, but China is just as active in building up its capabilities both formally within its military as well as a much wider network, almost like a patriarchic hacker community or a militia community.

26. The doctrine of Mutual Assured Destruction held that the rapid development of nuclear weapons by the United States and Soviet Union in the 1950s resulted in neither country wanting to use their nuclear weapons on the other first, for fear that "whoever shoots first, dies second." *See Mutual Assured Destruction*, NUCLEAR FILES, http:// www.nuclearfiles.org/menu/key-issues/nuclear-weapons/history/cold-war/strategy/strategy-mutual-assured-destruction.htm (last visited Mar. 16, 2015).

27. MARTIN DIBERGI, THIS IS SPINAL TAP 11-12 (Svein I Halvorsen et al. eds., 1996).

The difference is almost a quality-quantity aspect. There's a description of the Chinese approach towards internet censorship that's called the "human flesh search engine."[28] That's in many ways the parallel here of China, where to stay on the attack side, there's just a massive amount that's going on. The targets range from the military defense companies, oil companies to small furniture makers in New England to universities and even my think tank. That's just in the US. In the book we talk about Operation Shady RAT,[29] which was linked back to China. It hit everything from international organizations that range from trade groups to the International Doping Agency prior to the Beijing Olympics to Coca-Cola has been hit.[30] It's just a massive scale, and that may be the differentiator here.

MICHAEL SCHARF: Well, let me turn to the legal issue. To start with something that Peter was telling us about earlier, and that is the Stuxnet attack where the United States and Israel actually were able to do a cyber-attack on these nuclear facilities that put Iranian construction of nuclear weaponry back about two years as I understand it. So, when the US attacks another country like that, Milena, doesn't the President have to authorize an attack? Does he need congressional approval? How does this fit into our conventional thinking about warfare?

MILENA STERIO: Under any kind of a conventional analysis of warfare, normally our President does need congressional authorization to deploy troops.[31] On the other hand, our President has the inherent

28. The "human flesh search engine" is a form of cyberbullying in which people are targeted after the public takes an interest in their actions. Private information immediately becomes public, and the targets are often stalked and threatened. *See* Celia Hatton, *China's Internet Vigilantes and the 'Human Flesh Search Engine*,' BBC NEWS (Jan. 28, 2014), http:// www.bbc.com/news/magazine-25913472.

29. Operation Shady RAT (for Remote Access Tool) originated in China and hacked into over seventy entities, including elements of the U.S. government, the International Olympic Committee, and the United Nations. At the time of its discovery, the Operations was still in the process of hacking. *See* Ellen Nakashima, *Report on 'Operation Shady RAT' Identifies Widespread Cyber-Spying*, WASH. POST (Aug. 2, 2011), http:// www. washingtonpost.com/ national/ national-security/ report-identifies-widespread-cyber-spying/2011/ 07/29/ gIQAoTUmqI_story.html.

30. Ellen Messer, *Cyber-Espionage Attacks Threaten Corporate Data in New Unrelenting Ways*, NETWORK WORLD (Aug 8, 2011, 7:00 AM), http://www.networkworld.com/article/2179877/security/cyber-espionage-attacks-threaten-corporate-data-in-new-unrelenting-ways.html.

31. *See Executive Power*, LEGAL INFO. INST., http://www. law. cornell. edu/wex/executive_power (last visited Mar. 16 2015) ("Congress holds the power to declare war. As a result the president cannot declare war without their approval.")

Constitutional authority as our Commander in Chief to use force.[32] The very difficult Constitutional question is really then: under what circumstances can the President act alone without Congress? I think most scholars would agree that the President can act alone if our nation is faced with some kind of a sudden threat.[33] To bring it back to this issue of cyber-attacks against Iran, you would have to make the argument that the Iranian nuclear enrichment facilities were producing nuclear material at such a pace where they were about to reach the stage where they were about produce a nuclear weapon, which then would be—could be a sudden immediate threat to the United States. Under that rationale then you could say our President can use force, but that assumes that we're conceiving of a cyber-attack by the United States a conventional military attack. I think that goes back to—

MICHAEL SCHARF: If it's zeroes and ones, we shouldn't?

MILENA STERIO: Well, if it's zeroes and ones that makes it a lot more difficult. This is what Mike Newton was also talking about earlier. If we're talking about sending a computer worm called Stuxnet over to Iran that doesn't really require the deployment of US troops, is not going to kill anybody, and might slow down their production of uranium, we're not talking about human lives. Can we really think of it the same way that we think of, for example, sending ten thousand American troops to Afghanistan? I think—

MICHAEL SCHARF: We're talking about the U.S. Constitutional view, but what about the international view? If a country's borders are sacrosanct, they're supposed to have, under the UN Charter, the right of inviolability.[34] What if another country comes in and penetrates you not physically but with zeroes and ones over the Internet and does damage to you that costs a lot of money and hits at your very national security? Is that a violation international law?

MILENA STERIO: That kind of an act under international law could be viewed as aggression, which is really a use of force by one state against another state or group of other states that doesn't comply with the normal rules of international law. Basically, you can use force only in self-defense or if the United Nations Security Council authorizes you to use force.[35] Here we have to analyze the nature of the cyber-attack. Is it just zeroes and ones? Are we just talking about

32. *Id.*

33. CHRIS EDELSON, EMERGENCY PRESIDENTIAL POWER 7 (2013).

34. U.N. Charter art. 51 ("Nothing in the present Charter shall impair the inherent right of individual or collective self-defence if an armed attack occurs against a Member of the United Nations, until the Security Council has taken measures necessary to maintain international peace and security.").

35. *Id.*

slowing down a nuclear plant or are you also taking down an entire power grid? Are you talking about neutralizing an entire infrastructure? All the defense missiles? It really comes back to the scope and nature of the cyber-attack.

MICHAEL SCHARF: I want to talk to Shannon about the ethical aspects of this. Let's say you're the expert who was tasked to launch the cyber-attack. As an ethicist, what are your thoughts about the psychological and ethical implications on that person, on US personnel who are engaged in cyber warfare acts?

SHANNON FRENCH: Well, as an ethicist, you always worry when there's distance and potential detachment. Every time someone has to make a decision that has an impact on the lives of others and the harder it is for them to see and judge that impact, the less likely they are to make the ethical choice. They're likely to be more callous, and that is simply a consequence that we're familiar with. It's interesting— we've actually talked about this on this program in a different context. There's a lot of worry about that with the drones. Actually, it was discovered, to some folks surprisingly, my own in one stage, that the drone operators were seeing their victims very close up and were actually experiencing high levels of PTSD.[36] They were having to work, almost like a sniper does, their relationship to the people that they were targeting.

MICHAEL SCHARF: But, that wouldn't be true here.

SHANNON FRENCH: That wouldn't be true here. That very distance that people thought the drone operators would have is something the cyber folks really could have. Maybe that worry needs to be revived in this context.

MICHAEL SCHARF: You've said before if you don't have skin in the game you're likely to make mistakes.

SHANNON FRENCH: But, I do have to put a caveat in here. It actually connects back to something that Peter said. I think we can't lose sight of the potential good herein terms of cyber weapons. Actually, I think he suggested they might be more ethical in some contexts. And I recognize that. If they are more precise and if they actually don't have the kind of collateral damage that we worry most about, if they're not harming vulnerable populations—

MICHAEL SCHARF: If our option was to either do cruise missile strikes on the nuclear weapon facilities in Iran, and there was a lot of

36. *See Post-Traumatic Stress Disorder (PTSD)*, NAT'L INST. MENTAL HEALTH, http://www.nimh.nih.gov/health/topics/post-traumatic-stress-disorder-ptsd/index.shtml (last visited Mar. 17, 2014) (explaining PTSD); *see also* Agata Blaszczak-Boxe, *Drone Pilots Suffer PTSD Just Like Those in Combat*, LIVE SCIENCE, http:// www. livescience. com/ 47475-drone-operators-develop-ptsd.html (Aug. 20, 2014, 5:20 PM) (providing specific examples of soldiers who piloted drones and experienced PTSD as a result).

collateral damage to civilians, but instead just send the zeroes and ones over the internet and we accomplish the same thing, well, yeah, that makes sense.

SHANNON FRENCH: And maybe we don't care how callously we feel…if in fact in the real world—with an outcome with saving a lot of lives and including again vulnerable population lives.

MICHAEL SCHARF: Well, let me then turned to Mike Newton. Mike, you've got a new book about proportionality in the laws of war. Who, by the way, is the publisher of that?

MICHAEL NEWTON: That would be Oxford University Press, and it makes a great Saint Patrick's Day present.

MICHAEL SCHARF: So, Oxford's got this broadcast down. But let me ask you, if the harms caused by a cyber-attack would sometimes rise to a physical level that might justify a conventional military response— is that possible?

MICHAEL NEWTON: It's theoretically possible, but this is the issue that Shannon was just edging up to. The entire corpus of the laws and customs of war really is— designed to regulate kinetic hostilities, to protect innocent civilians, and to keep the thread of humanity. Even in the middle of intense armed conflict for all commands and for all persons with some core, there's a fundamental recognition of basic human dignity and human rights. And the problem is in cyberwar that when you begin to talk about taking zeroes and ones, as Peter correctly says, and using them to inflict real physical damage, and then talk about applying the laws and customs of war in response to that, that's a paradigm shift in response to the paradigm shift.

MICHAEL SCHARF: But, let me make this more concrete, Michael. What if the cyber-attack by the United States didn't just damage the nuclear research that was going on, but actually caused the nuclear reactor to blow up? Now what?

MICHAEL NEWTON: Well, you get two huge problems: one is the problem of causation. Was it caused by private actors, public actors, because of the basic law or principle that all of your activities must be directed at all times against lawful combatants or the participants in the conflict.[37] In the cyber context, it's enormously complex in real time to run that back and figure it out exactly in terms of causation because of how broadly that expands.

MICHAEL SCHARF: So, what happens like in the Stuxnet where a couple months later somebody leaked it out?[38] I don't know if it was

37. Derek Jinks, *State Responsibility for the Acts of Private Armed Groups*, 4 CHICAGO J. INT'L L. 83, 83 (2003).

38. *See* David E. Sanger, *Obama Order Sped Up Wave of Cyberattacks Against Iran*, N.Y. TIMES (Jun. 1, 2012), http:// www. nytimes. com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html.

the Obama administration bragging about it or if it was someone who's unhappy about it that just leaked it, but these things do leak out. So, let's say the US does the attack in cyber space, it blows up the nuclear reactor in Iran, and then it leaks out that it was the US and not some non-state actor that was behind this. Then what?

MICHAEL NEWTON: But, that's one of the attractive beauties of cyber operations. It's designed not to blow up the nuclear reactor in Iran, and it didn't, in fact. There was no human being—no effect whatsoever. So, it's a highly theoretical question.

MICHAEL SCHARF: So, you won't take the bait then?

MICHAEL NEWTON: Peter talked about the responsibility of Cyber Command. I think that's the key authority. Immediately as soon as you move into the military context, you have got to articulate what is the mission statement, what is the scope. And from that, the specified tasks, precisely what is the military supposed to accomplish, and the implied tasks, the things that are necessarily implied, that have to happen in order to accomplish that.

MICHAEL SCHARF: All right so, let me switch it around here—

MICHAEL NEWTON: Within the context of cyberwar that is very difficult, if not impossible, to do.

MICHAEL SCHARF: So, Mike, let's switch it around. Let's say it was Iran who does the cyber-attack against the United States, and there's maybe a nuclear reactor that blows up. Right? Because you're focusing on well, the US won't do this, but I'm just trying to get to the question of what if some country does it to another. Does that then equate to an armed attack?

MICHAEL NEWTON: In theory, yeah, if you cause the legal languages that the damages are of the scope, magnitude and intensity to equate to an armed attack. But, the problem is that by definition these are not armed attacks; they are cyber-attacks, denial of services, or clogging of computer networks. It takes an incredibly—and in fact I would say it would be the worst cyber-attack in history if it did actually unintentionally result in some physical damage.

MICHAEL SCHARF: Peter, do you think that there would ever be a cyber-attack from one country to another that would result in physical damage? Is this just a hypothetical or is this something that's perhaps possible and more even likely?

PETER SINGER: Well, I mean, it's not a hypothetical because you've been talking about a real-world case where it happened. I mean, Stuxnet was a cyber-attack that resulted in physical damage.[39] Now, it was what we would describe as an act of espionage, not war, but you can get back and forth on that and that's reflecting domestic

39. *See Stuxnet: Computer Worm Opens New Era of Warfare*, CBS NEWS (Jun. 4, 2012), http://www.cbsnews.com/news/stuxnet-computer-worm-opens-new-era-of-warfare-04-06-2012/.

legal concerns. But, to your broader question of when does a cyber-attack become an act of war, in the meaningful term of "Oh, it just happened in cyber but it means we've got to go to war." The reality is—so, first, this is not always so clear when you're talking about regular armed warfare. Think about the example of if someone fires a weapon, a rifle, or what not at my nation, that's of course an act of war. Well, actually, no. We have border disputes all the time. Okay, well, actions that have no weapon use can still be an act of war. You could, for example—if you deliberately flooded your neighbor's entire country, and it was a cascade that caused thousands of lives to be lost, no one would say, "Well, goodness, there was no gunpowder there, so it's not an act of war." We judge it by the effects. But, in the book, where I wrestled with this, in the end there's this quote from a guy who puts it best: "in the end, the President's going to decide."[40] And, that's—it comes down to a human judgment when it's a war, when it's a state of armed conflict, when it's something else. But, it's a human decision. The concern, though, to one of your prior points, and where it ties in with drones, is not so much how the operators look at this but how the politicians look at it. Whether you're talking about a drone or a cyber-weapon, it's very seductive to politicians because it seemingly offers an effect without risk. As we've seen with whether it's drones or cyber weapons like Stuxnet, what you often want to happen is not always the way it plays out, whether it's physical collateral damage or the fact that this covert operation leaked or the fact that this weapon that was designed only to go after one target in the world popped up in twenty-five thousand other computers around the world,[41] which is not something that would happen with a regular bomb. It's just a complex space. But, again, to me it's—if we want to worry about the human views of it, it's not so much the operator. It's us. It's the body politic and the politicians.

MICHAEL NEWTON: Michael, this is Mike, just one clarification—

MICHAEL SCHARF: Mike, we need to take another a short break now and then we'll start the conversation back in just a minute. I love it when we can end, and things are hot and heavy because that means the listeners will stay tuned. We'll be right back.

MICHAEL SCHARF: This is Michael Scharf, and we're back with "Talking Foreign Policy." I'm joined today by Peter Singer in D.C., Mike Newton in Nashville, Shannon French and Milena Sterio are with me here at WCPN ideastream in snowy Cleveland. We're talking

40. P.W. SINGER & ALLAN FRIEDMAN, CYBERSECURITY AND CYBERWAR: WHAT EVERYONE NEEDS TO KNOW 126 (2014).

41. *See* Mathew J. Schwartz, *Cyber Weapon Friendly Fire: Chevron Stuxnet Fallout*, DARK READING (Nov. 12, 2012, 2:30 PM), http:// www.darkreading.com/attacks-and-breaches/cyber-weapon-friendly-fire-chevron-stuxnet-fallout/d/d-id/1107339?.

about cyberwar. Now, just before the break Mike Newton, our Colonel from the JAG wanted to jump in and add something, so Mike, here's your chance.

MICHAEL NEWTON: So, I just want to really clarify, very briefly, one of the things that everybody is alluding to, but I want to say very clearly in legal terms. The big difference between acts short of an all-out armed conflict in response to a cyber-attack or in a cyber-context is that the law actually only permits the actor to do what's strictly required—what's narrowly tailored only to ameliorate the threat. That's the law of self-defense, the classic law of self-defense, the classic law of counter-measures, and the classic law of embargo short of armed conflict.[42] The point is that that rule and the legal construct and all of the other range of laws and customs of war change dramatically once we recognize we're in the context of an armed conflict. That's why this distinction matters a great deal because in the cyberwar context, it's easy to say we're only allowed to use that degree of force or cyber technology necessary and narrowly tailored to strictly eliminate the threat. The problem is it is so incredibly difficult to ascertain precisely what that means in that context.

MICHAEL SCHARF: And that's a great segue for what I wanted to talk about next, which is the question of how international law applies to the conduct of a cyber-war. Let me begin with Shannon. You have written books about this. What was it, the last book? *The Code of the Warrior*.[43] Is it possible to apply century's old criteria of just war tradition[44] to something so new and different like cyber warfare, a form of war made possible by advanced technology?

SHANNON FRENCH: Well, this is a drumbeat of mine. This is something that I try to get out there as much as possible. There is nothing new under the sun in the way that is relevant to changing the just war tradition. What I mean by that is of course we have new technologies, of course we have new forms of weaponry, but the trick is not to then say, "Oh, my goodness, we must create a whole new theory of just war." It's to figure out how to apply these tried-and-true principles to these new advances. For example, we've already been alluding to many of them. The core principles of just war, things like proportionality,[45] discrimination,[46] right authority, [47] all of that is

42. The Just War Theory "deals with the justification of how and why wars are fought." There are both moral components and physical components to the theory. *See* Alexander Moseley, *Just War Theory*, INTERNET ENCYC. PHIL., http://www.iep.utm.edu/justwar/ (last visited Mar. 16, 2015).

43. SHANNON E. FRENCH, THE CODE OF THE WARRIOR (2004).

44. *See* Moseley, *supra* note 41.

45. Proportionality "concerns how much force is morally appropriate." *Id.*

still valid and true. And, it hasn't changed just because we have this new way of doing it. I would just like to emphasize again something that Peter mentioned earlier. It is the job of the just war tradition to try to limit the scope of war and also to hopefully, it seldom actually has succeeded at this, but actually to limit the number of wars we get ourselves into. Anything that lowers the bar towards getting into a war is very worrisome ethically. I would also add finally on this point that when we see groups with greater technologies, and especially world powers using them in a powerful way against weaker groups or groups that don't have the same technologies, that asymmetry can create new enemies, as well. So, where it may be appealing to a policymaker since we didn't put any boots on the ground, we may actually be leading to more deaths, more threats because we are putting ourselves out there in a way that is going to make more people angry at us as a nation.

MICHAEL SCHARF: And this is a theme that Peter makes in his book as well.[48] Peter do you want to elaborate on that?

PETER SINGER: Well, a of couple things. The first, in complete agreement that you shouldn't try to see these discussions like, "Oh, we need to write a new Geneva Convention for the cyber world." One, that doesn't make sense, and two, it's completely unworkable. Again, I'm in agreement with the idea to pull from the values that have been tried-and-true. We do need to understand, though, that there are new kinds of challenges that were never contemplated. One is the idea of disaggregating the military[49] versus a civilian. Makes perfect sense when you're thinking about conventional weapons, but the Internet itself is civilian, so you will inherently be using— you can't— if 98% of US military communications go over the civilian owned and

46. Discrimination in just war "concerns who are legitimate targets in war." *Id.*

47. Right authority, also known as "legitimate authority,[it is] the securing of peace and the uplifting of good." *See* LUKE BRADLEY CAMPBELL, JUST WAR, LEGITIMATE AUTHORITY, AND NON-STATE ACTORS iii (2011). The basis of legitimate authority "acknowledges that governments and law are the foundation of the good life." The presumption of order and security necessitates that war must sometimes be waged by a legitimate authority in the defense of such; this idea is a moral concept. *See also id.* at 6.

48. P.W. SINGER & ALLAN FRIEDMAN, CYBERSECURITY AND CYBERWAR: WHAT EVERYONE NEEDS TO KNOW 122–26 (2014) (discussing application of old laws to new technology).

49. Disaggregating the military means to give military satellite tasks such as communications and navigation to smaller military spacecraft. *See* Sandra I. Erwin, *Air Force Continues to Ponder New Ways to Buy Satellites*, NAT'L DEF. MAG., Oct. 13, 2013, http://www.nationaldefensemagazine.org/ blog/ Lists/Posts/Post.aspx?ID=1297.

operated Internet,[50] this is the mashing up of this already. The other, and this is where again there's a cross with drones, is that it's not that there's no decision making. It's that the locus of decision making is now moving both geographically, and now when you move into both autonomous robotics but also cyber weapons, chronologically in ways that make it very difficult for older laws to wrestle with. So, Stuxnet was a weapon that, so to speak, was fired, and its effect played out months later. It's a really interesting space. There are a lot of challenges to it. But, I'm the son of an army JAG officer, and one of the things you can argue on pretty much everything is that there's this idea that the law is conclusive on something. No. That's—there are huge amounts of arguments on everything from the Geneva Conventions to what the Constitution says about everything from abortion to gun rights. This is a new manifestation of it, so when someone says this is legal or this is not, that's their interpretation of the law. Unfortunately, the real world is much more difficult to figure out.

MICHAEL SCHARF: Shannon, did you want to add something?

SHANNON FRENCH: Well, I agree with all of those points. I simply wanted to add that often times the great difficulty, but the important work to be done, is to figure out what is the right analogy. If we have seen different kinds of weapons in the past and we have hopefully figured out how we ought to respond to them, how do we find the analogy with these new forces and then use those laws correctly?

MICHAEL SCHARF: Now, I have to point out that not everybody agrees with the view that the current law is sufficient for this new threat. And, if you go on blogs there are superstar experts in the field that are debating this issue, so let me turn to Milena. How would you make the argument that there needs to be a new Cyber Geneva Convention, and what would be its essential provisions?

MILENA STERIO: Sure, so the Hague Law,[51] the Geneva Convention, and the treaties that we have currently were written so long ago before nuclear weapons, before drones, and certainly before any kind of cyber weapons. There really—the drafters never contemplated anything like what we're seeing today. There is— I should mention that there is a treaty called the International Convention on Cybercrime[52] which was adopted in 2001 by the

50. Eric Talbot Jensen, *Cyber Warfare and Precautions Against the Effects of Attacks*, 88 TEX. L. REV. 1533, 1534 (2010).

51. The Hague Peace Conferences produced multiple provisions of the customs and international laws of land warfare. *See* Hague Convention (IV) Respecting the Laws and Customs of War on Land and its Annex: Regulations Concerning the Laws and Customs of War on Land, art. 1. Oct 18, 1907, *available at* http://www.icrc.org/ihl/INTRO/195?OpenDocument.

52. The International Convention on Cybercrime is an international treaty in regards to criminal acts through "computer systems, networks, or

Council of Europe, but that convention really falls short of detailing everything that you would want in a in a comprehensive multilateral treaty. So, some of the main points of view—

MICHAEL SCHARF: Let's focus this. It's low-level cyber-attacks, not this giant thing. We're talking— its low level—

MILENA STERIO: We're talking about low-level cyber-attacks and encouraging member states to prosecute those at the national level. So, if you want to talk about a big multilateral treaty on cyberwar/cyber-attacks, first you would want to carefully define: "what is a cyber-attack?" and "what is cyberwar?" Then you might want to think about prohibiting certain types of cyber-attacks, similar to how certain types of attacks are prohibited under traditional conventions. So, you might want to prohibit cyber-attacks on things like hospitals, infrastructure, airlines, and things where you basically think that the civilian suffering is going to far outweigh whatever military objective you're trying to achieve.

MICHAEL SCHARF: And then, you would basically say that any country that did that was the equivalent of someone who commits genocide or crimes against humanity. It's a violation of international law. Their leaders could be potentially prosecuted.

MILENA STERIO: Exactly. So then, you would want to somehow tie it into the existing international law and basically say, "Well, then that's an act of aggression that's illegal under international law." And the leaders now face individual international criminal responsibility.

MICHAEL SCHARF: So, Peter, you're against that approach. What do you think is the problem with it?

PETER SINGER: What we push for in the book is the idea of grafting. Grafting is something that both studies in international relations have found to be more effective in building international cooperation but also it's taken from horticulture. And it's the idea that, let's just be blunt, if you tried to create an entirely new Geneva Conventions right now, you'd never get any agreement on it. You would not get any ratification of it by the key states. A good example in the cyber world is that NATO asked a group of top, really smart minds to come up with a manual for the legal side of cyber warfare: the Tallinn Manual.[53] It's in many ways a great document, a lot of

---

data." There is no legal bind to the treaty until the country's government ratifies the treaty. *See International Issues: Cybercrime*, CTR. FOR DEMOCRACY & TECH. (Feb. 15, 2011), https://cdt.org/insight/international-issues-cybercrime/.

53. Relevant provisions of the Tallinn Manual include the following:

- Nations cannot knowingly use cyber infrastructure to harm other nations
- Nations may be held responsible for cyber-attacks done by private agencies directed against other nations; if any individuals or actors that

interesting stuff in it, and then what happened? The United States, a NATO member, said, "Yeah, but we're not bound by that." So the point is that grafting— it's instead of trying to plant a new tree, it's to build off of what already works effectively. And so, the example that was mentioned there would be the cybercrime treaty that's— there's some trying to bring new members in. What I'm getting at is that I would love the idea of trying to combine legal thinking with real-world politik, and that's the challenge of this space. We need to not approach it in siloed arguments from our own issue areas, but understand what's possible or not possible both on the technical side, on the political side, and also on the legal side and bring them all together. One last point, it's sort of a fascinating one that illustrates the kind of cool but crazy aspects of this space. When we have an illustration of what we might want to build into a treaty that would not find its space in a traditional Geneva Conventions approach is when we say, "Okay, there are certain things we don't want to target." In regular national laws it's—we shouldn't target civilians, and there are really important things not to target among civilians like ambulances, churches, or hospitals. You particularly don't go after those. In cyber, we typically say things like hospitals and the like, but the one that really matters on a huge level that most everyone would agree to is the financial system. The only nation that wouldn't be taken down by an attack on anyone's financial system because of the ripple effects would be North Korea.

MICHAEL SCHARF: Milena, you wanted to add something.

MILENA STERIO: Just a very quick note. I mean, I definitely agree with Peter that it would be extremely difficult and probably impossible as of now to negotiate a big multilateral treaty. But an approach which would maybe fit under that idea that Peter's talking about is maybe to use soft law[54] instruments to supplement what we already have. So, it is much easier to negotiate codes of conduct guidelines and things of that sort that can then supplement, for example, the cyber convention that we already have. And the hope— the goal would be that over time, if states then are using that kind of

---

commit such acts are under state direction, then accountability for the acts will be attributed to that state

- Any cyber attach that causes harm to people or objects will justify a response with force, though cyber operations that merely annoy or inconvenience states will not justify armed responses

See COUNCIL ON FOREIGN RELATIONS, TALLINN MANUAL ON THE INTERNATIONAL LAW APPLICABLE TO CYBER WARFARE (2013).

54. Soft law is usually seen as an agreement upon a rule that is not binding. *See* Gregory Shaffer & Mark Pollack, *Hard vs. Soft Law: Alternatives, Complements, and Antagonists in International Governance*, 94 MINN. L. REV. 706 (2010).

soft law (the guidelines, the codes of conduct) that maybe at some point we'll be closer to a customary norm of law.

MICHAEL SCHARF: As I understand it, the Tallinn manual that Peter mentioned is something of that sort. Mike Newton, you've studied this. Do you have particular criticisms of any of the provisions of the manual?

MICHAEL NEWTON: I think it's good. I agree with Peter. To extend the horticulture metaphor, the fig leaf of law here is really no solution. We feel really good that we've got a new convention, we've got some software, and we've got some codes. The problem is that we haven't really dealt with the relevant actors. The big problem in the Tallinn Manual as well as the ICRC whole study about when a civilian crosses the threshold into legally participating in conflict to the extent that they can be targeted,[55] the direct participation study, is exactly the same thing as discussions for close to a decade. And in the end, no real agreement. So, I think the—this approach that says, "Well, we need more laws" is kind of quixotic. I agree with Peter about the financial system. The other one that I would say that almost everybody would agree with ought not to be messed with is this system that regulates transnational aviation flight. How many flights around the world go down with all kinds of consequences? That's a no brainer. The problem is that all the things that we want to protect in a real all-out cyberwar become the indirect victims of an all-out cyberwar. There's no real way in an all-out cyberwar when you shut down the electric grid, at least theoretically, to control who that affects and how that affects them. So, that's the core problem with trying to reach any real binding legal code of conduct, if you will.

MICHAEL SCHARF: So let me throw out one other issue that sort of keeps me up at night. And, that is if we're spending all this money, if we have Cyber Command, and we're making it have major military approach to the possibility of cyberwar and cyber-attacks, can that be used as a way to erode our own civil liberties and privacy? And I know, Shannon, you've been thinking about this. What would you say?

SHANNON FRENCH: Well, yeah. I mean, this is a very big concern because always you do have to balance security against other rights issues like privacy. But, something that Peter mentioned earlier is really important for us to remember, and that is how easily you can hype these kinds of fears. When you think about that survey that Peter mentioned where people are more afraid of a cyber-attack than they are of these very real urgent threats that we are not giving money towards and that are not getting enough attention, focus, or

55. NILS MELZER, INTERPRETIVE GUIDE ON THE NOTION OF DIRECT PARTICIPATION IN HOSTILITIES UNDER INTERNATIONAL HUMANITARIAN LAW (2009), *available at* https:// www.icrc.org/eng/ resources/ documents/ publication/p0990.htm.

resources to try to address them, that's actually quite horrifying.[56] And if you put in front of people in very stark terms: "this is how much money you are spending as a nation to prevent this cyber-attack, which is in many ways not likely to happen and would be not even in the interests of the groups you're afraid of, in the end of the day when you could spend that same amount of money and save this many lives if you put it towards cancer research or this much benefit towards education and so forth," it would be very frustrating. And yet, if you scare people enough, they will hand over their privacy incredibly easily. And I'll just add one other point which is I think this is where the lack of transparency is also a bit terrifying for ordinary civilians, which is that we don't know exactly how much privacy we have already given up.

MICHAEL SCHARF: All right so we're almost out of time. I want to go back to Peter Singer, the author of the book *Cybersecurity and Cyberwar: What Everyone Needs to Know* and say Peter, you've got the last word. Where do you think we're going to be in ten years in terms of this issue? If we're having this broadcast ten years from now, what are we talking about?

PETER SINGER: Well, we'll probably be downloading it into our brains. In all seriousness, the one word that I would—that I hope we'll end on at that point is "resilience." You can think about resilience in terms of the physiological or the psychological. The physiological is that I hope we have an approach to cybersecurity with what it means more broadly that goes beyond just thinking we can build up higher walls, we can deter the danger, or we can scare it away. Your body expects that it's going to be in a dangerous world, and so it has layers of defenses, and it does everything from isolate the attack to it has an internal monitoring system to a triage. There are all different ways, and so we've got to move out of this mentality of just thinking that I can keep it out. The more important meaning of resilience is a psychological side. It's—you can think of the parallel in the British approach to terrorism versus ours. "Keep calm and carry on." Resilience in a psychological way is saying, "I expect that there will be bad things in the world, but it's all about how I'm going to power through them. And if I get knocked down, how I'm going to get back up rapidly." That's really where I hope this shifts to. So, the bottom line here is that as long as we are using the Internet, and ten years from now we will be, we will face these threats. And so, therefore we have to work to manage them and be more resilient about them.

MICHAEL SCHARF: That's a great final note. On September 5th, Case Western Reserve University School of Law is going to be having

56. Bruce Stokes, *Extremists, Cyber Attacks Top Americans' Security Threat List*, PEW RES. CNTR. (Jan. 2, 2014).

a day-long symposium on this subject. I invite you to join us live by coming to Case Western, if you're in the Cleveland area, or you can tune in, listen to it, and watch it by webcast anywhere in the world. Meanwhile, if you want to weigh in on the discussion that we've been having or suggest a topic for an upcoming broadcast, please send an email to talkingforeignpolicy@case.edu. I want to thank again our panel of experts: Peter Singer, author of *Cybersecurity and Cyberwar: What Everyone Needs to Know*, Col. Mike Newton from Vanderbilt University, Professor Milena Sterio from Cleveland Marshall College of Law, and Doctor Shannon French from the Inamori International Center for Ethics and Excellence at Case Western. I'm Michael Scharf. You've been listening to "Talking Foreign Policy" produced by Case Western Reserve University and WCPN 90.3 ideastream.