The International Journal of Ethical Leadership

Volume 3 Article 11

2015

Talking Foreign Policy

Talking Foreign Policy Radio Broadcasts: Sept. 6, 2013 and Jan. 31, 2014

Talking Foreign Policy Transcripts

Talking Foreign Policy is a production of Case Western Reserve University and is produced in partnership with 90.3 FM WCPN ideastream. The quarterly program is hosted by Case Western Reserve University School of Law Interim Dean Michael Scharf. This issue of the *Journal* contains the transcripts of the September 2013 broadcast about combatting maritime piracy and the January 2014 broadcast about regulating cyberwarfare. Archived broadcasts (both in audio and video format) of *Talking Foreign Policy* are available at law.case.edu/TalkingForeignPolicy.

Talking Foreign Policy, September 6, 2013 broadcast[1]

Participants:
Michael Scharf
Roméo Dallaire
Rosemelle Mutoka
Sulakshna Beekarry
Milena Sterio

SCHARF: Welcome to *Talking Foreign Policy*, I am your host Michael Scharf of Case Western Reserve University School of Law. In today's broadcast we'll be discussing the persistent problem of maritime piracy. We'll begin our discussion with General Roméo Dallaire, the UN Force Commander who tried to save the Tutsis during the 1994 Rwandan Genocide. Nick Nolte played him in the award-winning 2005 film *Hotel Rwanda*. Since then, General Dallaire has been appointed a Canadian senator, written two best-selling books, and is the founder of the Roméo Dallaire Child Soldier Initiative[2] at Dalhousie University in Nova Scotia. Thanks for being with us General.

DALLAIRE: Thank you.

1. Transcript edited and footnotes added by Cox Center Fellows Aaron Kearney and Nathan Nasrallah.
2. See http://www.childsoldiers.org/.

SCHARF: I would like to start off by asking you to tell us a little about your journey from UN Force Commander to human rights advocate, focusing on child soldiers.

DALLAIRE: It was very much based on the experience in Rwanda. Previous to that, I was a NATO commander, so we were essentially engaged in classic warfare at the end of the Cold War. All these new imploding nations and failing states got us involved in a number of countries. The Rwandan mission that I commanded, which ultimately ended with the genocide in Rwanda, brought me face to face with the ability of human beings to be able to destroy each other on massive scales and with near impunity. Also, the use of youths and children, using youth militias to conduct a lot of this destruction and those traumas of 1994. I was able to then nurture this feeling that there had to be something better in the world than simply letting these catastrophic failures happen, and so I got engaged in trying to get back into the field and trying to prevent some of it from happening.

SCHARF: Now you have written two best-selling books. The first one was *Shake Hands with the Devil*[3] and it's a powerful indictment of the international community's inaction in the face of genocide in Africa. Do you think the world has learned the lessons from Rwanda now that it is twenty years later?

DALLAIRE: It is interesting the way you put it, in a professorial way—they learned a lesson. I think they learned to create some tools that would prevent that from happening. As an example, and I think the dominant example, is the Responsibility to Protect doctrine that was finally approved in 2005 in the General Assembly,[4] which essentially the world signed up to. [It] states that if a nation is massively abusing the human rights of its own people or can't stop it, we and all the other nations under the UN must go in and intervene to protect. So that was an extraordinary product that was brought about. The problem, however, with that is that although they have learned that and they know it's there, they are not applying it. They are not operationalizing it.

SCHARF: So, for example, with respect to Syria, Obama has been saying we have to take action for humanitarian reasons and other countries and

3. Roméo Dallaire and Brent Beardsley, *Shake Hands with the Devil: The Failure of Humanity in Rwanda*. (Da Capo Press, 2005).
4. UN General Assembly, Resolution 63/308, "The Responsibility to Protect," October 7, 2009, http://www.un.org/en/ga/search/view_doc.asp?symbol=A/RES/63/308.

members of our Congress here in the United States are saying it's not legal to do so and we have no obligation.[5]

DALLAIRE: Well, both are wrong. In fact it starts as far back as Libya, as we went in sort of half-cocked sending in air forces, where, in fact Ghadafi said, "I am going to crush these cockroaches."[6] Those were exactly the same words used by the extremists in Rwanda that brought about the Responsibility to Protect. And we should have put boots on the ground to protect the civilians and ultimately not have them [Libyans] bleed in trying to establish some order. Well, Syria offered us exactly the same situation, but we didn't take it up. When I was asked two years ago, which was already six months into the Syrian campaign, "What do you think we should be doing?" I said, "We should be applying Responsibility to Protect, but there haven't been enough people killed to actually provide the politicians in this world who have the ability to intervene to want to intervene." So the will to intervene is not behind the Responsibility to Protect.

SCHARF: Now, in Rwanda we were talking about 800,000[7] slaughtered in four months. In Syria the recent estimates were 1,400 people were killed by recent chemical weapons attack, but maybe 100,000 people have been killed since the fighting began in March of 2011.[8] How many do you think would be enough before the scales tip in favor of some sort of humanitarian intervention?

DALLAIRE: You are hitting the heart of the problem. How many humans have got to suffer for those who have the capability of responding, and considering those humans equal to them, to be worth us taking those risks and going in and helping them? And we haven't broken that code. We've found means of maybe how we should do it, but we haven't found the willingness of our leaders, who are politicians who are risk averse [that] are not statesmen who are prepared to take risks to demonstrate responsibility, demonstrate a lot of willingness to move to a higher plain than self-interest. Those statesmen aren't there and that's why we are into number crunch-

5. Paul Campos, "Striking Syria is Completely Illegal," *Time*, September 5, 2013, http://ideas.time.com/2013/09/05/obamas-plan-for-intervention-in-syria-is-illegal.
6. "Libya Protests: Defiant Gaddafi Refuses to Quit," *BBC News*, February 22, 2011, http://www.bbc.co.uk/news/world-middle-east-12544624.
7. Roland Adjovi and Nandor Knust, "Rwanda," in *Max Planck Encyclopedia of International Law*, edited by R. Wolfram (Oxford University Press, 2013).
8. Josh Levs, *Syria* "'Red line' debate: Are chemical weapons in Syria worse than conventional attacks?" *CNN News*, August 28, 2013, http://www.cnn.com/2013/08/27/world/meast/syria-chemical-weapons-red-line/index.html.

ing. And to be quite honest, the recent gas attacks and chemical attacks are a crime against humanity. So fine, bring in the International Criminal Court, but that is not the red line in reality if we are responsible towards the Responsibility to Protect. The red line was two years ago and we didn't intervene. Now it's nearly impossible unless you get a ceasefire and move in a separation force under the UN to permit then a future negotiation stage.

SCHARF: Let's now talk a little bit about child soldiers, because that's what you have been working on lately. Your recent best seller *They Fight Like Soldiers, They Die Like Children*[9] is about the problem of child soldiers and you make the case that the international community is ignoring that problem at its own peril. Can you elaborate on that?

DALLAIRE: It's very much peer focused. Many of the nations that are seeing the use of child soldiers, either by government forces or nonstate actors, are countries where the demographics are such that 50 percent, sometimes more, of the population are under the age of eighteen, which is the age under the Optional Protocol on Child Rights where children are not to be recruited nor used in operations and conflict.[10] So you've got this massive reserve of youth that is being abused and they are seeing each other so used and it can sort of perpetuate itself because you know, "I went through it so maybe this is the way we can do it and let's keep it going." So the greatest risk of the child soldiers is the fact that it can be an instrument of war, a weapon of war that can sustain itself time after time, because the demographics are permitting it to happen.

SCHARF: Yes, and you have gone from looking at child soldiers to now focusing on an even more narrow problem, that of child pirates, maritime pirates. So your recent editorial in the *Toronto Globe and Mail* was headlined "Child Pirates are Everybody's Problem."[11] Can you tell us why we should be concerned about child piracy?

DALLAIRE: Because the impact of them is of course an economic one that is directly related to our self-interests, our economic self-interests, but also the child piracy has this funny way, in my perspective, of going beyond its

9. Roméo Dallaire, *They Fight Like Soldiers, They Die Like Children* (Walker and Company, 2011).
10. UN General Assembly, Resolution 44/25, "Convention on the Rights of the Child," November 20, 1989, http://www.un.org/documents/ga/res/44/a44r025.htm.
11. Roméo Dallaire, "Child Pirates are Everybody's Problem," *Toronto Globe and Mail*, February 10, 2012, http://www.theglobeandmail.com/commentary/child-pirates-are-everybodys-problem/article544972.

borders. This is not a border-restricted use of children, like let's say child soldiers which would be in a nation, a conflict zone, and apart from the LRA who have been sort of very mobile . . .

SCHARF: That's the Lord's Resistance Army, which operates in northern Uganda and Sudan.

DALLAIRE: Yes, and they are now in the Central African Republic and are being supported by Sudan to maybe ultimately subvert South Sudan. So it gets pretty complicated, but apart from that particular group, the others are very localized. So the question is, with pirates it is not, it spreads. We are seeing Western Africa now also seeing a surge in the use of piracy and the availability again of youths who can be given empowerment by weapons and indoctrination.

SCHARF: So what percentage of pirates are children would you say? Is it around 50 percent?

DALLAIRE: Well, the figures seem to be about a third or so, but imagine when they are on the seas and you got people on big ships, naval ships, or other ships, and they are protecting and opening fire against the pirates, are they able to discern whether or not this is an adult or a youth? What we are seeing are a lot of these kids being killed.

SCHARF: When they do discern who is a child and who is an adult, many of the countries have a policy that is sort of like the local fishing policy, when you catch a fish that's too small you have to send it back, so they call it "catch and release." Do you think that is the right way to be treating the juvenile pirates?

DALLAIRE: Absolutely not! In fact, the link that brought us in to child piracy comes from child soldiers, which is what is happening on the ground before they're actually deployed. If on the ground you have an atmosphere that permits this to happen, you have recruitment and rerecruitment, of course they are going to go to sea and you have a problem. So how do we curtail it on the ground? I am a strong advocate for a nonpunitive juvenile type of court process in which the youth that are taken, they are not incarcerated [but] they are held. In the process of this nonpunitive juvenile court, they are given the opportunity of being rehabilitated and reintegrated and ultimately are able to be extracted from that cycle of, if not banditry and piracy, maybe even conflict and fighting, if conflict erupts.

SCHARF: What about the adults? What can be done to discourage them from recruiting the children?

DALLAIRE: Take every one of them, throw them in jail, and throw away the key!

SCHARF: So in fact, what we're hearing is that some courts around the world are increasing the penalty when an adult pirate is found on a ship with children. They're treating that as an aggravating factor. And that can send a signal that might have a deterrent effect. It is time for a short break. When we return we will bring three of the world's leading experts on piracy into the conversation, stay with us.

SCHARF: Welcome back to *Talking Foreign Policy*, brought to you by Case Western Reserve University and WCPN 90.3 Idea Stream. I'm Michael Scharf, and I am joined in studio by General Roméo Dellaire, Judge Rosemelle Mutoka of Kenya, piracy prosecutor Sulakshna Beekarry of Mauritius, and Professor Milena Sterio of the Cleveland Marshall College of Law. We are talking about the problem of child pirates. Let me begin with Sulakshna Beekarry; to prepare for your first piracy cases in Mauritius I understand that your government studied the best international practices and adopted a state-of-the-art approach. Walk us through what that means. What does your government do when an accused pirate appears to be a juvenile?

BEEKARRY: I have to say, we have not faced that issue in practice yet, but it is an issue which is expected and guidelines have been discussed, a draft put up, but not yet finalized with other states of the region, in particular the Seychelles. Now, these guidelines would include what to do in that situation and how to determine an age, going from teeth examination and a lot of other medical ways of determining the real age.

SCHARF: That's because everybody they catch, knowing that there's often a catch and release policy, will say, "I may have a beard and a low voice but I am only fourteen," right?

BEEKARRY: And how do you know who is speaking the truth and who isn't? But I feel as well that the decision might come much earlier. It might come on a decision to accept that at transfer or not where juveniles are involved, but this remains to be seen in the future.

SCHARF: Judge Rosemelle Mutoka, you spent 2011 in the United States as a distinguished jurist in residence at Case Western Reserve and we are

glad to have you back in Cleveland. You have presided over seven piracy cases in Kenya. Were any of those juvenile cases?

MUTOKA: Thank you, Michael. Yes, I have presided over seven cases. I have concluded three and unfortunately none of the three have had any juveniles. But at least two of them had juveniles. I took plea in two cases. Before my court, it is not very common for the pirate defendants to claim that they are juveniles. In fact, they avoid saying that and you perhaps just want to look at them and because of their size and the way they appear, you perhaps think you should take them for age assessment, because they will not tell you, that was not my experience.

SCHARF: Now that is very interesting, so where I thought everybody would want to claim to be a juvenile, either because they are fearful of the pirates that hired them or for other reasons, they are all claiming to be adults when you suspect they are actually under age?

MUTOKA: It is an interesting phenomenon, and the reason for it became evident later in the process. When they come in, we had the challenge of communication because they speak Somali and they can't communicate in the language of our court, English. What became evident to us later was the fact that they did not want to be separated from each other. They knew that if they were classified as juveniles, then they would be taken to a juvenile facility. That meant they would be kept away from their comrades, which they did not want. So they would not admit they were juveniles.

SCHARF: Now, from our conversations I know that you had all sorts of special care for these convicted pirates. You sent them to special prisons, not as part of the regular population. You helped educate them so that if they were illiterate they could learn to read and write. What was your thinking on that?

MUTOKA: It is because we had juveniles among the convicted pirates, and we wanted to make sure that the juveniles in particular were protected and received special care. It was easier to group them all together in a special facility because of the issue of language. If you had them together in one place it was easier to arrange for an interpreter to be with them and to be able to communicate with, not only just among themselves and the prison authorities, but also when they had people visiting, because there was a lot of interest in these cases and we had a lot of people coming from all over the world.

SCHARF: How long were the sentences usually?

MUTOKA: The first case we had, the first case registered in Kenya, was 2007. The first conviction was in 2009 and each one of them was sentence to serve twenty years imprisonment and immediately they appealed. Subsequently they received sentences between five and seven years, and right now that seems to be the trend. There is one case from about two years ago where the sentence was to serve twenty years, and the only reason is because people died as a consequence of their acts of piracy.

SCHARF: So there were murders? They were convicted of murder?

MUTOKA: No, not murder. They were charged with piracy not murder, but people were killed during the attack.

SCHARF: When these pirates are in the Kenyan jails as part of rehabilitation you do educate them? You teach them to read and write? Is that part of it?

MUTOKA: Yes, that is part of it.

SCHARF: So let me ask this—it's been said that short sentences and decent jails, three square meals with educational opportunities, is not much of a deterrent for people facing famine in their own country. Some have even compared the treatment of the Somali pirates in Kenya, in the Seychelles, and in other countries, as similar to going to university.[12] Is that a fair criticism?

MUTOKA: Well, I do not agree with that. I think that is a very simplistic approach to what has been done. Actually, when you think about the fact that in Somalia there is a complete breakdown in law and order and most of these young men that are used to committing piracy offenses are not educated, so they look for something to do. If you take out [these men,] it doesn't matter how many you take out, because there are still others available. So it's not so much the fact that you think you are going to pass a message to people who really don't care. They are looking for a livelihood, so for them that is collateral damage, you move on, so I think that argument is simplistic when you look at what's happening in Somalia.

SCHARF: So prosecution is not really going to deter anybody no matter what the penalty? In the US they have given some life sentences,[13] for

12. Jessica Hatcher, "Somali Pirates Find Life in Kenyan Jail More Comfortable than on Ocean Waves," *The Guardian*, August 16, 2013, http://www.theguardian.com/world/2013/aug/16/somali-pirates-kenya-jail-indian-ocean.
13. Brock Vergakis, "Jury Recommends Life Sentences for Somali Pirates," *USA Today*, August 2, 2013, http://www.usatoday.com/story/news/nation/2013/08/02/somali-pirates-jury-life-sentences/2613527/.

example, and the prosecutors in their closing arguments said, "We need to give them the most serious penalty." In fact they were asking for the death sentence in order to send a signal back in Somalia that piracy won't pay. What I hear you saying is, they are not listening in Somalia. It doesn't matter what signals the prosecution is sending in foreign courts—that's not being heard by the populations that are resorting to piracy.

MUTOKA: I am not saying that it's not effective. I do believe, of course, that it may be a deterrent, but I don't think it's a deterrent to the extent that you say, if you give long sentences, of course that would stop them. Because these are desperate young people who are looking for a livelihood, so my argument and my experience is that they are contrite about the things that have happened. If you talk to them one-on-one, they will tell you that and most of them—who have been sentenced by Kenyan courts—have tried to get something else to do because, of course, now after educating them and talking to them, they feel that there's something else they can do with their lives. Somalis' are enterprising people; they are very hard working people.

SCHARF: Do they obtain employment in Kenya or do you send them back to Somalia after they have served their sentence?

MUTOKA: They are usually sent back to Somalia, but you know Kenya has a unique situation where we have Somali-Somalis and we have Kenyan-Somalis and, of course, the only difference between them is the border. They speak the same language. So, where as we make orders for repatriation and they are sent back, but you know the systems we have in place do not insure that they go back and they stay back in place in Somalia.

SCHARF: Let's bring Professor Milena Sterio into the conversation. Milena, before the break General Dallaire gave us his prescription for solving the problem of child piracy and we just heard Judge Mutoka's discussion of how Kenya dealt with child and youthful pirates. What would you add to that and do you agree with the approach that they are enumerating?

STERIO: Yes, I do agree with the approaches and it would be great if either one of us could say or do something that would, in the short term, solve the problem of child piracy. That is not the case unfortunately, but we can certainly offer best practices or recommendations. So I think the proper approach is definitely trying to ascertain the suspected pirate's age from an early stage so that they can be appropriately treated, separated from the adult population, and provided with those educational opportunities.

When it comes to the prosecution and then the sentencing, the age of the suspected defendants should definitely be taken into account. Then once we are talking about sending them to an appropriate correctional facility to serve their sentences, they should definitely be sent to a facility for juveniles where those educational rehabilitation opportunities are present. It might be easier said than done but…

SCHARF: How do we know what the line is between a juvenile and an adult? Are we talking about eighteen years of age?

STERIO: So there is really no consensus in the international community as to the appropriate age of minimal criminal responsibility. There is a United Nations convention called the Convention on the Rights of the Child[14] that defines a juvenile as anybody who is under eighteen, so under that convention the age would be eighteen. However, when it comes to the prosecution treatment of suspected juveniles it's ultimately up to each country and the domestic juvenile system to determine where we set that minimum age of criminal responsibility.

SCHARF: Where do we set that in the United States?

STERIO: In the United States it really depends from jurisdiction to jurisdiction. The minimum could be as early as seven or eight. In some jurisdictions the prosecutor will have the discretion to charge somebody as an adult or not. But certainly in the United States when somebody is fifteen or sixteen, many times when it comes to violent crimes, we treat them as adults.

SCHARF: So, in particular those people who are older teenagers, sixteen, seventeen, seventeen and a half, they are, under the current approach, being treated as juveniles. And the current approach seems to be very black and white, very rigid. Are you advocating a looser approach where you look at facts and circumstances like they would do in the United States?

STERIO: If you adopt an approach that says that you should take the person's age into account, into consideration, that gives you the flexibility to then say, "If you are thirteen we'll give you a lighter sentence. If you're seventeen, which is much closer to eighteen, however arbitrary that age might be, we might give you a slightly harsher sentence."

SCHARF: Okay, now looking at the other side trying to not deter the child pirates, but deter the people that are recruiting and using them, I wonder

14. UN General Assembly, Resolution 44/25, "Convention on the Rights of the Child," November 20, 1989, http://www.un.org/documents/ga/res/44/a44r025.htm.

if we can go back to General Dallaire and focus on what they do to deter use of child soldiers. Recently, the ICC, International Criminal Court, prosecuted a military commander for the recruitment of child soldiers as a crime against humanity, is that right?

DALLAIRE: That's right, but it was a long, long, glacial exercise to get that first convictions in front of the court. But it's also been very difficult to get the court to fully grasp the impact on these children when they are recruited in order to establish the right level of punishment to be given to the adults. One of the reasons why it's difficult to establish that is that when you are bringing these children in as witnesses or they're young, nineteen, twenty, and the court is in the Hague, there's a whole exercise of that, but the defense is also very, very powerful. The defense lawyers are just taking the witnesses apart because of what they've gone through. The girls especially—they've been raped, they've been abused, they have a child or two, they are probably even sick with AIDS. The defense tactics are destroying the witnesses' ability to provide the court with a sustained logical explanation of what has happened to them. In the recent case before the International Criminal Court, that resulted in the prosecution having to withdraw the charge of rape where we know the individual was engaged in rape on a series of occasions, but they just could not get the witnesses to talk about it in court.

SCHARF: The case you are talking about is the Lubanga case.[15] They did end up convicting Lubanga of recruiting child soldiers.

DALLAIRE: Well, he only got fourteen years, while the guy has been using all kinds of children and he's been slaughtering and killing and using them as we were using World War I soldiers, you know, in frontal assaults and having them be blown away. He's been throwing kids back into the bush when they are injured, when they are sick. I mean the scale of what this individual has done is off any of our scales. But he ends up with only a fourteen-year sentence.

SCHARF: So you're saying that that case did not send the signal you wished it had?

DALLAIRE: It's not strong enough yet; it's a start, because we finally got it there, but the handling, how we can handle this is not resolved. How

15. Prosecutor v. Thomas Lubanga Dyilo, Case No. ICC-01/04-01/06, March 14, 2012, http://www.icc-cpi.int/iccdocs/doc/doc1379838.pdf

can we protect the witnesses so that they are going to be credible in front of the court to be able to bring the right sentence?

SCHARF: Now, when countries in the area like Mauritius, Kenya, and the Seychelles are prosecuting the pirates that the United States, the European Union, and Canadians are apprehending, they often are prosecuted not just under the crime of piracy as defined in the UN Law of the Sea Convention[16], but sometimes under other terrorism conventions, for things like hostage taking and hijacking of a ship. Do you think they should also prosecute the pirates for crimes against humanity using the precedent of the International Criminal Court's conviction of Lubanga?

DALLAIRE: This is a great opening to the maturing of the whole international judicial system. Can crimes against humanity be prosecuted in domestic courts? I say, absolutely. In Canada, we recently prosecuted a genocidier from Rwanda, though we did so for multiple murder because we did not have a statute criminalizing crimes against humanity.

SCHARF: Let us go back to our prosecutor from Mauritius, Reshma Beekarry. Would your country be able to prosecute crimes against humanity? Do you have that crime on your books?

BEEKARRY: Interestingly, our thinking has gone in that direction, but with a slight variation. Two years ago, we reached an agreement with the ICC. The ICC will be coming to sit in Mauritius and to have those crimes prosecuted in our local courts. We actually enacted a piece of legislation called the International Criminal Court Act 2011 in Mauritius. And for us, that is a novel idea. We have not quite reached the kind of thinking you are mentioning, Professor Scharf. We could give it thought; but it could take quite a bit of thought.

SCHARF: So there is the possibility that if Mauritius finds itself with a major recruiter of child pirates, you could prosecute that person not just for piracy, but maybe for the crime against humanity of recruiting child pirates, like the ICC has done for recruiting child soldiers?

BEEKARRY: Possibly. I would think the seed for that has already been sown. We have already opened the door for the ICC to come and sit and for us to start looking towards bigger crimes. Until now, these crimes have only been prosecuted in The Hague.

16. United Nations Convention on the Law of the Sea, December 10, 1982, 1833 U.N.T.S. 397.

SCHARF: Now, there is one little wrinkle here. Piracy is normally, as I understand it, a crime committed in international waters, on the high seas. But where is the recruitment being committed? That is on dry land. I will turn this to our professor from Cleveland State, Milena Sterio. Is there any recent precedent for prosecuting dry land piracy?

STERIO: Yes. We actually have very interesting, important recent precedents on that in the United States courts. There have been two cases—one called *Ali*[17] and the other one called *Shibin*[18]—where the defendants were essentially prosecuted for aiding and abetting piracy [facilitating piracy] for acts that they committed from dry land. They were prosecuted under the United States Piracy Statute.[19] One of them was convicted and received a life sentence; and the other one's proceedings are still ongoing. In both instances, the United States courts have accepted this notion that you can commit acts of facilitation on dry land and be prosecuted as a pirate.

SCHARF: Tell us about this Ali case. What was he actually doing?

STERIO: Ali was essentially a hostage negotiator. After there were hostages taken by Somali pirates, he had facilitated the negotiation of the ransom. He, I think, had stepped foot onboard the vessel, but the vessel, at that point, was in the Somali territorial waters. So Ali, the defendant himself, had never acted on the high seas. He had committed other acts of negotiating the ransom from Somalia [dry land].[20]

SCHARF: Wasn't his defense that he was actually trying to facilitate the rescue and the release of the victims?

STERIO: Yes. He basically claimed that he was a good guy, since he was trying to help the release of the hostages. Of course, United States prosecutors did not buy that argument and prosecuted him as a piracy facilitator, instead of a hero.

SCHARF: What is the difference between that case and the situation of insurance companies? If you are insured by a company like Lloyds of London, your vessel is hijacked, and the pirates say, "We want a million dollars for the release of your vessel and its crew." Lloyds of London sends in a hostage negotiator who handles everything. Then, they pay it off and

17. United States v. Ali, 718 F.3d 929 (2013).
18. United States v. Shibin, 722 F.2d 233 (2013).
19. 18 U.S.C.A. § 1651 (West 1948).
20. *See* United States v. Ali, 718 F.3d 929 (2013).

maybe jack up your insurance premium for the future. Everybody lives happily ever after, especially Lloyds of London, who is making a fortune. Why shouldn't Lloyds of London be prosecuted under the Ali precedent?

STERIO: Good question. There is a provision in the United Nations Convention of the Law of the Sea that might make prosecution of insurance companies difficult. In the article that deals with aiding and abetting, it says the defendant must intentionally facilitate. So the insurance companies could make the argument that they are not really "intentionally" doing anything. If anything, they are helping after the fact. But I agree with you; it is a fine line.

SCHARF: Okay. And this guy Ali, I have heard that he was the highest-level pirate prosecuted in modern times. Is that right?

STERIO: That is right. And by the way, the Ali case is the only modern piracy case based on universal jurisdiction in the United States courts. Ali had no nexus and no connection to the United States; the victims were not American, he was not American, and the case occurred in Somalia. So it's really a fascinating case.

SCHARF: So the highest-level guy is just a negotiator. No kingpins, no financiers, no top people have been prosecuted?

STERIO: Not yet. But this opens the door for those kinds of prosecutions, at least in the United States. Now we know that, in US courts, if you commit acts on dry land of aiding and abetting piracy [facilitating piracy], and that can include financing a future pirate attack, you can be prosecuted for piracy.

SCHARF: Judge Mutoka was saying earlier that Kenya has only been prosecuting the foot soldier pirates that they capture, and she is not absolutely sure if there is a deterrent effect. I guess if these people are fungible and they are just the foot soldiers, this is sort of like trying to deal with the narcotics trade by just going after the so-called mules. What we learned in that area is until you start going up to the leaders of the cartel, you were not able to make a big difference. General Dallaire, what does that say about our strategy for combatting piracy? Are we going about it all wrong by just plucking the foot soldiers off from the vessels and prosecuting them?

DALLAIRE: I think that there has got to be concurrent activity. You can't stop prosecuting the pirates and only focus on the financiers. In the case of the child soldiers and the child pirates that continue to be recruited, used,

and later become the casualties, we meet judicial solutions for them as best we can. I think that you have to keep at that to make a responsible action in that regard. However, where we are failing is not pursuing action before the International Criminal Court, equating acts of piracy to crimes against humanity. But the International Criminal Court does not have its own police. If the pirate kingpins are in nation that is a failing state, which does not have a rule of law or a basis for wanting to go after those guys, how do you get into a sovereign state, go after them, and haul them out? That is where there is a nuance that I think has not yet been pursued. When we introduced the Responsibility to Protect doctrine, we began to question whether the Westphalian concept of sovereignty was still absolute. Now, we can intervene for a good reason in certain cases. I would argue that piracy is affecting the international community. We should find a means of actually getting people to go after the bad guys and haul them out.

SCHARF: Now, Judge Mutoka, you have told me that the bad guys [the financiers] are living pretty openly and well in Kenya. Can you tell us a little bit about that?

MUTOKA: Yes. Actually, research has shown that there is a lot of investment of piracy proceeds in Kenya. In fact, statistics show that there is about $2.1 billion that has been invested in Kenya and cannot be accounted for. Of course, then, it has something to do with organized crime. And piracy is an organized crime . . .

SCHARF: So they are not investing it in the stock exchange; they are investing it in narcotics trade and such things.

MUTOKA: Exactly. Then, they invest in real estate. One of the effects of investing in that kind of business or venture is that they have to use illegal means. There is a lot of bribery in order for them to be able to get licenses and to do what they are doing. Eventually, the Kenyan economy is affected very negatively by this.

SCHARF: But your government does not seem to be doing a lot about these pirates who are living openly, driving fancy cars, and living in big mansions. How do you explain that?

MUTOKA: In fact, I think that because of a need to do something about it, the chief justice in my country decided that we are going to set up an international crimes division. He said that one of the main reasons we are setting it up is that the economy is mortally threatened by interna-

tional-related crimes. This division is going to deal with all manner of international-related crimes, including piracy, trafficking, narcotics trade, and so on. I believe that, through this effort, the obligation will fall on law enforcement agencies to do something about these crimes, particularly money laundering. That is where you can be able to get a hold of this kind of investment in Kenya.

SCHARF: We have been discussing some interesting approaches to try to deter the pirates: going after the financiers, the money launderers, and the recruiters. It is time for a short break. When we return, we are going to look at what needs to be done to prevent a resurgence of piracy when the Anti-Piracy Naval Forces have to depart the Indian Ocean, which is going to happen soon. Stay with us. We will be right back.

SCHARF: I am Michael Scharf, and we are back with *Talking Foreign Policy*. I am joined in studio by a former UN force commander, a judge who has presided over dozens of piracy trials in Kenya, the chief of piracy prosecutions of the island-country Mauritius, and an international law professor. We are talking about the scourge of maritime piracy. Let me go back to our prosecutor, Reshma Beekarry. In our final segment, let's step back to discuss the big picture. Reshma, you know the prosecutors from the Seychelles, you know them from Kenya, you know them from several other countries; you have had a lot of discussions in order to get the best practices for your upcoming prosecutions. Do you think that the prosecutions all around the world are having a deterrent effect on piracy?

BEEKARRY: I understand from discussions I have had that views are split on this. I do not think there has been any study to give us a definite answer as to whether these prosecutions are having a deterrent effect. I think some people have been quoting naval operations or the use of private guards as the real reason for a deterrent effect; so there is an issue there. As far as I am concerned, my personal feeling is that they actually do. Prosecutions send out a very strong signal that impunity is not going to be allowed, and you will be made to pay for it.

SCHARF: In the last segment, Professor Sterio was telling us about some of the recent precedents in the United States. Judge Mutoka, can you tell us about what you consider your most important piracy judgments in Kenya?

MUTOKA: I think it is the first one that I handled. It was a case where pirates hijacked a Norwegian ship, which was rescued by the Swedish

Navy. The most interesting thing was that when the case came up for hearing before me, we had to have three sets of interpreters. We had a Somali interpreter for the Somalis; we had a Norwegian interpreter, who communicated with the Swedish interpreter; the Swedish interpreter would then take it back to the court interpreter, who would say it in English. That was very interesting. Eventually, I convicted the pirates and sentenced them to serve eight years imprisonment.

SCHARF: How many pirates, in total, have been convicted in Kenya?

MUTOKA: To date, one hundred and fifteen pirates have been convicted and seventeen cases with seventy-seven defendants are pending.

SCHARF: When those seventeen cases are over, is it correct that Kenya is washing its hands of these prosecutions and walking away?

MUTOKA: I would imagine that that is a correct summation. The prosecutions were based on understandings that were entered into between Kenya and the countries that would be affected by piratical attacks in the Horn of Africa. To my knowledge, we have not renewed any of the understandings that we had. The last case we had was last year. To date, they have not brought any new cases.

SCHARF: Was there sort of a quid pro quo? Was the United Nations giving money and assistance to Kenya in order to take on these pirate cases?

MUTOKA: I might not be able to correctly answer that, because I am not too sure about what went on behind the scenes. I only know what is on paper. I do know that there was a lot of assistance that was given towards improving the infrastructure. Technical assistance was also given to the judiciary, the president, and the police.

SCHARF: Is that money no longer flowing? Is that part of the calculus?

MUTOKA: I imagine that it is still there. We do have interest that has been expressed in areas of training, especially the training of judicial officers; this means that support is still being provided.

SCHARF: Let's go back to our prosecutor from Mauritius. Is Mauritius receiving international donor money to try to convince Mauritius to take on piracy cases?

BEEKARRY: I am not sure I would make that link straightaway. But the transfer agreement with the European Union came with an assistance package. This was fully related to the trials themselves, the training of

prosecutors, and just having a secure courtroom with metal detectors, dogs, and video link facility. That is how far the assistance has extended.

SCHARF: Milena Sterio, you and I went to the Seychelles to assist in some piracy work, and we were told that the UN built a state-of-the-art prison in their national park. Can you tell us about that?

STERIO: It wasn't actually a new prison, but rather a special prison wing, where the suspected pirates are being held. There was certainly assistance by one of the United Nations offices with respect to training the judges, the prosecutors, and the defense counsel. We've been focusing on the prosecution side, but the defense is also important for fair trials. I do know that the international community has been involved in helping.

SCHARF: I am sure that it is not just the money that convinces countries to prosecute. For instance, both in the Seychelles and Mauritius, tourism is being negatively affected by the perception that there are pirates in your waters. Reshma, your country worries about that as well, right?

BEEKARRY: We do. It has affected the whole region in a lot of ways. You would not want it to continue.

SCHARF: The US has also been prosecuting pirates, as Milena Sterio told us earlier about two recent cases of dry-land piracy. But there was also a case that was really unusual; it is not your typical piracy case. It involved the Sea Shepherds.[21] This is that vessel called the *Bob Barker* that you see in the TV series *Whaling Wars*. The vessel goes after the Japanese whaling fleets and tries to ram them to stop them from hunting endangered whales. What happened in that case, Milena?

STERIO: The Sea Shepherds case was just recently decided in the Ninth Circuit here in the United States. In that case, which was actually a civil law suit [private tort case], the judge in the Ninth Circuit found that a marine organization like the Sea Shepherds can be considered a piratical organization, as long as they are not operating on behalf of a government. As long as they are operating for their own private purposes, it does not really matter that they are not sea robbers; they were ramming the whaling fleets to protect the whales. If they are committing violent acts on the high seas, for the purposes of United States law, they can be considered pirates.

21. Institute of Cetacean Research v. Sea Shepherd Conservation Society 708 F.3d 1099 (2013)

SCHARF: Greenpeace better watch out, right?

STERIO: [laughs] Yes, definitely.[22]

SCHARF: We have been talking about prosecutions, and we have been talking about precedents. And we've been debating whether prosecutions deter piracy. Another deterrent is the use of private security guards, with whom companies that own private vessels are contracting to protect their ships. And most importantly, several countries have sent armed vessels to patrol the waters off the coast of Somalia. General Dallaire, how many vessels would you say are out there? It sounds to me like there is an armada of US and European vessels.

DALLAIRE: I do not have the figure, but I think you are quite right. It is a sizeable fleet, which includes Chinese and Russian vessels as well. It is a very polyglot fleet. There is problem with using extreme measure [using the military] in any conflict or any situation with insurrections. The military takes a very definitive position, and the position is not one that can be sustained in the long term. It is not the normal course for a nation to always have its military deployed in a security role.

SCHARF: It is quite expensive, isn't it?

DALLAIRE: It is expensive, and it is not necessarily the most effective tool. When we moved all those naval assets there, we obviously recognized that this had a sort of finite time to it. This was because of the nature of the fleets that could be maintained there, the cost, and the like. The question that never seemed to be coming to the floor and that people have been avoiding is, "What happens when they leave?" They're going to leave. So the fear is that you leave a vacuum. So there have been these security companies and other arrangements made. I think that is where the international community fails. As an example, why isn't there a UN naval capability? We have UN land capabilities. When I was in Cambodia in 1992, we had a naval capability in that mission to fight pirates off Kompong Som. Why doesn't the UN have that? Why doesn't it have its own capability versus having to seek or wait for donor countries to provide?

SCHARF: It sounds almost like this is a surge. We can take an analogy from Iraq and Afghanistan and maybe go even farther back in history when the US sent the marines against the Barbary pirates. In these cases, the hope

22. A few weeks after the broadcast, Russia arrested the crew of a Green Peace vessel that had been protesting drilling in arctic waters, claiming that they were pirates.

was that if we have enough military assets there, we will finally defeat the pirates. Then, we can manage the situation on a lower level. But you're saying that is not going to happen. When they pull out those assets, you think piracy is going to spike.

DALLAIRE: You have not broken the back of the whole system.

SCHARF: Is it possible to do that without solving the failed state that is Somalia?

DALLAIRE: This is where I come back to the question of sovereignty. If a sovereign nation, by its inept capabilities as a failing state, is putting a whole bunch of other nations at risk, there is surely a means by which the International Criminal Court and international community can handle something like that. That is why I have always felt that the ad hoc international tribunals, which led to International Criminal Court, was the first step in bringing global justice. A new dimension is needed and I think this is a great opportunity to try to bring international justice to another level of engagement in a case where a nation-state is, in fact, putting other nation states at risk by its inability to curtail what is coming out of it.

SCHARF: Meanwhile, Somalia is like a vacuum; it is a lawless place. In fact, Al Shabaab, which is a terrorist organization affiliated with Al Qaeda, is on the border of Kenya. I understand that your government, Judge Mutoka, invaded Somalia to destroy the Al Shabaab troops two years ago?

MUTOKA: That is true, yes.

SCHARF: Are Kenya's troops still there?

MUTOKA: They are still there. In fact, there has been a call from the Somali government that they should leave; but they are still there. The Kenyan government argues that it has to protect the border between Kenya and Somalia so that any cautions are not renewed there. You are aware that there have been a number of sporadic attacks, especially on churches; I've never understood that, though. The attacks have been attributed to Al Shabaab. We feel as a country that Kenya has helped in bringing down piracy by insuring that they do not get any routes in passage.

SCHARF: I think what I'm hearing is that until Somalia has an effective government, a rule of law, and international justice helping out; the pirates are going to continue to flourish, along with the drug traffickers and the organized criminals, because that's what happens in a failed state. It is not

just Somalia—there is also Yemen, and now pirates are breaking out in some weaker states on the West Coast of Africa. We've heard today that just prosecuting is not enough, and just providing security is not enough—there needs to be a more holistic approach. Well, it's time to wrap up the program. Hollywood has always glorified piracy. But in today's broadcast of *Talking Foreign Policy*, we've seen that piracy is a scourge that continues to vex the international community. That is the version of piracy that you're going to see in the new Hollywood movie with Tom Hanks, *Captain Phillips*, which should be refreshing. If you want to weigh in on the discussion or suggest a topic for the upcoming broadcast of *Talking Foreign Policy*, please send an email to talkingforeignpolicy@case.edu. Let me thank our outstanding panelists, who have come from far and wide. Again, we have Judge Mutoka, who has come from Kenya; General Dallaire, who has come from Canada; Prosecutor Beekarry, who has come all the way from Mauritius; and from just down the street we have Professor Sterio, from Cleveland State Law School. Thank you all. I'm Michael Scharf. You have been listening to *Talking Foreign Policy*, produced by Case Western Reserve University and WCPN 90.3 ideastream.

Talking Foreign Policy, January 31, 2014 broadcast[1]

Participants:
Michael Scharf
Shannon French
Mike Newton
Peter Singer
Milena Sterio

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. We'll begin our discussion with Peter Singer, director of the Center for 21st Century Security and Intelligence at the Brookings Institution. 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.

SINGER: Thank you.

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

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 the future of world politics. Where we stand is that we are definitely in an age of huge cyberdependence—everything from our communications, our commerce, our infrastructure, and, yes, conflict. Ninety-eight percent of military communication runs over the civilian-owned and -operated Internet, so we all depend on this. We live in a digital world, and yet we're also in an era of cyberinsecurity. You can see it in everything from the 97 percent of Fortune 500 companies that have been hacked, and the 3 percent who just don't know it yet, to the over one hundred cybermilitary command equivalents that have been created around the world. There was a poll taken—the first poll of 2014 by PEW—found that Americans are more afraid of a cyberattack than they are of Iranian or North Korean nuclear weapons, or the rise of China or authoritarian Russia, or climate change. So, we've got this combination of massive use of the online world and its rippling effect into the real world via the Internet

1. Transcript edited and footnotes added by Caroline Moore.

of Things.[2] 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.

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 cyberwarfare different from conventional war?

SINGER: You hit it exactly. Part of the problem with how we've approached it is we lump together so many different 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. 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 cyberattacks," but to get that number of millions, he was combining everything from address scans and probes, to attempts at pranks, to attempts at political protests, to attempts to get inside the network to do 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 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 here in cyberwarfare. 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.

2. *See* Jacob Morgan, "A Simple Explanation of 'The Internet of Things,'" *Forbes*, May 13, 2014, http://www.forbes.com/sites/jacobmorgan/2014/05/13/simple-explanation-internet-things-that-anyone-can-understand/.

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

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 Command and NSA are, than there are in the Pentagon itself. This is a huge growth area.

SCHARF: How much money are we spending on that?

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 ten times as much in the governmental side on Defense Department cyberoperations as we do in the Department of Homeland Security on the civilian side. 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 cyberoffense research and development as we are on cyberdefense research and development. I don't think—I argue that that's not that most strategic approach. It's a lot like, you talked about those teenagers; if you're using a metaphor, it's a lot like being worried about 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."

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

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

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 cyberattack? What's the worst-case scenario that you can imagine?

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, despite 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 cyberterrorism, let's be fundamentally clear that no person has been hurt or killed ever so far by cyberterrorism, by the FBI definition of it. 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. 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 cyberwarfare. With the Internet more broadly, it's the shift to the Internet of Things where we're not just using Internet-enabled devices to communicate with one another. It is not just that I email you, but it's devices that range from our cars to our thermostats to our power grid to our refrigerators all being looped in. 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. But, then the second is the development of new cyberweapons, and Stuxnet[3] is the game changer here; where it's [a] 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 it's made of zeroes and ones.

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

3. *See* Michael Kelly, "The Stuxnet Attack on Iran's Nuclear Plant Was 'Far More Dangerous' Then Previously Thought," *The Business Insider*, November 20, 2013, http://www.businessinsider.com/stuxnet-was-far-more-dangerous-than-previous-thought-2013-11.

SINGER: It went after Iranian nuclear research. In particular, they were operating under a SCADA system[4] 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 of [them] showing that this new kind of weapon was causing physical damage through digital means. It's interesting in that it's a weapon that was here, there, and everywhere. It was in twenty-five-thousand-plus different computers around the world. On the other hand, it might have been 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.

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—

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.[5]

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?

SINGER: So, Cyber Command—one of the other things it's playing out right now is this question: what exactly are its responsibilities? Originally,

4. *See* Anshul Thakur, "SCADA Systems," *Engineer's Garage*, 2012, http://www.engineersgarage.com/articles/scada-systems.
5. *See* Dylan Love, "Hackers Can Infect Your Computer Even If It's Not Connected To The Internet," *Business Insider*, March 5, 2014, http://www.businessinsider.com/what-is-air-gap-malware-2014-3.

when it was created, Defense Department officials talked about how it would just be responsible for defending Defense Department networks. 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 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. 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 and causes a sort of sense of complacency. It takes away what responsibility should have. So, think about it this way: you'll sometimes hear people cite 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, and blocked 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.

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.*[6] 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 cyberwarfare. Stay with us.

SCHARF: Welcome back to *Talking Foreign Policy*, brought to you by Case Western Reserve University and WCPN 90.3 ideastream. I'm Michael Scharf, interim 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

6. P.W. Singer and Allan Friedman, *Cybersecurity and Cyberwar: What Everyone Needs to Know* (Oxford University Press, 2014).

Cleveland Marshall College of Law, and Dr. Shannon French from Case Western's Inamori Center. 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 cyberweapons as a kind of arms race?

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 to our 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 on to the context of cyberwar.

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*-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?

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 policy makers 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 cyberrealm can be translated better than a lot of the nuclear science, in terms of again speaking directly to policy makers. 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 strategy, which was mutually assured destruction. In the same way that major powers decided, "Well, we really can't nuke one another because everybody loses," you see the same kind of implicit restraint going on with

the use of major cyberattacks with the major powers. Because it doesn't make sense; 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.

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?

SINGER: There are a couple of 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 and you'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 WWI, 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 *Dr. 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 eleven. You can see that there, and that's of concern to me. 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. The difference is almost a quality-quantity aspect to it. There's a description of the Chinese approach towards Internet censorship that's called the "human flesh search engine."[7] That's in many ways the parallel here of China, where to stay on

7. *See* Celia Hatton, "China's internet vigilantes and the 'human flesh search engine,'" *BBC News*, January 28, 2014, http://www.bbc.com/news/magazine-25913472.

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,[8] 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 being hit. It's just a massive scale, and that may be the differentiator here.

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 cyberattack 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?

STERIO: Under any kind of a convention analysis of warfare, normally our president does need congressional authorization to deploy troops. On the other hand, our president has the inherent constitutional authority as our commander in chief to use force. 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. To bring it back to this issue of cyberattacks 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 to 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 also assumes that we're conceiving of a cyberattack by the United States as a conventional military attack. And I think that goes back to—

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

---

8. *See* Ellen Nakashima, *The Washington Post*, "Report on 'Operation Shady RAT' identifies widespread cyber-spying," August 2, 2011, http://www.washingtonpost.com/national/national-security/report-identifies-widespread-cyber-spying/2011/07/29/gIQAoTUmqI_story.html.

STERIO: Well, if it's zeros 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, which 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—

SCHARF: We're talking about the US 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. What if another country comes in and penetrates you, not physically, but with zeros and ones over the Internet and does damage to them that costs a lot of money and hits at their very national security? Is that a violation of international law?

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. Here we have to analyze the nature of the cyberattack. Is it just zeros and ones? Are we just talking about 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 cyberattack.

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 cyberattack. As an ethicist, what are your thoughts about the psychological and ethical implications on that person, on US personnel who are engaged in cyberwarfare acts?

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 ,the harder it is for them to see and judge that impact, the less likely they are to make the ethical choice and the more callous they are going to be, 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' surprise, and my

own in one stage, that the drone operators were seeing their victims very close up and were actually experiencing high levels of PTSD and having to work through, almost like a sniper, what their relationship was to the people that they were targeting.

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

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

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

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 here in terms of cyberweapons. 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—

SCHARF: If our option was to either do cruise missile strikes on the nuclear weapon facilities in Iran, and there was a lot of collateral damage to civilians, and instead just send the zeros and ones over the Internet and we accomplish the same thing, well, yeah, that makes sense.

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

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?

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

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

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, so at some core, there's a fundamental recognition of basic human dignity and human rights. The problem is in cyberwar that when you begin to talk about taking zeros 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.

SCHARF: But, let me make this more concrete, Michael. What if the cyberattack 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?

NEWTON: Well, you get two huge problems: one is the problem of causation. Was it caused by private actors or 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. In the cyber context, it's enormously complex in real time to run that back and figure out exactly in terms of causation because of how broadly that expands.

SCHARF: So, what happens like in the Stuxnet, where a couple months later somebody leaked it out? I don't know if it was 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 cyberspace, it blows up the nuclear reactor in Iran, and then it leaks out that it was the US and not some nonstate actor that was behind this. Then what?

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

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

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?

SCHARF: All right so. . . . Let me switch it around here—

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

SCHARF: So, Mike, let's switch it around. Let's say it was Iran who does the cyberattack against the United States, and there's maybe a nuclear reactor that blows up. Right? Because you're focusing on the assumption that 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?

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 cyberattacks, or denial of services, or clogging of computer networks. It takes an incredibly—and in fact I would say it would be the worst cyberattack in history if it did actually unintentionally result in some physical damage.

SCHARF: Peter, do you think that there would ever be a cyberattack 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?

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 cyberattack that resulted in physical damage. 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 legal concerns. But, to your broader question of when does a cyberattack 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 where someone fires a weapon, let's say a rifle, 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. 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." And, so it comes down to a human judgment when it's a war,

or when it's a state of armed conflict, or when it's something else. But, it's a human decision. The concern, though, back to one of your prior points 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 cyberweapon, it's very seductive to politicians because it seemingly offers an effect without risk. As we've seen with, whether it's drones or cyberweapons 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, which is not something that would happen with a regular bomb. It's just a complex space. But, again, to me, 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.

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

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.

SCHARF: This is Michael Scharf, and we're back with *Talking Foreign Policy*. I'm joined today by Peter Singer in DC, Mike Newton in Nashville, Shannon French and Milena Sterio are with me here at WCPN ideastream in snowy Cleveland. We're talking about cyberwar. Now, just before the break Mike Newton, our colonel from the JAG, wanted to jump in and add something. Mike, here's your chance.

NEWTON: 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 cyberattack or in a cybercontext, 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 countermeasures, and the classic law of embargo short of armed conflict. 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

cybertechnology 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.

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 cyberwar. Let me begin with Shannon. You have written books about this. What was it, the last book? *The Code of the Warrior.*[9] Is it possible to apply century's old criteria of just war tradition to something so new and different like cyberwarfare, a form of war made possible by advanced technology?

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, discrimination, right authority, all of that is 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—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 policy maker, 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.

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

SINGER: Yes, I'd like to mention a couple things. The first, I'm in complete agreement that you shouldn't try to see these discussions as, "Oh, we need

9. Shannon E. French, *The Code of the Warrior: Exploring Warrior Values Past and Present* (Rowman & Littlefield, 2004).

to write a new Geneva Convention for the cyberworld." 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 versus a civilian. It makes perfect sense when you're thinking about conventional weapons, but the Internet itself is civilian, so if 98 percent of US military communications go over the civilian-owned and -operated Internet, 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 cyberweapons, 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 I've learned is that the law is not conclusive. 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.

SCHARF: Shannon, did you want to add something?

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?

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 who 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?

STERIO: Sure, so The Hague Law, 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 cyberweapons. The drafters never contemplated anything like what we're seeing today. There is a treaty called the International Convention on Cybercrime which was adopted in 2001 by the Council of Europe, but that convention really falls short of detailing everything that you would want in a comprehensive multilateral treaty.

SCHARF: Let's focus this on low-level cyberattacks, not this giant thing.

STERIO: We're talking about low-level cyberattacks and encouraging member states to prosecute those at the national level. So, if you want to talk about a big multilateral treaty on cyberwar/cyberattacks, first you would want to carefully define what is a cyberattack and what is cyberwar. Then you might want to think about prohibiting certain types of cyberattacks, similar to how certain types of attacks are prohibited under traditional conventions. So, you might want to prohibit cyberattacks 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.

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.

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.

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

SINGER: What we push for in the book is the idea of grafting. Grafting is something that 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 cyberworld is that NATO asked a group of top, really smart minds to come up with a manual for the legal side of cyberwarfare called the Tallinn

Manual.[10] It's in many ways a great document, a lot of 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, instead of trying to plant a new tree, is 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 politic, 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 altogether. 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 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.

SCHARF: Milena, you wanted to add something.

STERIO: Just a very quick note. 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 may fit under that idea that Peter's talking about is to use soft law instruments to supplement what we already have. It is much easier to negotiate codes of conduct guidelines and things of that sort that can then supplement, for example, the cyberconvention that we already have. And the goal would be that over time, if states then are using that kind of soft law—the guidelines, the codes of conduct—that maybe at some point we'll be closer to a customary norm of law.

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?

10. *See* "The Tallinn Manual," NATO Cooperative Cyber Defense Centre of Excellence, 2014, http://ccdcoe.org/tallinn-manual-process.html.

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 soft law, 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 [International Committee of the Red Cross] whole study about when a civilian crosses the threshold into legally participating in conflict to the extent that they can be targeted, the direct participation study, is exactly the same thing as discussions for close to a decade that in the end, there is no real agreement. So, I think 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.

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 cyberattacks, 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?

FRENCH: Well, yes. 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 cyberattack 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 resources to try to address, that's actually quite horrifying. 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 cyberattack, 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.

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?

SINGER: Well, we'll probably be downloading it into our brains. In all seriousness, the one word 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, or 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 triage it. 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 the demands and be more resilient about them.

SCHARF: That's a great final note. On September 15, Case Western Reserve University School of Law is going to be having 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*, Colonel Mike Newton from Vanderbilt University, Professor Milena Sterio from Cleveland Marshall College of Law, and Dr. 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.