115th CONGRESS
1st Session

Printed for the use of the
Commission on Security and Cooperation in Europe

Building Cyber Confidence Between Adversaries: Can the OSCE Help Establish Rules of the Road?

SEPTEMBER 28, 2017

**Briefing of the
Commission on Security and Cooperation in Europe**

Washington: 2017

Commission on Security and Cooperation in Europe
234 Ford House Office Building
Washington, DC 20515
202–225–1901
csce@mail.house.gov
http://www.csce.gov
@HelsinkiComm

Legislative Branch Commissioners

HOUSE
CHRISTOPHER H. SMITH, NEW JERSEY
Co-Chairman
ALCEE L. HASTINGS, FLORIDA
ROBERT B. ADERHOLT, ALABAMA
MICHAEL C. BURGESS, TEXAS
STEVE COHEN, TENNESSEE
RICHARD HUDSON, NORTH CAROLINA
RANDY HULTGREN, ILLINOIS
SHEILA JACKSON LEE, TEXAS
GWEN MOORE, WISCONSIN

SENATE
ROGER WICKER, MISSISSIPPI,
Chairman
BENJAMIN L. CARDIN. MARYLAND
JOHN BOOZMAN, ARKANSAS
CORY GARDNER, COLORADO
MARCO RUBIO, FLORIDA
JEANNE SHAHEEN, NEW HAMPSHIRE
THOM TILLIS, NORTH CAROLINA
TOM UDALL, NEW MEXICO
SHELDON WHITEHOUSE, RHODE ISLAND

Executive Branch Commissioners

DEPARTMENT OF STATE
DEPARTMENT OF DEFENSE
DEPARTMENT OF COMMERCE

ABOUT THE ORGANIZATION FOR SECURITY AND COOPERATION IN EUROPE

The Helsinki process, formally titled the Conference on Security and Cooperation in Europe, traces its origin to the signing of the Helsinki Final Act in Finland on August 1, 1975, by the leaders of 33 European countries, the United States and Canada. As of January 1, 1995, the Helsinki process was renamed the Organization for Security and Cooperation in Europe [OSCE]. The membership of the OSCE has expanded to 56 participating States, reflecting the breakup of the Soviet Union, Czechoslovakia, and Yugoslavia.

The OSCE Secretariat is in Vienna, Austria, where weekly meetings of the participating States' permanent representatives are held. In addition, specialized seminars and meetings are convened in various locations. Periodic consultations are held among Senior Officials, Ministers and Heads of State or Government.

Although the OSCE continues to engage in standard setting in the fields of military security, economic and environmental cooperation, and human rights and humanitarian concerns, the Organization is primarily focused on initiatives designed to prevent, manage and resolve conflict within and among the participating States. The Organization deploys numerous missions and field activities located in Southeastern and Eastern Europe, the Caucasus, and Central Asia. The website of the OSCE is: <www.osce.org>.

ABOUT THE COMMISSION ON SECURITY AND COOPERATION IN EUROPE

The Commission on Security and Cooperation in Europe, also known as the Helsinki Commission, is a U.S. Government agency created in 1976 to monitor and encourage compliance by the participating States with their OSCE commitments, with a particular emphasis on human rights.

The Commission consists of nine members from the United States Senate, nine members from the House of Representatives, and one member each from the Departments of State, Defense and Commerce. The positions of Chair and Co-Chair rotate between the Senate and House every two years, when a new Congress convenes. A professional staff assists the Commissioners in their work.

In fulfilling its mandate, the Commission gathers and disseminates relevant information to the U.S. Congress and the public by convening hearings, issuing reports that reflect the views of Members of the Commission and/or its staff, and providing details about the activities of the Helsinki process and developments in OSCE participating States.

The Commission also contributes to the formulation and execution of U.S. policy regarding the OSCE, including through Member and staff participation on U.S. Delegations to OSCE meetings. Members of the Commission have regular contact with parliamentarians, government officials, representatives of non-governmental organizations, and private individuals from participating States. The website of the Commission is: <www.csce.gov>.

Building Cyber Confidence Between Adversaries: Can the OSCE Help Establish Rules of the Road?

SEPTEMBER 28, 2017

Page

PARTICIPANTS

Building Cyber Confidence Between Adversaries: Can the OSCE Help Establish Rules of the Road?

September 28, 2017

Commission on Security and Cooperation in Europe
Washington, DC

The briefing was held at 2:04 p.m. in Room 385, Russell Senate Office Building, Washington, DC, Alex Tiersky, Policy Advisor, Commission on Security and Cooperation in Europe, moderating.

Panelists present: Alex Tiersky, Policy Advisor, Commission on Security and Cooperation in Europe; Stacy L. Hope, Director of Communications, Commission on Security and Cooperation in Europe; Tim Maurer, Co-Director and Fellow, Cyber Policy Initiative, Carnegie Endowment for International Peace; Jaisha Wray, Acting Deputy Director, Emerging Security Challenges Office, Bureau of Arms Control, Verification and Compliance, U.S. Department of State; and Dr. Alex Crowther, Senior Research Fellow, Center for Strategic Research, National Defense University.

Mr. TIERSKY. Ladies and gentlemen, we will get started with our briefing. As you may have noticed from our "Matrix"-like poster outside, we're here for a discussion on cyber diplomacy. More specifically, this is a U.S. Helsinki Commission briefing on "Building Cyber Confidence Between Adversaries: Can the OSCE Help Establish Rules of the Road?" And on behalf of the Commission Chairman Senator Roger Wicker and the Co-Chairman Congressman Chris Smith, I would like to officially welcome you to this discussion.

For those of you who may not know the Helsinki Commission very well, the Commission is mandated by law to track the commitments made by the signatories of the 1975 Helsinki Final Act. A great deal of that 1975 Helsinki Final Act had to do with transparency and confidence building in order to reduce tensions and provide increased predictability and security in a very tense European zone during that time, in the thick of the Cold War. The Commission has been tracking these commitments throughout its history, with a strong focus on human rights, of course, as well as the security challenges that in recent years have grown in their intensity in Europe. And the Commission has equally increased its attention to some of these challenges.

Now, obviously, we are here today to talk about state-based cyber threats to security and what might be done about those. But it's clear, I think, to all of us that they're an increasingly dominant part of the global security landscape. The Commission is tracking a process at the Organization for Security and Cooperation in Europe, the OSCE, which is an organization that essentially flowed from the 1975 Helsinki Final Act process. And at the OSCE in recent years, diplomats and experts have been seeking to play a leading role in the international system in the development of confidence-building measures between states to reduce the risk of cyber conflict. These discussions feature voluntary agreements among the participating states that include, quite crucially, the United States and Russia.

The measures that have been agreed to are designed to—and here I'm going to read an OSCE document if you'll allow me for just a moment—they're designed to enable states to read another state's posturing in cyberspace and draw red lines. They're designed to allow for timely communication and cooperation, including to defuse potential tensions emerging from the use of information and communication technologies, another word—a buzzword for cyberspace—and they're designed to promote trusted cyber neighborhoods through enhanced national preparedness.

Those who are tracking the OSCE would suggest that this process has been one of the few bright lights in what has otherwise been a very difficult period for the organization. So we are here today to rely upon this all-star panel to help us understand what are confidence-building measures, what are our norms, how do they relate to each other in the field of cyberspace, what's happening at the U.N., what's happening at the OSCE on these issues, and ultimately, what difference could this make in the real world?

As I mentioned, this is an all-star cast. They're obviously technical experts, and I will push for them to be as non-technical as possible—and forgive me in advance if I need to interrupt you to explain some terminology, some particularly wonky term. They're extraordinarily distinguished individuals.

We will first hear from Tim Maurer. Tim is from the Carnegie Endowment for International Peace. He's the co-director of the Cyber Policy Initiative there. He's going to talk us through state-based threat, and he's going to explain to us confidence-building measures and how they might be useful against this threat. And I think he'll give us a bit of a short historical overview of how this relates to the U.N. and the genesis, and what goes in which direction.

We will secondly hear from Jaisha Wray, who is the acting deputy director of the Emerging Security Challenges Office in the Bureau of Arms Control Verification and Compliance at the U.S. Department of State. I'd like to thank the administration for providing a witness today, and someone clearly that's as expert and well placed to talk to us about this as Jaisha. She will provide us with some official views on where the value is in this process, and the latest on what's going on in these fora today.

Finally, we'll hear from Dr. Alex Crowther, who is a senior research fellow at the Center for Strategic Research in the National Defense University. He'll be batting cleanup for us. He gets to talk about more or less whatever he would like to in reaction to the previous panelists, but also he has a particular perspective on some of the harder security challenges that are implied by these discussions.

So before I hand it over to Tim to start our substantive discussion, I need to make sure to let you know that we are live on Facebook right now, and that stream is at

Facebook.com/HelsinkiCommission. If you're tweeting this discussion, you're welcome to do so, but use the hashtag @HelsinkiComm. We are able to take questions on social media, if anyone who's watching on Facebook would like to send in some questions. Please do that, and someone will signal those to me as appropriate. And then just to let everyone know, there will be a transcript available of this event within a few days on our website.

So, Tim, please kick us off. Give us the overview.

Mr. MAURER. Great. Thanks, Alex, and thanks to all of you joining us. We'll be talking about cyber diplomacy which, as you, I'm sure, are familiar with, has gained attention and risen on the agenda, particularly in the past few weeks, but also certainly in the past few years. I'm going to start off by briefly talking about the state-based threat, and then we'll talk about this concept of confidence-building measures, which dates back to the Cold War, and why there's also this effort now underway to use it in the context of cybersecurity, which is not evident, right?

I'll walk you through the utility of the confidence-building measures, or CBMs for short, and then I'll tie to the broader discussion at the U.N. in terms of trying to develop the rules of the road. And there's also connection to the G–20, which in 2015 the heads of state for the first time included a specific reference to this U.N. process in their outcome document at the time.

So to start, what's the threat landscape when it comes to state-based threats? When we talk about cybersecurity, it's helpful to put into context that cyber operations can have a variety of effects. Cyber operations range from espionage to profit-driven malicious activity to political and military activity. As you all know, hacking and cyber operations, as we use it today, are essentially initially coming out of the intelligence world, and were initially designed to steal data. As more and more devices connected to the internet, and the internet proliferated as a network and became the backbone for the economy but also for military systems and other systems that are politically relevant, all of a sudden, the operators in the national security agencies realized that there were other effects that they were able to cause.

One of the main inflection points for this now 30 years of history of cyber conflict, so to say, or conflict that included a cyber component, is probably the 2007 DDoS attack that occurred in Estonia and was the first incident that kind of made front page news and brought this issue back to the attention of a lot of people. You had a community back in the 1990s that focused on cybersecurity, but after 9/11 and the terrorist attacks a lot of those people shifted their attention to counterterrorism. And I would argue it wasn't until 2007 that it really started to come back into people's minds and in terms of headlines.

2008 was also the year where during the war between Georgia and Russia you saw for the first time how offensive cyber capabilities were used during a conventional conflict on the ground, and how the two could be married. In fact, Chris Demchak coined the term "cybered conflict" as a result of that, suggesting the notion that we should rather think about cybered than cyber conflict, because her argument is that what we are likely to see is conventional war and conflict be married with hacking capabilities.

As you all know, in the last five years there's only been deterioration in the security environment. We've had the Sony hack, where for the first time you had the United States President—in this case President Obama—who went in front of public television cameras and accused North Korea for having hacked Sony Entertainment Pictures and subse-

quently resulting in several movie theaters in the United States pulling a movie that was critical of the North Korean leader. That was a significant escalation, I think, when we look back in terms of the history of how states have been using it, because it takes a lot for the president of the most powerful country in the world to go on public television and accuse another country of this type of activity.

You also have more destructive attacks, actual destruction that took place. For example, the Saudi Aramco attack, where you had the malware that was wiping the hard drives of the Saudi Arabian oil company that significantly impacted their operation to the extent that the single company that had been hit with this malware had to purchase and replace its hard drives, and had such an impact that the price of the hard drives from anybody else was increasing because of the sudden surge in demand for the hard drives that had to be replaced. So apart from the actual impact, you had secondary effects that took place.

To mention a couple of others—we are all familiar with Stuxnet, the malware that was found to have infiltrated the Iranian nuclear enrichment facility. That was clearly a critical point in time in terms of the state use of these tools, because it showed that hacking is now also being used to target some of the most sensitive and most critical systems for international security and national security. Last year the U.S. Government unsealed a range of indictments, including one in which the Department of Justice had indicted seven Iranian hackers for having targeted U.S. financial institutions in 2012 and 2013. And you had a group of essentially seven people in their mid-20s to late 30s who stand accused of having used DDoS attacks and targeting a range of U.S. financial institutions, causing significant economic damage.

So, long story short, the last decade has seen a significant increase in state-based threats, using offensive cyber capabilities. James Clapper testified last year on the record that there are now 30-plus countries that are developing offensive cyber capabilities. And many of these countries consider cyberspace a new operational domain to further their political and military aims. At the same time, there's little transparency about how these countries think about using these capabilities and what their doctrines are, and what their underlying strategies are. In fact, many countries don't even agree on the same terminology. For example, in the Russian Federation and China they use the term information security and have a much broader approach for how they think about this, compared to the U.S.

That is where I'm now transitioning to the confidence-building measures, which back in the Cold War were essentially the tool to avoid accidental escalation. I'm putting the emphasis on the adjective "accidental" because sometimes, obviously, there is deliberate escalation as part of a political conflict. But during the Cold War, the Soviet Union and the U.S. realized that there was also a significant risk of accidental escalation that neither side intended, either because the other side was misinterpreting a signal that was being sent or just as a result of an accident. And that became the foundation for a range of measures put in place to reduce the risk of this kind of escalation, and to create this regime of confidence-building measures for the two sides.

I think the best example is the red telephone between the Kremlin and the White House, that I think is featured in several movies. I don't think it's actually red, but it became a Hollywood meme.

Dr. CROWTHER. But it's still functional.

Mr. MAURER. It still works. [Laughter.] So the reason why I think for the past few years there's been a focus on CBMs in the cyber context as well is because it's a new domain, there's a lot of uncertainty. There's a lot of intransparency. And these confidence-building measures that you've seen come out of the OSCE in 2013 and 2016 put a particular focus on trying to reduce some of that uncertainty. And there's value just in the fact that sharing of doctrines, where, if you like, sharing of doctrines, what is the real impact of that? Like, can you just send that in the email? It actually does have a real impact because this is such a new domain and the uncertainty of how states think about this.

I'd also like to point out, just as I come to the end, that the initial confidence-building measures were not driven necessarily by the diplomats. They actually came out of the military community, as Thomas Schelling reminds us. They were a necessity that military commanders realized, to really try to reduce the escalatory dynamics and the potential for accidents to occur. So this is something where there's a lot of history and tradition also coming from the military community.

Now, to tie it to the broader discussion at the U.N., the OSCE's work—and I'm sure we'll hear more about this in greater detail in terms of what has come out of the OSCE in 2013 and 2016—this is part of a broader effort of the international community to create a regime for how states use offensive cyber operations. The OSCE has always been focused on much more practical mechanisms and terms to create more confidence and to create more transparency. But there's a higher-level effort that's been taking place at the U.N., where the international community is trying to come to a consensus and understanding for what is appropriate behavior, what states are permitted to do when it comes to the use of offensive cyber operations, and where do we draw the lines. What are things we can all agree on, that should not take place?

This is an effort that dates back to the late 1990s, when the Russian Federation proposed a bilateral treaty between the U.S. and Russia which, for a number of reasons, the U.S. has objected to, which continued to be very valid today. And the U.S., in response, developed this framework for voluntary norms, particularly in peace time, to create more of a regime and to create boundaries for what appropriate behavior could look like. Final sentence on that, this process at the U.N. has produced two significant reports that are the most advanced in terms of providing insight into how the international community is currently thinking about what constitutes appropriate behavior. I encourage you all to take a look at that.

The bad news is, in spite of the progress that's been made in the last several years, the security environment has continued to deteriorate. And this process at the U.N. collapsed in June when the latest group of governmental experts—the fifth iteration of it—failed to come to a consensus document. And there is now a big debate about where to go next. And I'm happy to discuss this more in detail after the event or on the margins of it. But I hope that provides some good overview of the CBMs, the OSCE, and——

Mr. TIERSKY. Thanks, Tim. That was excellent. That was exactly what I was hoping for. As I said, I'm going to put you on the spot, though. I'm fairly certainly that 90 percent of our audience knows what a DDoS attack is, but if you could give us 10, 15 seconds on a DDoS attack, which you mentioned several times.

Mr. MAURER. Thank you. Yes, of course. So DDoS stands for Distributed Denial of Service attack. And it's essentially—remember the phone prank as a teenager, you try to call somebody repeatedly at the house so they wouldn't be able to use the phone? Think

of that as the equivalent for what a DDoS attack is in cyberspace. It's essentially somebody who uses a number of machines that the malicious actor controls. And it floods the system that's the target with so many pings that the system can't process normally anymore. So if you target a website, the website will be inaccessible because it receives so many requests that it can no longer be processed, and therefore the website is down. That might seem not like a big deal if you're thinking about—I don't know, pick your favorite website for, maybe, cooking. But it becomes a much bigger deal if you're thinking, for example, a government website at a time of crisis, or for a banking website. If the banking website is down and you can't actually make transfer, that's actual money loss for the bank.

So the last escalation we've seen of DDoS attack was the Dyn attack, where a significant amount of the internet on the East Coast went offline for a long period of time, because as more and more devices like your fridge and your webcams become connected to the internet, the number of devices that can be used for these flooding attacks significantly increases and poses a bigger threat.

Mr. TIERSKY. Thank you for that. And of course, you mentioned that in the context of Estonia, which I think was a such a remarkable example, particularly given the leadership Estonia has taken in terms of its citizens' ability to interact with government online. And I think that was a big part of why it was so impactful on Estonia.

You laid out for us the threat very compellingly. You described a history of confidence-building measures and their importance in particular as they regard the risks of accidental conflict or accidental escalation of conflict. And then I think you left us with a sense that the process of the development of norms at the United Nations was largely driven by the United States in response to an initial Russian proposal, but that it now may be languishing. And it faces a bit of an uncertain future. Have I captured more or less? Great.

Let us move over to Jaisha for her comments. Thank you.

Ms. WRAY. Thank you, Alex, and good afternoon, everyone. I'd like to start off by thanking the Helsinki Commission for inviting me to speak on this very important, but perhaps not so well known topic today.

The United States has worked for the past decade to promote stability in cyberspace through the development and promotion of a framework of responsible state behavior. And our approach has been focused on building international consensus on what constitutes responsible state behavior in cyberspace. And this includes consensus on the applicability of international law as well as consensus on the development of norms of responsible state behavior. In addition to norm-setting, we have also focused on the development and implementation of practical confidence-building measures for cyber to reduce the risk that cyber incidents will result in misperceptions, escalation and potential conflict.

And while CBMs are being developed multilaterally, as Tim mentioned, through the U.N. group of governmental experts, they're also being developed through regional security organizations, such as the Organization for Security and Cooperation for Europe, the OSCE. I have participated in many meetings of the OSCE informal working group on cyber, which began just six years ago. And I look forward to sharing U.S. perspectives on the work of this very important body. I'll also discuss the importance of cyber CBMs, the role of regional security organizations and their development, and the current state of play in the OSCE cyber informal working group.

As I mentioned in my introduction, cyber confidence-building measures can play an important role in building stability in cyberspace. CBMs are particularly helpful in the cyber domain, since cyberspace and military cyber capabilities have a number of unique characteristics that make them potentially destabilizing. First of all, there's a lack of external observables, which means that states have no real tactical warning of when an incident is about to occur. Next, even when a state knows that there is a foreign actor's presence on their systems, they might not have a clear understanding of that state's intentions. And finally, information and communication technologies, or ICTs, are ubiquitous, meaning that we are all vulnerable to some extent.

These characteristics heighten the possibility that a cyber incident will result in misperception, escalation, or even outright conflict. In short, confidence-building measures are meant to reduce the risk of misunderstandings or conflict between states stemming from cyber incidents. We see three types of CBMs particularly useful in the cyber arena. The first type is transparency measures, which are aimed at reducing uncertainty about states' intentions in cyberspace.

Now, I think you all received a packet when you came in today, and the OSCE's cyber CBMs that have been developed are inside your packet. And one of them, which is CBM 7, is that participating states will voluntarily share information on their national organization strategies, policies and programs relevant to the security of and use of ICTs.

The second type of CBMs are cooperative measures, which are meant to provide states with channels to work together cooperatively to respond to or manage tensions related to cyber incidents. And there are plenty of examples of cooperative measures in the OSCE cyber CBMs as well. One is CBM 3, which says that participating states will, on a voluntary basis, hold consultations in order to reduce the risk of misperception and of the possible emergence of political or military tensions that may stem from the use of ICTs.

Finally, there are stability measures, which in the cyber environment are measures of self-restraint. And there are many stability measures in the Group of Government Experts [GGE] reports that Tim mentioned. But as of now, the OSCE CBMs do not include stability measures.

Now, I'll discuss regional security organizations and the role that they play in the development of cyber CBMs. These organizations can play a critical role in conflict prevention through providing a venue for capacity building as well as the sharing of best practices. As a result, we are pleased to see that many of these regional security organizations have begun discussing cyber. And the United States participates in the cyber-related discussions of the OSCE, as well as the ASEAN Regional Forum and the Organization of American States.

We view regional security organizations as key places to discuss cyber issues because even in the age of the global internet we believe that many of the tensions that could implicate state use of cyber capabilities are likely to be regional in nature. Further, many of the vulnerabilities—like cross-border interdependencies within critical infrastructure—are likely to be regional or sub-regional in nature as well. The role of regional security organizations—like the OSCE—is to help states manage shared security concerns.

And it makes sense to build on their experience in doing this in other domains to address the specific risks of cyberspace. A benefit of discussing cyber and regional organizations is that these organizations are able to address the particularities of that

region's security concerns and issues. In addition, these organizations are able to shape their efforts based on local conditions as well as the comparative advantages and institutional competencies of the organization. And finally, different regions may balance their priorities differently—whether it's developing CBMs or endorsing principles or building capacity.

We also believe that regional confidence-building measures can play an important role in universalizing the consensus reached in the multilateral organization, such as the U.N. Group of Governmental Experts. And it's not by coincidence if you put the OSCE CBMs side-by-side to the Group of Governmental Experts report that you'll notice many of the CBMs are similar or complementary in nature. Since the inception of the informal working group on cyber in the OSCE, which I mentioned, just six years ago, so it's fairly new, the OSCE had made groundbreaking progress to advance cyber confidence-building measures and stability. In some ways this isn't surprising, since building confidence lies at the very heart of what the OSCE does.

The OSCE-participating states have adopted two different sets of confidence-building measures. The first set was adopted in 2013, and that focuses on official points of contact and building communication lines to prevent possible tensions resulting from cyber incidents. The second set was adopted just last year in 2016, and that focuses on further enhancing the cooperative mechanisms between participating states; for example, to effectively mitigate cyberattacks on critical infrastructure that could affect one or more participating states.

The challenge, of course, once a CBM has been agreed to, is meaningful implementation. And I emphasize the word "meaningful" here. As an example, one of the CBMs states that participating states will nominate a point of contact to facilitate pertinent communication and dialogue on security of and in the use of ICTs. Now, it's one thing to have each state provide a policy point of contact, but it's another to have all of those points of contact know exactly what to do when they receive a call about a cyber incident.

So as a result, it's essential that all participating states have the correct contacts within their own governments, as well as the procedures in place to be able to respond to or make such a call. Successful implementation of the CBMs requires shared experiences regarding how individual CBMs will work in practice, as well as awareness raising within individual governments, and finally capacity building, which may be necessary in some cases. And this is exactly what the OSCE and others, including the United States, are working on right now. In fact, just last week I was in Uzbekistan for a conference on the implementation of the cyber confidence-building measures to raise awareness in that sub-region.

Other recent positive steps towards implementation have been two recent communication checks. During these checks, the OSCE secretariat sends an email to each of the participating states to test the responses from the officials listed on the point of contact list. And we recently did a scenario-based exercise as well to see how states would respond to a particular incident.

In conclusion, the United States has been pleased with the progress of the OSCE cyber informal working group in its swift development and its work on a range of cyber confidence-building measures. However, there's still work to be done on the implementation and we look forward continuing to play an active role as the work of this body moves forward.

Thank you.

Mr. TIERSKY. Thank you, Jaisha. That was an excellent overview of USG policy and perspective on the ongoing processes. I guess one element that I take from where you ended up was the implementation challenges that we face are really underlined by the fact that we are still trying to get the right person to answer the phone call when the OSCE secretariat does a test of this system. So as you pointed out, one of the confidence-building measures really is just a directory of who to talk to if you have a problem, if you think another participating state of the OSCE is creating conditions that are threatening in cyberspace. Just getting that telephone or email directory to work is a challenge. That, I think, to me at least, suggests kind of the nascent nature of these confidence-building measures and the need to continue to do more in that respect.

Ms. WRAY. That was the first step. But our second communications check took it one step further, to ask the policy points of contact to reach back within their own governments and to form a coordinated response back to the OSCE secretariat. So I would say we're at the next step on that one in terms of implementation.

Mr. TIERSKY. And, thus, building their own capacity to coordinate.

Ms. WRAY. Exactly.

Mr. TIERSKY. That's great. Thank you for that clarification. Let me ask you one more technical term, since I put Tim on the spot for his DDoS. Why do we talk about ICTs in the international format? Whereas in this context we'd be more comfortable saying "cyberspace" or something of this sort?

Ms. WRAY. That lies in the 57 participating states and the terminology that they feel most comfortable with. So while "cyber" is what the United States uses, we mentioned earlier that there's no real set of definitions. But we have been able to agree internationally through the U.N. and through the OSCE that information and communication technologies for the U.S. is relatively the same thing as cyber.

Mr. TIERSKY. Very good. Thank you. Dr. Crowther, if you would.

Dr. CROWTHER. Alex, thank you very much for this invitation to the Helsinki Commission. Thank you, everybody, for sharing your afternoon with us. I'd like to start with talking just for a second about China and Russia, because although we don't have to sympathize with their point of view, we do have to empathize or understand their point of view, because they're the ones who are provoking a lot of this. China feels that bad things happen when the little people get too much information. And so they talk about their responsible use of information because irresponsible use of information is when you give too much information to the little people. The Russians, on the other hand, feel that they've been directly attacked by us. They feel that our criticism of their 2012 election was a direct attack at Putin's validity as the leader of Russia. And so they feel that we're conducting hybrid operations against them in order to achieve regime change.

The OSCE is important in this because most organizations have stopped talking to Russia in the wake of the 2014 seizure of Crimea. Only the Norwegians, NATO, the U.S. and U.N. really are talking to the Russians anymore. But history has shown us that in these times of tension, it's very important to continue discussing things. The 1932 departure of Japan from the League of Nations is sometimes seen as one of the precursors for World War II, because it forced the Japanese out and then we no longer had a platform with which to talk to them. Over the years, we've continued to talk to the Cubans, we've continued to talk to the North Koreans, we've continued to talk to the Russians. So it's

really important that we continue to do this. The OSCE is a vital platform for continuing that discussion.

It's a wonderful platform also because all 29 NATO allies are in it, 21 Partnership for Peace nations, and then there's seven other smaller nations from Europe that are in it. So when you talk to the OSCE, you're reaching from Canada over into Uzbekistan. It's a tremendous swath of the globe that's covered by this. We heard two people talk about the Group of Government Experts—the GGE talks about norms, and the OSCE seeks to operationalize that through the use of confidence-building measures. They've—and I think it was Tim that mentioned it—they've had two tranches of confidence-building measures. You heard Jaisha mention several of them, and there are several more. I don't want to read them to you, but they're all available to you in your packets.

The most important consensus coming out of the GGE is that international law applies in cyberspace, because before that the Russians and the Chinese—essentially their point of view was cyberspace is a Wild West because it's so new and different that normal laws don't count. So in the 2015 GGE everybody agreed, we reached consensus that international law runs writ in cyberspace. That means cyber intelligence is an intelligence operation. Cybercrime is a criminal operation. So you don't need an entire new chunk of the United States code to cover this because crime is already covered in Title 18. You just have to modify Title 18 to take into account cybercrime. Everybody's admission that international law is applicable in cyberspace was a huge leap forward.

From the perspective of the Department of Defense, the OSCE rules are a very important venue to talk to the Russians, because, as I mentioned, few organizations are talking with the Russians. And even ones that are aren't doing that much. For instance, the NATO–Russia Council has met twice in the last year. And my buddies are telling me not much came out of that. But the OSCE is really a trifecta for the Department of Defense. Number one, they get to talk to the Russians and reiterate what they're saying in private to the Russians. Number two, they get to say it in front of all of the other 28 NATO allies, which reinforces what NATO says within NATO. And number three, it hits all those other Partnership for Peace countries and the smaller countries, which is our opportunity to ensure that they understand what our point of view is and where we should be at.

From NATO's perspective, NATO does agree that international law applies in cyberspace. They welcome voluntary norms and confidence-building measures. And they want to see a norms-based predictable and secure global cyberspace. And they see CBMs through the OSCE as a way to achieve that. You can see how important the OSCE is to NATO. NATO has three international organizations that they partner with—the United Nations, the European Union and the OSCE. So you can see that it's extremely important to them.

Tim mentioned cyber conflict. I've been doing a lot of work on what is the cyber domain recently. And interestingly enough, although there are pure cyber operations—like the Shamoon virus for the Saudi Aramco attack in 2012—what's become more popular are cyber-enabled operations. What you saw in Georgia was a conventional land and air operation enabled by cyber operations. You're going to see more and more—with the informationization of our society—you're going to see more and more of our intelligence operations, information operations, and conventional and special operations being cyber-enabled, until someday it's just going to be totally suffused and you're not even going to talk about cyber-enabled operations because everything is going to be cyber-enabled.

And Tim mentioned in passing the Internet of Things and the attack on the grid in the northeastern United States last year. This is super important. They went in through a camera—the kind of camera that hangs on your computer screen. The problem is, when you buy a smart device, when you ask for a smart refrigerator, you say: I would like a refrigerator that tells me when I'm out of milk. You don't say: I would like a refrigerator that seamlessly integrates into my home cybersecurity system. The people who are making these things are not building security in from the very beginning. And so as the number of smart devices in our homes proliferates, we have more and more attack surfaces and it makes us more and more vulnerable. So with that, the OSCE vitally important and a great platform for confidence-building measures.

Mr. TIERSKY. Thank you, Alex. That was a terrific endorsement of the value of the OSCE going forward, and certainly something that I think the Helsinki Commission would get behind, in terms of the value that we see in these discussions that take place in Vienna and then, of course, in other places.

I want to throw some red meat on the table for us to kind of bat around, but I'll very shortly turn to the audience for your questions, so please gather your thoughts in that respect. And I also want to give you a chance to react to anything that you've heard from each other before we go too far.

But I think we can't have this conversation in a kind of honest way without really addressing the elephant in the room, which is the Russian offensive cyber activities that have been widely reported and widely discussed. I was just recently scrolling headlines again, and I was reminded that—this is only in public reports—Russia was accused of hacking the OSCE itself in December of last year. We also know that the Russian leadership is accused of not observing various arms control treaties, such as the Conventional Forces in Europe Treaty, the INF treaty—the Open Skies Treaty is the one that's been in the headlines the last couple of days. Certainly, confidence-building measures in political military affairs, like the Vienna document and their major exercises in Russia and Belarus that they were just having last week.

So I put this on the table for my colleagues here to chew over, and I will phrase this in a provocative way—what confidence can we have that confidence-building measures that are developed in this process will be treated differently by the Russians? And if there is not confidence that these confidence-building measures will be treated differently by the Russians, is there still value in the process as a whole? And can you put your finger on what that value is? And over what time frame might that value manifest? Would anyone like to take a first crack at that?

Dr. CROWTHER. I can.

Mr. TIERSKY. Please.

Dr. CROWTHER. The problem is you can't prove a negative. If they were cleaving to these, we might not know it. Part of the problem goes back to—and I'll expand on what I said earlier—the Russians feel like we're conducting hybrid operations against them. I stopped there. The corollary to that is they're conducting counter-American hybrid operations, from their perspective. They believe that they are performing these offensive cyber operations to counter our hybrid operations. But we think they're doing hybrid operations. So we can't figure out how to counter their operations because we don't understand that they're doing counter hybrid operations. So we're actually doing counter-counter hybrid

operations, which is kind of hard to wrap your head around, which is one of the problems that we're having. We just don't understand what they're doing, so we can't stop it.

I would propose to you that the Russians have always played fast and loose with the rules. You can track a lot of their behavior, if you want to look at how they do information operations and stuff like that, actually goes back into the 1800s. They've been doing these types of information operations—*maskirovka*, deception is hardwired into the Russian culture. So they're going to continue to do this kind of stuff. Confidence-building measures actually are kind of our only hope. There's a yin and yang to it, right? We have to have confidence-building measures, but at the same time we have to practice deterrence. And deterrence consists of two parts—coercion and denial. We have to get a lot better at doing denial back home so that they will see their operations as being fruitless.

Mr. TIERSKY. Tim, please.

Mr. MAURER. Let me jump in—when in 2013 the OSCE agreed to the confidence-building measures, that only occurred several months after the United States and Russia came to a bilateral agreement, in the spring of 2013. And you had the White House together with the Kremlin agreeing on a bilateral set of confidence-building measures. The White House has put out a fact sheet, so some information is available on what that agreement entailed. I do think that the events of last year, in terms of what that means for the bilateral relationship and the efforts of the OSCE, raise a big question to what extent it undermines trust in Russian commitments over the long term. I do think, from our perspective, from the U.S. perspective, there is a big question mark to what extent there is good faith when you negotiate with Russian counterparts, given some of these events.

But on the flip side, a concern that I think we've had at Carnegie and that has been informing a lot of our work is, in order for these agreements and norms that have been agreed to to be effective, they need to be also slightly more specific in terms of how they're actually being implemented, and what we mean by them. And without a certain degree of specificity—and I'm not talking about red lines, which is obviously a whole different discussion of the pros and cons of identifying red lines—but the level that some of these agreements are at right now is still fairly vague and general. We talk about critical infrastructure in the GGE report, right? And if you look at different countries, different countries define their critical infrastructure very differently based on where they sit and what is particularly important for their economy.

One question, I think, that came up as a result of what happened last year, is to what extent election infrastructure is considered critical infrastructure across the board. So is that covered by the very norm? The similar question arose when the electrical grid in Ukraine was targeted. You actually had, since Stuxnet, the first real cyberattack, in the sense that for six hours power went out in Western Ukraine. And some people said that's a violation of the norms that were agreed to at the U.N. GGE because it's targeting civilians. Well, it turns out actually the United States Government considers Ukraine to be currently in an international armed conflict, and therefore it wasn't a violation of the norms.

But you also talk to several U.S. officials who say, no, it was a violation of the norms. So even within the U.S. and the OSCE we don't seem to have a consensus on what a violation of the norm actually looks like. I think there's a bigger question here in terms of moving forward, also for the OSCE, and the practical implementation of what's been

agreed to, that we need to get a little bit more specific so both sides understand when the line is crossed and what the implications are of that.

Mr. TIERSKY. Thanks, Tim.

Jaisha, I'd like to move to something a little more abstract for you, although it relates to Russia in the sense that one of the challenges that is often talked about in the context of cyber that makes it different than other domains is the problem of attribution. How does the problem of attribution, or knowing where an attack comes from, feature into these discussions on confidence-building measures or norms? Is it a part of what's being discussed in diplomacy when you're in these meetings in the informal working group in Vienna?

Ms. WRAY. You can't avoid the attribution factor, which is somewhat more challenging for some countries than others. But where these confidence-building measures come into play is after a state does have the attribution. Then it's a matter of: What are the next steps? What are the resources available to reach out to where the incident appears to be emanating? It provides a resource once the attribution step is crossed.

Mr. TIERSKY. Anybody want to comment on attribution?

Dr. CROWTHER. If you read reports like the Mandiant report on Advanced Persistent Threat 1, they have shown that you can actually trace things back to an IP address or an individual computer. The hard part is who does that computer belong to and who's actually operating that computer.

Mr. MAURER. I think we are spending way too much time talking about whether attribution is possible or not because, apart from the national security context, law enforcement agencies for decades now have been able to arrest cyber criminals. So, if you look at the U.S. Secret Service, the FBI, for decades now have been arresting particularly criminals from Eastern Europe, and the only reason they were able to do that, and then for them to actually go to jail in the U.S., is because they were able to do the attribution that was required to also meet the standard that's required in U.S. courts for somebody to go do jail.

I think that there was a bit of a longtime debate about whether it's possible that shifted to how long it takes for attribution to actually be possible. And as Jaisha just pointed out, I think the debate needs to move much more in a direction of what are the implications of asymmetric attribution capabilities—meaning, yes, it is possible for a certain number of states, especially those that can combine signals intelligence and forensics with human intelligence and having spies in certain countries, to corroborate what they're hearing and to figure out who was actually behind it—and what is the implication of that for countries who will not have that capability, and what are the implications of that for the coalition and the alliance—the NATO alliance. Because if we have a NATO partner that requests, for example, assistance from the U.S. Government when it comes to attribution, there are always tradeoffs involved from an intelligence perspective, because if you share that information you might burn an intelligence source. And it gets even more complicated if you move beyond NATO and the alliance framework when it comes to international incidents with countries that might not be a partner or ally, where you might have to have a briefing on the Security Council and demonstrate what happened. So I think that those are some of the looming questions when it comes to attribution moving forward.

Mr. TIERSKY. From my perspective, that brings us back to a point that Jaisha made, which is the potential utility of regional organizations like the OSCE to help build the capacity of countries to engage perhaps not on something as what I would say high level as digital forensic attribution, but even just to engage in the discussions on cyber policy. Do I have that right?

Ms. WRAY. In terms of capacity building, exactly—we just last week were in Uzbekistan, and the first step with some governments is just raising awareness on what the CBMs are, and capacity-building in terms of helping to understand how you need to organize within your own government, and make sure that all the agencies are aware of the CBMs and the processes that should be in place should an incident occur.

Mr. TIERSKY. Ladies and gentlemen, I have a zillion more questions, but I would love to hear from you or perhaps any of our Facebook users. Does anyone have something they would like to put on the table? Yes, please, in the back. Because of our video feed, if you wouldn't mind coming to the microphone, that would be very helpful for us, thanks. And if you could identify yourself, appreciate it. Attribution, of course. [Laughter.]

QUESTIONER. I'm Diana Parr from Representative Ted Lieu's office.

Question about the incident management part. You said there's a lot of confusion on, do the different countries actually have a mechanism for communicating with each other. So you looked at the ransomware attacks like WannaCry and Petya, and the ability for these different international countries to communicate between each other about the fact that this malware's coming is really important. And the government's put in the CTIIC and the NCCIC that DHS manages. Is anything happening in that area to formalize it? And is anybody leading that from a country perspective?

Mr. MAURER. I think this relates to the capacity-building efforts that Jaisha mentioned, where the computer emergency response teams—that there's now a growing number of national computer emergency response teams that are for each state set up to essentially help with the communication in terms of that. But there remains huge confusion, even in Europe, where some of the anecdotes that after the ransomware attacks happened, where companies called institutions that they shouldn't be calling for cyber kind of incidents.

So one is building the institutions where many countries still don't have a CERT that they should be setting up, so that they have a point of contact. But then, even if there is a point of contact in the CERT, in some countries there are three or five people who are working part time because they don't have the resources to actually manufacture that.

And then, multinational companies, they have their own teams who don't really rely on these institutions. So I think that's where essentially that will be moving in the future in terms of the capacity building.

QUESTIONER. OK. Thanks.

Dr. CROWTHER. That's one of the things that makes the OSCE useful, is among their confidence-building measures are requirements for the 57 different signatories to be talking to each other, and requirements for them to share data on threats and things like that. So 57 of the 193 or 196 countries in the world, depending on what list you use, are theoretically operating off the same script.

Tim mentions that there's some confusion, but I would propose that there's confusion in the United States. There isn't a single phone number in the United States to call either. This is kind of an ongoing type of thing.

Ms. WRAY. And this OSCE points-of-contact list is more government-to-government. There's also the cert-to-cert and law enforcement channels. But through the OSCE, each state has been asked to provide a policy point of contact and a technical point of contact in case they want to try to reach out from a state perspective regarding an incident that rises to the level of national security concern.

Mr. TIERSKY. Thank you. That was a great question.

Yes, please.

QUESTIONER. Good afternoon. My name is Erin Dumbacher with the Nuclear Threat Initiative.

I'm curious if you could talk a little bit about whether you see in the critical infrastructure space potential for additional, or perhaps even more concrete and even more technical, confidence-building measures. In the past, you know, starting with scientist or technologist to technologist has worked globally. Is there an opportunity to focus on the industrial control side of things first, before we focus on everything else?

Ms. WRAY. Well, our focus has been now on implementation rather than the development of additional confidence-building measures. There's a degree of flexibility with the current confidence-building measures. For example, number 12 discusses workshops and seminars and roundtables, so I think there is a degree of flexibility of who could be involved and the specific topics there. So in the future, perhaps.

Mr. MAURER. At Carnegie we've been doing some thinking about what could be avenues to further advance the ongoing discussions, and particularly in light of the fact that earlier this year, in June, this group of governmental experts at the U.N. didn't produce a new report. And we for the past years have worked specifically on financial stability and cybersecurity, with the assumption being that that might be an area where there's a lot of common interest, even with countries where we might disagree on many other issues. We've actually put forth a proposal that this might be an area where we could make further progress, given the common interest—financial instability is something that most countries don't want—and whether you can build more cooperation on that particular issue to tackle the threat and threat actors that might still have an interest to potentially do this kind of thing. So that goes back to the earlier comment about trying to get a little bit more specific on what certain agreements mean operationally and moving that forward.

Ms. WRAY. I'd also encourage you to look at the CBM 15, which is focused just on critical infrastructure and engaging various aspects, including industrial-control systems and raising awareness on that importance, sharing national views. And I think the OSCE is very focused on the importance of critical infrastructure and the need to increase confidence in that specific arena.

Mr. TIERSKY. I understand we have a couple of questions coming from our Facebook feed, and I would like to take both of those at once.

Ms. HOPE. Hi. The first question, I think, was covered in your last answer, so thanks very much. You've preempted one of our online questioners.

The second question is from Geoff. He asks, establishing norms and confidence-building measures may work well for nation states, but what diplomatic tools are available to mitigate the threat of nonstate actors, such as terrorist groups and criminal networks, from using cyber weapons against us?

Mr. TIERSKY. Excellent question from Geoff. I'm sure our panelists will want to jump on. So what about nonstate actors? I would add not only the question of how does the diplomatic process address the threat from nonstate actors, but also flip it on its head and what nonstate actors, including the private sector—how do they participate in the diplomatic process productively?

Let's start first with the threat and kick that around a bit. Please, Alex.

Dr. CROWTHER. The good news, getting back to my previous comment about international law does run writ in cyberspace: Terror and crime are against the law. We all have codes. All of the countries have legislation that defines what is a crime and what is terror. That's working pretty well.

Part of the problem is, obviously the diplomatic side of things doesn't bring in terrorists or crimes, but, like the Budapest convention, which started out as a European thing but is now global, is a convention that defines certain cybercrimes. And their goal is to kind of define the spectrum of crimes. The Tallinn Manual, of which the second version just came out, also talks about operations in cyberspace, both in an in-war context but also not-in-war context. So they talk about that as well. But the anonymity of cyberspace really kind of super-empowers terrorists and criminal organizations.

Ms. WRAY. Regarding terrorist use of the internet, on the diplomatic front we are working cooperatively with other governments to ensure that we can protect our networks, to defend against incidents coming from terrorist use of the internet. But bringing this back to the OSCE an example where we might be able to see the CBMs in place is that if there was an incident that appeared to be emanating from another state's territory, and you called that state and they weren't aware of it because it wasn't a government activity, it could be an opportunity for those states to work together to mitigate the incident.

So it could be that it's a proxy incident. And just because I am making a call to another government does not mean that I am blaming them. I'm calling to inquire and see if we can share information about the incident.

Mr. TIERSKY. Let's talk about the second piece of that, then, that I raised, which is the good nonstate actors, so to speak. What is the involvement of public-private partnerships? You know, help us understand to what extent relationships between governments and the private sector feature into any of these discussions, certainly into implementation of these confidence-building measures.

Mr. MAURER. I think there are a couple of components to that. And the first one is, unlike probably any other security realm, you have private companies that have investigative teams that can conduct attribution at a very similar level to governments and probably better than most countries. So you have your security companies that have been detecting malicious activity in their published reports and that put that out in the limelight and often expose state-sponsored malicious activity, which you don't really see in many other spaces.

You don't really see a lot of other security environments where a covert operation might be exposed other than through an investigative journalist. But when it comes to cybersecurity, you have all of these companies that have an incentive model, a market-driven, profit-driven model, to put out these reports and to expose essentially what are covert operations by states. So that is one that I think is an important factor here.

The other one is, you have an entire industry that's based on identifying vulnerabilities and trying to find the vulnerabilities and then to patch them that are used for offensive cyber operations. So while, on the one hand, you have the arms race among countries now to develop offensive capabilities, you have this private-sector disarmament race of essentially private companies trying to find these vulnerabilities and to match them, and thereby disarming the access point that has been developed to deploy certain payloads for offensive cyber operations.

And then the third one that I'd mention is that a lot of the major internet companies have a visibility into a network that a lot of governments don't have. And in order to get a full comprehensive picture, the two need to be talking to each other to really understand what is happening, because many malicious actors don't just target an individual company, but they might target multiple companies.

And there have been incidents where one company has been hacked and the company's like, oh, I got hacked, but I don't really need to report it because they can't really do much with just our information. But another company has been hacked as well and thought the same thing. And if you put the two together, the malicious actor actually had a lot of information that was a lot more useful by combining the two. And that requires kind of a coordination both within the companies, but then also with the government, to really understand what kind of campaign is going on and what has happened.

Ms. WRAY. I'll highlight that in the lead up to the latest round of the U.N. Group of Governmental Experts, the United States and the Netherlands sponsored a series of workshops that were hosted by the U.N. Institute for Disarmament Research and CSIS on some of these issues related to norms and international law and confidence-building measures that involved industry and academia and a wide range of participants to seek input in advance of the formal U.N. governmental group, which includes only governmentally designated experts.

The OSCE informal working group is also a governmental meeting. But, that said, one of the newest CBMs in the last year's tranche, CBM 14, talks about promoting public-private partnerships. So that is something where the OSCE does want to focus in the future. And I'll note that in the workshop I attended last week, we had some folks from the private sector and academia in attendance as well. We are seeking to involve our industry partners as well as academia in these discussions as much as possible.

Dr. CROWTHER. Both in North America and in Europe, 90 percent of the internet is in private-sector hands. The United States, the European Union and NATO all have very strong efforts to build public-private partnerships. And the United States also, when the U.S. Government talks about internet governance, we prefer a multi-stakeholder approach. And we tend to involve the private sector in that as well, where they're actually invited in as voting members of whatever organization it is.

Mr. TIERSKY. Great. Let me go back out to the audience, if anyone has a question they'd like our brilliant panel to bat around.

QUESTIONER. This is kind of a more general philosophical question. In view of the name of the organization, the word cooperation sticks out at me. I was just noticing Uzbekistan, Turkmenistan, Tajikistan, Serbia, Turkey and Russia.

What is going on in the organization as they meet to deal with the relative un-aspect of the cooperation of these nations, particularly in light of this latest struggle with the cyber issue? Now, I know some of those nations mentioned are kind of who-cares coun-

tries, I guess, when it comes to the technology aspect of this. But I'm assuming they have some influence because of their membership.

Mr. TIERSKY. Thanks. Actually, that may be a question that I would have a couple of thoughts on myself, as someone who's regularly out at the OSCE. And I think it's broader than just the question on cyber that we've asked the panelists to discuss, but I will want the panelists to, if they have any words.

The value of the OSCE is precisely in the fact that it is the organization of 57 participating states, from Canada all the way to Russia, where the participating states have agreed, in founding the organization and in signing up to a number of very basic commitments, that include respecting the territorial integrity of other countries, respecting their sovereignty, respecting their ability to choose their own security alliances, but also on basic principles that human rights are important and a concern to all.

This is a place where that discussion happens on a weekly basis, where countries are expected to hold each other to account for not living up to those commitments, whether it be on human rights, on military transparency, and now increasingly on some of these cyber confidence-building measures, where they are discussed on a regular basis.

I don't think anyone on the panel is suggesting that everything is an easy discussion in Vienna or in most other international fora. But I think, from the Helsinki Commission perspective, we certainly see the value of an ongoing dialogue, in particular where we disagree. We need to make sure people remember the principles that the organization is founded on and that all of the 57 participating states have signed up to.

So having given that bumper-sticker full-throated endorsement, would anyone like to comment further on that? Thanks.

Ms. WRAY. Now, we've managed to maintain a working relationship with all 57 OSCE participating states through the Cyber Informal Working Group and managed to get consensus twice on the various confidence-building measures. And I think we're lucky in a sense that the issue is relatively technical and it's focused on reducing misperceptions and figuring out procedures if there were to be an incident. We've been able to keep it at a fairly technical level and make really groundbreaking progress.

Mr. TIERSKY. You mentioned, Jaisha, that the U.S. Government's intent to develop confidence-building measures in ICTs, information communication technologies, was not limited to the OSCE but that the United States also participates in the ASEAN Regional Forum and the Organization for American States.

It's my perception that the OSCE is kind of the head of the class, as it were, in terms of the regional organizations that are actually working on this issue. Why is that? And I'd like others to comment if they would wish to.

Ms. WRAY. Well, we started earlier through the OSCE process. We have a bit of a head start. We also have an able secretariat, which is hugely useful in terms of moving us along through our implementation and priorities, whereas the ASEAN Regional Forum does not have a secretariat.

And so while the other two regional groups are a bit behind, we're trying to do work between the regions. For example, there was a workshop in the spring in Seoul with the ASEAN Regional Forum and the OSCE to kind of provide lessons learned from the OSCE, as the ASEAN Regional Forum begins to develop their own confidence-building measures. I think efforts like that will be important to ensure that all of these regional groups make progress.

Dr. CROWTHER. I'm actually helping the Organization of American States with theirs. I'm running a two-day get-together in Miami next month, as a matter of fact, to do that. But if you think about these different organizations, who are the four major cyber actors in the world? U.S., Russia, China and Europe. Well, three of the four are in the OSCE. And that's the only organization that has three of the four. And that's why I think the most way forward is happening there.

Mr. TIERSKY. Audience, last chance for questions. And then I'm going to challenge the panel with a last big-picture question.

QUESTIONER. Hi. I'm Lauren Williams. I'm a reporter with FCW.

I have two questions. One, has there been any discussion of when a cyberattack warrants a kinetic attack, or vice versa, since we're moving to a space where all operations are going to become one?

My second question has more to do with modernization. We talked a little bit about asymmetrical capabilities. And I want to know where that fits in, particularly with DOD and how we're working with other countries on that, and making sure that we can protect ourselves but also other countries being on the same level—or if it's, I guess, making sure that we don't get to, like, a nuclear arms race, but in cyberspace.

Mr. TIERSKY. I suppose both of those questions would relate to the concept of escalation from cyber to kinetic. Well, I suppose that needn't necessarily be an escalation, but certainly not getting into an arms race in cyber.

Alex, you seem eager to jump. Please.

Dr. CROWTHER. So in the 2011 U.S. International Strategy for Cyberspace, it says that we will reserve the right to respond in any way that we see fit, including all the elements of national power—diplomatic, information, military and economic—understanding that the military is a last resort.

There's a lot of discussion about this in the international-law crowd, as you could imagine. The prevailing definition of when something crosses the line of being an armed attack under the U.N. charter is when the cyber operation has the same effect as a kinetic operation. If you drop a bomb on a village and it destroys buildings and kills people, that's clearly an attack, right, an armed attack. If you open the sluice gate of a dam and it washes away the village and destroys buildings and kills people, that's clearly an armed attack because it achieves the same effect.

There are differing opinions out there on when that threshold is triggered. And I must say the Russians are doing a very competent job of operating in what is known as the gray zone, which is very specifically designed to stay under a threshold which would trigger a military response.

In reference to helping other countries, unfortunately, because cyber is new and because everybody is building their cyber capabilities, it's kind of like building the car while driving it. There's not a whole lot of additional capacity left over to do building-partner-capacity type things. So there's a long list of partners that have asked for help and that we want to help, but it's very difficult to generate the additional cyber resources to help them out. That is being looked at both by Cyber Command, by the Office of the Secretary of Defense, and each of the combatant commands as well. And European Command is working with partners. NATO also has a capacity to help build partner capacity within the alliance.

Mr. MAURER. And just on the point of the capabilities and the asymmetric threat, I think that's already happening. And we're already seeing this arms race taking place where North Korea, just being in the news in the last two or three years, is the latest state that has been escalating, how aggressive it's become in using hacking.

For example, prior to offensive cyber capabilities, we were worried about the North Korean conflict becoming global once it would get ICBMs. Hacking has now made this conflict global because you can reach—geography doesn't really matter anymore in terms of the reach you can have. And the cost of these tools is nothing compared to conventional weaponry that were to be built.

I think right now what we're seeing is that most nonstate actors are profit-driven rather than politically active. It's more a question of intent and who would have an intent to really exploit the kind of vulnerabilities that currently exist. But there are certainly nonstate actors out there that are very capable. In terms of how this might progress, I'm more worried about how the nonstate-actor threat will evolve compared to some of the state-based, and how states will use nonstate actors to project power as proxies.

Ms. WRAY. Regarding whether these bodies are talking about kinetic attacks, the purpose of the OSCE Cyber Informal Working Group is to kind of prevent that from happening in the first place. We're very focused on the other end, and what can we do to prevent a conflict before it reaches that stage?

And then, with regard to capacity-building, where we're focused in that realm can be at the very basic level, so it's helping other countries write a cybersecurity strategy or helping them investigate cybercrimes. We use that as a tool to ensure the internet is more secure, interoperable and reliable.

Mr. TIERSKY. Wonderful.

I am going to pose a final challenge, but I'm going to pose it to the speakers on my right, because it's a challenge about talking about U.S. policy and what it should be.

What I would like Tim and Alex to chew on is, earlier in our conversation Alex referred to CBMs as our only hope, or our last best hope. Tell me what you think is the best-case scenario and the worst-case scenario for the development of CBMs and of norms for the next decade. And what does that depend on?

What I would like you to comment on, I think, in that rubric is the extent to which U.S. leadership is a driving factor in this field.

Would either of you care to start?

Dr. CROWTHER. Sure. The best-case scenario is that the U.S., the Europeans, the Chinese and the Russians all agree on confidence-building measures, they adopt transparency, and they swear and adhere to that they will never attack critical infrastructure.

The worst-case scenario is that nobody pays any attention to any confidence-building measures and just kind of runs amok, attacking each other's intellectual property, financial systems and other critical infrastructure at will. I don't really see that one happening because everybody's got critical infrastructure. So if you start—and I hate to equate it to nuclear warfare, but when you start dropping nukes on somebody else, they start dropping them on you. So if country A starts attacking the critical infrastructure of country B, what's to prevent country B from attacking the critical infrastructure of country A? So it's more of a mutually assured destruction scenario.

U.S. leadership is key in this whole thing. The executive branch, of course, is working this. The State Department is doing wonderful things with, for instance, the Group of

Government Experts and everything like that; Chris Painter's old office. Department of Defense is working on it. Congress could help out with this as well by essentially—remember earlier I said deterrence is coercion and denial. So the congressional role I would see more of supporting the denial part at home; for instance, mandating Internet of Things standards for security, or mandating kindergarten-through-12 cyber-hygiene education.

We could do things back home. And then that way, if everybody knows not to click on that phishing attack, that link—90 percent of successful cyberattacks come from phishing attacks. If every American knew not to click on the link and didn't click on the link, we would be much less vulnerable than we are today.

Mr. MAURER. I think it was Joe Nye who, a couple of years ago, came up with the phrase "mutually assured vulnerability" as the concept that might be underlying this field, and that that mutually assured vulnerability is actually one of the reasons why there might be restraint in the area, because there's such great interdependence that the type of operation that might be launched would backfire on the source of the malicious activity.

So in terms of best-case scenarios, my hope is that there will be much greater understanding of these interdependencies. Sometimes I have the impression that we are still in the very early stages of really understanding how the network operates and what is really connected to it and what happens if you do X and Y, and it might happen in Z, which you never expected. And that includes, I think, some of the leading countries in this; so a better understanding on that.

Second, I think right now what is blocking further progress is the insistence of some countries to combine what back in the 1970s with the Helsinki Accords were separate buckets. We had the bucket on security and you had the bucket on human rights and you had the bucket on security that was negotiated and had an outcome. And you had the bucket on human rights that had an outcome.

And some governments, who define information security much broader, to include things like content, and who are viewing information security as essentially the control of information, is combining and bundling these two buckets, which makes it impossible to make much more progress and substantial progress on the actual security side. And they do this because they have a concern about the stability of their domestic regime, which they prioritize over the security threat.

My concern is, looking at the security environment in the last decade, it's continued to deteriorate. The cost is going up. You've seen Maersk and another company who just reported that each company suffered a $300 million loss as a result of the ransomware earlier this year; two single companies suffering a loss each of $300 million a year because of a single malware that was locking out their systems.

So my hope is that these countries that have prioritized their domestic-stability concerns for reasons that make sense from their perspective will agree to decouple them out of the realization that the security risk that is tied to the technology is so great that we need to make further progress on the real security part of that.

Mr. TIERSKY. Great. Without putting Jaisha on the spot, I'd like to offer you the opportunity for any final thoughts on what you've heard today.

Ms. WRAY. Well, thanks again for the opportunity to participate in this panel. Like I said before, some of these issues are not widely known, so I think it's important to raise

awareness on the work the OSCE is doing as well as the really landmark reports that the U.N. Group of Governmental Experts have produced. And even though the last session was not able to reach consensus, it does not take away from the importance of these reports that reached consensus in the past. And the United States looks forward to continuing to work with the international community on these important issues.

And I'll note in particular one of our key priorities is trying to reach consensus on how international law applies in cyberspace.

Thank you.

Mr. TIERSKY. I'd like to thank the panel. These kinds of discussions are absolutely crucial towards informing the work of the Helsinki Commission and that of our members, both in their capacities as commissioners with us but also in their other roles as members of Congress and crucial committees that are making important decisions on a lot of this, but also our direct involvement in some of the discussions ongoing in Vienna.

Please, audience, join me in thanking our panel in the customary way.[Applause.] Thank you all for joining us. And thank you, Facebook, for providing some excellent questions as well.

This concludes the briefing.

[Whereupon, at 3:28 p.m., the briefing ended.]

○

This is an official publication of the **Commission on Security and Cooperation in Europe.**

★ ★ ★

This publication is intended to document developments and trends in participating States of the Organization for Security and Cooperation in Europe (OSCE).

★ ★ ★

★ ★ ★

www.csce.gov **@HelsinkiComm**

The Commission's Web site provides access to the latest press releases and reports, as well as hearings and briefings. Using the Commission's electronic subscription service, readers are able to receive press releases, articles, and other materials by topic or countries of particular interest.

Please subscribe today.