S. HRG. 115–716

STATE–SPONSORED CYBERSPACE THREATS: RECENT INCIDENTS AND U.S. POLICY RESPONSE

HEARING

BEFORE THE

SUBCOMMITTEE ON EAST ASIA, THE PACIFIC, AND INTERNATIONAL CYBER SECURITY POLICY

OF THE

COMMITTEE ON FOREIGN RELATIONS UNITED STATES SENATE

ONE HUNDRED FIFTEENTH CONGRESS

FIRST SESSION

JUNE 13, 2017

Printed for the use of the Committee on Foreign Relations

Available via the World Wide Web:
http://www.govinfo.gov

U.S. GOVERNMENT PUBLISHING OFFICE
38–379 PDF WASHINGTON : 2019

COMMITTEE ON FOREIGN RELATIONS

BOB CORKER, Tennessee, *Chairman*

JAMES E. RISCH, Idaho
MARCO RUBIO, Florida
RON JOHNSON, Wisconsin
JEFF FLAKE, Arizona
CORY GARDNER, Colorado
TODD, YOUNG, Indiana
JOHN BARRASSO, Wyoming
JOHNNY ISAKSON, Georgia
ROB PORTMAN, Ohio
RAND PAUL, Kentucky

BENJAMIN L. CARDIN, Maryland
ROBERT MENENDEZ, New Jersey
JEANNE SHAHEEN, New Hampshire
CHRISTOPHER A. COONS, Delaware
TOM UDALL, New Mexico
CHRISTOPHER MURPHY, Connecticut
TIM KAINE, Virginia
EDWARD J. MARKEY, Massachusetts
JEFF MERKLEY, Oregon
CORY A. BOOKER, New Jersey

Todd Womack, *Staff Director*
Jessica Lewis, *Democratic Staff Director*
John Dutton, *Chief Clerk*

SUBCOMMITTEE ON EAST ASIA, THE PACIFIC, AND INTERNATIONAL CYBERSECURITY POLICY

CORY GARDNER, Colorado, *Chairman*

JAMES E. RISCH, Idaho
MARCO RUBIO, Florida
JOHN BARRASSO, Wyoming
JOHNNY ISAKSON, Georgia

EDWARD J. MARKEY, Massachusetts
JEFF MERKLEY, Oregon
CHRISTOPHER MURPHY, Connecticut
TIM KAINE, Virginia

CONTENTS

Page

Gardner, Hon. Cory, U.S. Senator from Colorado 1

Markey, Hon. Edward J., U.S. Senator from Massachusetts 2

Merkley, Hon. Jeff, U.S. Senator from Oregon 3

Ravich, Dr. Samantha, Senior Advisor, Foundation For Defense of Democracies, Washington, DC 4

Prepared statement 25

Rosenbach, Hon. Eric, Co–Director, Belfer Center for Science and International Affairs, Harvard University, Cambridge, MA 6

Prepared statement 8

STATE–SPONSORED CYBERSPACE THREATS: RECENT INCIDENTS AND U.S. POLICY RESPONSE

TUESDAY, JUNE 13, 2017

U.S. SENATE,
SUBCOMMITTEE ON EAST ASIA, THE PACIFIC,
AND INTERNATIONAL CYBERSECURITY,
COMMITTEE ON FOREIGN RELATIONS,
Washington, DC.

The subcommittee met, pursuant to notice, at 2:50 p.m. in Room SD–419, Dirksen Senate Office Building, Hon. Cory Gardner, chairman of the subcommittee, presiding.

Present: Senators Gardner [presiding], Markey, Merkley, and Kaine.

OPENING STATEMENT OF HON. CORY GARDNER, U.S. SENATOR FROM COLORADO

Senator GARDNER. Well, thank you. I will call this hearing to order.

Thank you all for being here and welcome to the third hearing in the East Asia, The Pacific, and International Cybersecurity Policy Subcommittee meeting in the 115th Congress.

Today's topic is state-sponsored threats in cyberspace, which has emerged as one of the primary national security challenges for the United States Government, the primary risk to the U.S. economy in the private sector, and the primary threat to our Nation's critical infrastructure.

Simply put, our national and economic security depends on both securing our networks and effectively deterring our adversaries who are getting stronger, not weaker, by the day.

According to the 2017 Worldwide Threat Assessment of the United States intelligence community, "our adversaries are becoming more adept at using cyberspace to threaten our interests and advance their own, and despite improving cyber defenses, nearly all communication networks and systems will be at risk for years."

The report specifically mentions China, Russia, Iran, and North Korea as the four cyber actors of greatest concern. These countries have developed asymmetric cyber capabilities that can cause significant damage to the United States and American interests with little public awareness of the immense consequences.

Yesterday, the "Washington Post" reported hackers, allied with the Russian Government, have devised a cyber weapon that has the potential to be the most disruptive yet against electric systems that Americans depend on for daily life. This is the same group that attacked Ukraine's electric grid in 2015, leaving 225,000 people without power. Last month, the so-called WannaCry ransomware affected over 200,000 users in 151 countries, allegedly by exploiting certain machines with an unpatched software flaw.

Our policies have not effectively kept up with the threat. The U.S. international strategy for cyberspace is now over 6 years old, and so in technology terms, it is a fossil.

Our efforts to develop effective global cyber norms and the components that are necessary for global partnerships have also sputtered. As the 2017 Worldwide Threat Assessment stated, although efforts are ongoing to gain adherence to certain voluntary, nonbinding norms of responsible state behavior in cyberspace, they have not gained universal acceptance, and efforts to promote them are increasingly polarized. The good actors are being outpaced by the dark arts of cyber.

Our diplomatic and economic response has been similarly lacking. Despite the bevy of executive orders and legal authorities available for successive administrations to punish state-sponsored actors, only a handful of North Korean actors were designated after the Sony attack in 2014.

Last year, Senator Menendez and I led the passage of the North Korea Sanctions and Policy Enhancement Act, the first legislation to mandate sanctions on malicious cyber actors working on behalf of that regime regardless of where they are based. Not one—not one—has been designated to date under this legislation.

Cyber attackers do not sleep. They do not sleep at the switch. They reprogram it. We must choose to either use all instruments of national power, including diplomacy, economic sanctions, and offensive capabilities to deter the malicious cyber actors or cede the field to our adversaries and face catastrophic consequences.

I look forward to hearing from our distinguished witnesses today on ways that we can strengthen U.S. policy to address these grave threats.

With that, I will turn it over to our ranking member, Senator Markey from Massachusetts.

STATEMENT OF HON. EDWARD J. MARKEY, U.S. SENATOR FROM MASSACHUSETTS

Senator MARKEY. Thank you, Mr. Chairman, very much. And thank you for convening what I believe is going to be one of the most important hearings that is conducted here in Washington this week.

As you mentioned, the recent WannaCry ransomware attack has yet again highlighted the vulnerability of digital devices to exploitation and disruption by malicious actors. Today's era is known as the IOT, the Internet of Things. But IOT can also stand for Internet of Threats.

And 24 years ago in April of 1993, I, as the chairman of the Telecommunications Committee in the House of Representatives, conducted a hearing in 1993, during which a group of specialists from Sun Microsystems demonstrated in real time how simple tools could be used to steal data from personal electronic devices. That hearing showed that the architecture of the Internet was created for ease of access, not for security. And as Secretary Rosenbach notes in his testimony today, heavy U.S. reliance on digital devices and communications means that these security gaps could have an outsized impact on U.S. national security and economic prosperity. That hearing in 1993 also demonstrated, as they pointed out, how there could be a cracking into the Kremlin or to the Pentagon or to our South Pacific fleet.

So these are not new issues. These are issues that we just cited not to fully deal with in terms of what the implications are for our Nation.

And just yesterday, the "Washington Post" reported that Russian hackers have developed a cyber weapon that can attack our electricity systems. They were already successful in disrupting an energy system in the Ukraine, making it that much more important that we double down on protections to have our grid at home be protected.

In fact, just a few Congresses ago, Congressman Fred Upton and I were able to pass a bill through the House of Representatives, which was called the GRID Act, that mandated an upgrading in the overall protections against cyber attacks which could occur in our country. But that was in 2010. It came over here to the Senate, and unfortunately it died. But those hearings—that record all was established because the National Security Agency, because the intelligence agencies had come to Fred and I asking us to do something because they felt the threat was real.

So this is something that is possible. It already happened in the Ukraine. It is something that keeps national security people up at night worrying about how vulnerable our own national electricity system could be and other parts of our system as well. That is why this hearing is so important.

Thank you, Mr. Chairman.

Senator GARDNER. Thank you, Senator Markey.

Senator Merkley, thanks for joining us. Anything that you would like to say off the bat here as we begin?

STATEMENT OF HON. JEFF MERKLEY, U.S. SENATOR FROM OREGON

Senator MERKLEY. It is extremely important, both as it relates to the security of our infrastructure, certainly the security of our elections, the security of our financial systems. We have seen attacks in each area, and I am looking forward to the testimony of our experts.

Senator GARDNER. Thank you, Senator Merkley. Thanks for joining us today.

We will turn to the testimony now. Our first witness is Dr. Samantha Ravich who currently serves as a Senior Advisor to the Foundation for the Defense of Democracies, or FDD, as well as the principal investigator on cyber-enabled Economic Warfare Project at FDD's Center for Sanctions and Illicit Finance. Dr. Ravich is the former Deputy National Security Advisor for Vice President Cheney and served in the White House for over 5 years. Following her time at the White House, Dr. Ravich was the co-chair of the congressionally mandated National Commission for Review of Research and Development Programs in the United States intelligence community. Welcome, Dr. Ravich.

Our second witness today is the Honorable Eric Rosenbach, who serves as Co-Director of the Belfer Center for Science and International Affairs at the Harvard Kennedy School. Mr. Rosenbach formerly served as chief of staff to Secretary of Defense Ash Carter and also as Assistant Secretary of Defense responsible for leading all aspects of the Department's cyber strategy, policy, and operations. He also served here in the Senate as national security advisor for then Senator Chuck Hagel and as a professional staff member on the Senate Select Committee on Intelligence. Welcome, Mr. Rosenbach.

And Dr. Ravich, thank you very much for being here, and we will go ahead and proceed with your testimony.

STATEMENT OF DR. SAMANTHA RAVICH, SENIOR ADVISOR, FOUNDATION FOR DEFENSE OF DEMOCRACIES, WASHINGTON, DC

Dr. RAVICH. Thank you. Chairman Gardner, Ranking Member Markey, distinguished members of the subcommittee, thank you for inviting me to participate in this important hearing.

My testimony today focuses on an area that I believe is woefully underappreciated, yet cannot be more important for our country, and that is the use of cyber means by adversarial states to purposefully undermine our economy in order to weaken us militarily and politically.

It is my contention that the threats are real, the warfare is ongoing, and that the U.S. Government is inadequately structured to properly and comprehensively detect, evaluate, and address cyber-enabled economic threats. The U.S. Government has made great strides in organizing itself to protect and defend the .gov and .mil realms, but our Nation's greatest vulnerability may lie with adversarial attacks on the U.S. private sector.

It is true that the business of America is business, and the business of America is at risk of being hollowed out from the inside by everything from theft of intellectual property to the malicious infection of the supply chain to the degradation of confidence in our commerce, banking, and transportation sectors.

But it is not the pure cyber criminal that should keep this committee up at night. Rather, it is the hostile state actor who recognizes that while it may not be able to compete directly with America's strength of arms, it holds a significant asymmetric advantage in attacking our economic wherewithal and, by so doing, weaken us militarily or politically. We call this purposeful strategy cyber-enabled economic warfare.

Two of the most active players in this field are the Chinese and the North Koreans. For decades, China has been engaged in a massive, prolonged campaign of intellectual property theft against U.S. firms, costing potentially hundreds of billions of dollars and more than 2 million jobs. China's IP theft campaign constitutes a large, if not the largest, part of what appears to be Beijing's overall cyber-enabled economic warfare strategy against the U.S. and the West more generally, which they themselves have described as, "a form of non-military warfare which is just as terribly destructive as a bloody war but in which no blood is actually shed."

Recently Beijing punished a private South Korean company in part by denial of service attacks for participating in the THAAD deployment. The revenue loss was marginal, but the move has prompted deep concerns in Seoul. South Korea exported over $120 billion to China last year, about a quarter of the country's total exports, and is particularly vulnerable to Chinese coercion. A possible result, South Korean President Moon has suspended further deployment of THAAD.

However, Washington and its allies have been slow to comprehend the threat from China primarily because they view each cyber-enabled economic attack individually as separate incidents instead of collectively as elements in an overall coordinated campaign.

And North Korea. South Korean police cyber investigators stated in 2016 that North Korea had operationalized a long-term plan involving the seeding of malicious code at over 160 South Korean private firms and government agencies, "aimed to cause confusion on a national scale by launching a simultaneous attack."

As well, North Korean hackers most likely initiated the WannaCry ransomware attack. The monetary haul from the scheme was minimal, leading some analysts to question if the effort was a test for a larger attack. Similar assessments have been made about the 2016 cyber bank heist on the New York Fed tied to a North Korean cyber group. While some have remarked that it appears that the North Koreans may now be robbing banks, it is more chilling to consider that the North Koreans now may be targeting our banking sector.

With a GDP per capita of barely $1,000, North Korea has an obvious need to rob banks. But Kim Jong-un is not simply a Korean Willie Sutton. In a military confrontation with the U.S. and South Korea, Kim would look to any capability that could help even out the overwhelming military advantage of the allies. Attacking our economies, which he has already proven he can and will do, may be the quickest way to gain battlefield advantage since it could potentially cause panic in our markets and on our streets.

Without a concerted effort, the United States' economy will become increasingly vulnerable to hostile adversaries seeking to undermine our military and political strength. The U.S. Government must immediately undertake a number of actions to prevail in this new battlespace, including sustained attention in understanding the capabilities and intentions of adversarial leadership with a long-term strategy to deter and defeat them.

But the U.S. cannot go it alone in its endeavors to safeguard the networks and systems upon which our economy depends and which we must take steps to formalize the cyber partnerships that already exist with the other free market democracies that are leaders in cyber science and technology, specifically with the UK and Israel.

I have included additional recommendations and policy prescriptions in my written testimony. I thank you for the opportunity to testify, and I look forward to your questions.

[Dr. Ravich's prepared statement is located at the end of this hearing transcript, beginning on page 25.]

Senator GARDNER. Thank you, Dr. Ravich, and thank you for being very prompt. Thank you.

Mr. Rosenbach?

STATEMENT OF HON. ERIC ROSENBACH, CO–DIRECTOR, BELFER CENTER FOR SCIENCE AND INTERNATIONAL AFFAIRS, HARVARD UNIVERSITY, CAMBRIDGE, MASSACHUSETTS

Mr. ROSENBACH. Mr. Chairman, before I started, I wanted to let you know something I hope does not get me in trouble with Senator Markey. I was born and raised in Colorado, a die-hard Denver Broncos fan. So despite the fact I live in Cambridge, Massachusetts, I am going to fly a big Denver Broncos flag out there all the time.

Senator GARDNER. Did you go to school at the University of Colorado, the hub of the West?

Mr. ROSENBACH. I grew up in Colorado Springs and Breckenridge. So not in college, but still cheering for the Orange Crush. Sorry, Senator.

Chairman Gardner, Ranking Member Markey, and Senator Merkley, thank you very much for the invitation and thank you for calling this important hearing today.

As technology advances and we become more connected, we increasingly live in a digital glass house that must be much better protected. I like to use the glass house analogy because it helps to illustrate two important points.

First, that cyber warfare is truly asymmetric: a small nation with an offensive cyber capability can have an outsized effect on a larger power. For example, the U.S., a technological and economic powerhouse, is significantly more vulnerable to cyber attack than North Korea, as we just heard from Dr. Ravich, a nation most citizens do not even have an Internet connection. We should, therefore, think very carefully about the implications of a possible North Korean cyber attack against the United States, something that I unfortunately believe is likely to happen within the next year if current trends continue.

Second, democracies' transparent, open societies also make them vulnerable to foreign information operations. This vulnerability is exacerbated by high levels of Internet accessibility and the rapid pace and breadth of information sharing. In contrast, authoritarian societies like China, Russia, and North Korea often control the media, censor domestic online activity, and shield their nations to some degree from outside information and cyber operations through the use of national-level firewalls like the Great Firewall of China, for example.

Unfortunately, no nation, including the United States, has responded to Russia's recent potent hybrid of cyber and information attacks in a way that is visible and forceful enough to deter future attacks. The fragility of our national security posture, combined with our adversaries' perception that Russia's recent actions achieved unprecedented success, increases the likelihood that the

U.S. and our allies will experience more serious attacks like this in the coming years.

Thus, the U.S. needs to bolster its deterrence posture by both raising the costs and decreasing the benefits to hostile actors of engaging in this conduct.

In 2015, the Department of Defense articulated for the first time our strategy on deterrence in cyberspace. In short, the strategy said that deterrence is partially a function of perception. We said that deterrence works by convincing a potential adversary that it will suffer unacceptable costs if it conducts an attack against the United States and by decreasing the likelihood that the potential adversary's attack will succeed. And this is all based on their perception of that.

In terms of increasing the costs of an attack, the U.S. and international community should be less circumspect about employing all available foreign policy tools, particularly those outside of the cyber domain. Given the glass house effect that I previously described, we should be careful about responding to cyber attacks with military options. However, we should be prepared to use our superior cyber capabilities strategically and creatively to demonstrate our willingness to act in the face of serious provocations.

Additionally, the U.S. must increase the costs of cyber and information operations by using foreign policy tools outside the military domain such as: 1) attributing publicly cyber and information attacks as soon as we have confidence in their origins and not waiting for months or longer; 2) pushing for sustained multilateral economic sanctions against states that use cyber and information weapons; 3) reinventing our capabilities with respect to information operations and our strategy for countering them; and 4) taking a leading role in building international capacity to disrupt the proliferation of black market destructive malware.

As I mentioned, reducing the benefits that adversaries derive from cyber and information operations is another key aspect of bolstering our deterrence posture. To do this, the administration, Congress, and the private sector should work together to: first, pass legislation that the government and the private sector can share threat information, including with State election bodies and campaigns to facilitate that; two, legislate mandatory compliance of the new Cybersecurity Framework, something that I know you have done some work on; three, pursue aggressive steps to mitigate the effect of information operations on the platforms of leading tech companies, including Facebook, Twitter, and Google; and four, incentivize private sector investment in cloud-based security, blockchain-enabled transactions, and quantum computing.

In the interest of time, I will submit the rest of my testimony for the record.

But I would like to say that the strength of the American tech sector has driven the American economy for almost 2 decades, driven our democracy. It is very important that we protect that center of gravity by bolstering our deterrence posture and doing some of the things that I spoke about and some of the things also that Dr. Ravich just mentioned as well.

Thank you very much.

[Mr. Rosenbach's prepared statement follows:]

PREPARED STATEMENT OF HON. ERIC ROSENBACH

"Living in a Glass House: The United States Must Better Defend Against Cyber and Information Attacks"

Chairman Gardner, Ranking Member Markey and other distinguished members of the Committee, thank you for calling today's hearing on cybersecurity and for the invitation to testify.

As technology advances and we become more connected, we increasingly live in a digital "glass house" that must be much better protected. I like to use the glass house analogy because it helps illustrate two important points.

First, that cyber warfare is truly asymmetric: a small nation with an offensive cyber capability can have an outsized effect on a larger power. For example, the U.S.—a technological and economic powerhouse—is significantly more vulnerable to cyberattack than North Korea, a nation where most citizens do not even have an internet connection. We should therefore think very carefully about the implications of a possible North Korean cyberattack on the United States, something that I believe is likely to happen within the next year if current trends continue.

Second, that democracies' transparent, open societies also make them vulnerable to foreign information operations. This vulnerability is exacerbated by high levels of internet accessibility and the rapid pace and breadth of information sharing. In contrast, authoritarian societies like China, Russia and North Korea often control the media, censor domestic online activity and shield their nations (to some degree) from outside information and cyber operations through the use of national-level firewalls, such as the Great Firewall of China.Unfortunately, no nation, including the United States, has responded to Russia's recent potent hybrid of cyber and information attacks in a way that is visible and forceful enough to deter future attacks. The fragility of our national cybersecurity posture, combined with our adversaries' perception that Russia's recent actions achieved unprecedented success, increases the likelihood that the U.S. and our allies will experience more serious attacks in the coming years.

Thus, the U.S. needs to bolster its deterrence posture by both raising the costs and decreasing the benefits to hostile actors of engaging in this conduct.

In 2015, the Department of Defense articulated for the first time our strategy on deterrence in cyberspace. In sum, the strategy articulated that deterrence is partially a function of perception. As the DoD strategy explains, deterrence works by "convincing a potential adversary that it will suffer unacceptable costs if it conducts an attack on the United States, and by decreasing the likelihood that a potential adversary's attack will succeed." [1]

In terms of increasing the costs of an attack, the U.S. and international community should be less circumspect about employing all available foreign policy tools, particularly those outside of the cyber domain. Given the "glass house effect" that I previously described, we should be careful about responding to cyberattacks with military options since the U.S. has more to lose from an escalation in cyber-initiated conflict. We should, however, be prepared to use our superior cyber capability strategically and creatively in order demonstrate our willingness to act in the face of serious provocations.

Additionally, the U.S. must increase the costs of cyber and information operations by using foreign policy tools outside the military domain, such as: 1) attributing publicly cyber and information attacks as soon as we have confidence the origins; 2) pushing for sustained multilateral economic sanctions against states that use cyber and information weapons; 3) reinventing our capabilities with respect to information operations and our strategy for countering them; and 4) taking a leading role in building international capacity to disrupt the proliferation of black-market destructive malware.[2]

As I mentioned, reducing the benefits that adversaries derive from cyber and information operations is a key aspect of bolstering our deterrence posture. To do this, the administration, Congress and private sector should work together to: 1) pass legislation that improves the ability for the government and private sector to share cyber threat information, including with state election bodies and campaigns; 2) legislate mandatory compliance with the NIST's Cybersecurity Framework for critical

[1] The Department of Defense Cyber Strategy, April 2015, p.11.

[2] By disrupting the black market for destructive malware and other exploits, the international community would increase the costs associated with conducting? cyber and information attacks. This is a difficult challenge, but the Proliferation Security Initiative for weapons of mass destruction—a global initiative supported by over 100 countries—provides an analogous model for action.

infrastructure providers; 3) pursue more aggressive steps to mitigate the effect of information operations on the platforms of leading tech companies, including Facebook, Twitter and Google; and 4) incentivize investment in cloud-based security, blockchain-enabled transactions and quantum computing.

Developing and employing operational cyber capabilities is an important way to advance U.S. national interests. That said, we simply must keep sensitive vulnerabilities and exploits secure. Allowing this type of sensitive knowledge to get into the public domain damages American tech firms and increases the likelihood that hostile actors will conduct malicious actions against the U.S.

In sum, the strength of the tech sector and the internet has driven American economic growth and strengthened our democracy for the past two decades. The corollary of this success, though, is that the U.S. is increasingly vulnerable to cyber and information attacks. In order to maintain the "center of gravity" for the United States, we must bolster America's cybersecurity posture and rethink our strategy for countering foreign information operations.

Senator GARDNER. Thank you, Mr. Rosenbach.

And we will proceed with questions.

I guess I would kind of lay out just a question about process and the construct of our ability to deal with cyber threats. You both mentioned various elements and various dimensions of the cyber challenge we face. You talked about cyber-enabled economic warfare. In your testimonies, you talked about IP theft. You talked about theft of intellectual property in the United States, which some estimate as high as $540 billion a year I believe is in your testimony. We have talked about how North Korea has hacked Sony Pictures. We have talked about the ransomware. And so there are so many different elements of cyber policy.

We have different elements within the Federal Government to respond to those. We have a tech czar at the White House. We have a cyber position at the Department of State. We have offices within the Pentagon.

As you look at the Federal Government, who is in charge of our cyber policy? Either one of you.

Mr. ROSENBACH. Senator, I think that is a great question. And I have to be honest, when I look at the administration right now, I am not as sure about that. There is still the White House cyber coordinator, but I am not sure, even during the Obama administration, that that position was empowered enough to bring all of the people from around the government to the table and to really drive some of the change that is necessary to make a big difference.

I think when it comes down to it, there has to be collaboration between all the departments and agencies. When I first started in the Obama administration almost 8 years ago, it was a mess in terms of figuring out even what the roles and responsibilities were and the lanes and the roads were for defending the country and working with the private sector. I think that is more established now, but we still could use a very strong leadership position there.

Senator GARDNER. Dr. Ravich, who is in charge?

Dr. RAVICH. Well, I have to agree with my co-panelist that for the entire apparatus there currently is not an empowered either an individual or an agency to do what I think is necessary which, borrowing a phrase from the military, is a bit of an OODA loop. I mean, how are we going to understand the threat that is out there so that we make sure that as we are putting in the right—either on the defense or an offense, it is having the effect that we want.

Right now, still cyber war is not run by computers. It is run by the man behind the man behind the computer. These are decisions being made on the adversarial state level by leadership and people empowered by the leadership in adversarial states. It does not just all of a sudden happen.

So the first of the OODA loop, observe. Do you we really know who is in charge of making these decisions in a Russia, in a China, in Pyongyang, in a Tehran so that we can exploit fissures and vulnerabilities to go after the people that are making those decisions and then funneling it down to the operators and being able to see the effects? I do not see this loop.

Senator GARDNER. And I think that is a significant problem that we face because we do not know who is in charge, and that is a big challenge because in your testimony I think you lay out as the U.S. economy grows and as an economy anywhere on the globe becomes more sophisticated, then they are more vulnerable and more susceptible to cyber attacks. And as the asymmetric ability of North Korea or Iran rises, it is pretty doggone important that we have somebody that we can turn to and say you are in charge of this government's cyber policy.

One of the things that I have supported and others on the committee have supported is the creation of a select committee on cybersecurity that would take the ranking member and the chair of each committee that has jurisdiction over cybersecurity, put them on one committee so that they can have a whole-of-government view because this is a complex issue. This is not just about weapons systems that the Defense Department Science Board noted that the nation's weapons systems are at risk from the malicious insertion of defects or malware. It is not just about that. It is not just about North Korea's Sony attacks. It is about changing decimal points at hospitals that could result in deaths. It is about a whole-of-government view, and we need to know who is in charge.

So with that being said, a scale of preparedness. Where on the scale of preparedness, 0 to 100, where is the United States Government in preparedness against some kind of major cyber event?

Dr. RAVICH. Well, given what I wrote in my testimony and what I said, that the U.S. Government looks after .mil and .gov and .com is essentially on your own, right there you are starting from less than 50 percent or more because who is watching out for the very lifeblood of our country? We would not be the number one military if we were not the number one economy. So I think right there you are starting out and you have the beginning of your answer.

Senator GARDNER. Mr. Rosenbach, just to maybe ask a different question to you. You talked about raising costs and decreasing benefits for the acts of a cyber hack. Did we make the costs sufficient enough on North Korea in relation to Sony? Did we make it sufficient enough in Iran after a variety of hacks of electric facilities in this country? Did we make it sufficient toward Russia? And I have an amendment to the sanctions bill that would require cyber sanctions on Iran. Just briefly if you could hit that and then we will turn to Senator Markey.

Mr. ROSENBACH. Yes, sir. I think in the case of the North Korean cyber attacks against Sony that the response was strong enough and was quite good because it then mitigated attacks from North Korea down the road.

That said, I do not think the response in the case of the recent Russian cyber and information operations against the United States was strong enough at all, which leaves, unfortunately, I think the perception that other adversaries will try to take advantage of our system to do something similar down the road.

Senator GARDNER. We are going to work on this week. So thank you.

Senator Markey?

Senator MARKEY. Thank you, Mr. Chairman, very much.

Turning to those Russian elections—the Russian interference in our elections, it does not have to be complex. It can be a relatively simple spear phishing attack, and that can ultimately have very important consequences within our country and just luring someone into giving over their credentials to an attacker. And by the way, the same thing could happen in China, lure people in in utilities to give over information that can be valuable then for the subsequent, much more devastating attack.

So when you were answering the questions of the chairman about the vulnerability of our government, when you look at the utility sector, Mr. Rosenbach, do they take it seriously enough yet? Do they actually want to spend the money in order to ensure that they have got state-of-the-art protections which are built in? Are they just willing to run kind of the risk that maybe they will be lucky and it will never hit them but they never had to spend the money in order to protect against an attack, which we know that Russia already launched against Ukraine successfully and that they or the North Koreans or other could launch against us? So does the utility industry take it seriously enough?

Mr. ROSENBACH. Senator, it is definitely on their radar. They have dedicated efforts. All of the utility companies look at this, but they do not take it seriously enough. And that is the right way to ask the question I think.

Senator MARKEY. Why is that?

Mr. ROSENBACH. I think when it comes down to it, some of this stuff can be expensive and it can be complicated. And normally you are not forced to do things unless you have to or there is a return to your bottom line. Cybersecurity is a cost center. In some domains—banks, for example—they are willing to spend the extra money because they see that it is a good investment. I am not sure it is the same in the utility sector.

Senator MARKEY. Joe Tucci is a friend of mine. He is the CEO of EMC. He was until Dell purchased EMC. But that is the largest company in Massachusetts. But within that company is a subgroup called RSA, which is kind of state-of-the-art cyber protections. And I asked Mr. Tucci. I said why do companies not buy the state-of-the-art from RSA? He said, well, they do not want to spend the money. And I said, well, what if they did spend the money? Well, he said, then they would be protected because we are constantly upgrading, but they do not want to spend the money. And then I continued to pursue it because it goes to government contractors or to private sector companies as well, just trying to probe why they will not spend the money. And as you said, it is a cost center. They do not want to spend it, but it causes inevitably kind of a catastrophic event.

So can you get into that mentality a little bit more and what your recommendations would be to us in order to make sure that we prepare our country properly for the inevitable, which is that cyber is going to become the tool which is used in so many more instances than conventional weapons because they do not potentially cause fatalities, but the disruptions could be catastrophic?

Mr. ROSENBACH. Senator, like I mentioned in my opening comments, a starting point is to make the NIST framework mandatory for critical infrastructure and the energy sector in particular. And remember, the private sector, the energy sector works with NIST on this to come up with the framework. It is not as if it is legislated in law that you need to have three firewalls and your networked needs to be architected in that way. When you read the "Washington Post" article from yesterday and you see what happened in Ukraine, you better take the warning because, if you do not both play defense and then have a strong deterrence posture, something bad is going to happen and we will regret we did not do more.

Senator MARKEY. And then you turn to the industry and you say to the industry, let us have standards. And they go, yes, but voluntary standards. Please do not make it mandatory. That would be like financially catastrophic for us. But we agree with you. It could be catastrophic if there is an attack on the electric grid.

So how do we deal with that issue if we know what the threat is, we know it happened in Ukraine, we know it could apply just as easily to the electric grid of the United States, and we have an industry that wants voluntary, not mandatory protections which are built into the system?

Mr. ROSENBACH. Sir, I think you need to legislate on it. You know, there have been various bills that incorporate both information sharing and some sort of standard for infrastructure protection. Do it in certain sectors. Make sure that it is not overly burdensome, that it is done in conjunction with the private sector. I also believe that it is a little counterintuitive but that it would do something to spur the economy and the tech sector because there would end up being more demand for that. And in the end, it would be two net positives rather than something that would be an overly burdensome regulatory regime.

Senator MARKEY. And I agree with you.

Do you agree with Mr. Rosenbach, Dr. Ravich?

Dr. RAVICH. I do. But I think this also points to an area where government-funded research and development is needed, whether we are talking about new advances in SCADA legacy systems or the truly long tail R&D that the private sector has a hard time making a case for up front with its investors because when they are going to get the returns from it is a little unknown are perfect areas for serious cyber R&D that I believe the U.S. Government should be on the forefront of promoting with, I would add, two of our closer friends and allies that are the other two most technologically savvy countries in the world, the UK and Israel. We should be thinking about working closer with those two nations in some form of cyber co-op with a structured R&D agenda as potentially the first thing that we go ahead on, things that the private sector may not put their money to do but is necessary for the security of our economies and our systems.

Senator MARKEY. Senator Merkley and I were in—Senator Gardner—we were in Israel last year, and that is one of the points that the prime minister was making to us, that they are really focusing upon cybersecurity. It is a big, new industry for them. And so when I got back up to Boston, I asked one of the cyber company CEOs about Israel. And he said, oh, they are the best. They are state-of-the-art. We bought five of their companies this year.

So you are right. There is a close working interrelationship, and it would get better if there is a mandate that especially the critical infrastructure in our country had to be protected. You would not have to worry. It would get developed and the costs would go down. The technology would become more ubiquitous, but until that signal is sent, I think we are going to just see a constant repetition syndrome of a cycle where the same thing happens. Everyone responds. They are actually shocked. They hope that the issue goes away. And then we wait for the very next thing to occur but in a slightly different setting.

Thank you, Mr. Chairman.

Senator GARDNER. Thank you, Senator Markey.

Senator Merkley?

Senator MERKLEY. Well, thank you, Mr. Chair.

And thank you both for your testimony.

Dr. Ravich, I was fascinated by your story about South Korea and China. If I understand right—is it pronounced Lotte?

Dr. RAVICH. Lotte.

Senator MERKLEY. The Lotte Company. That, of course, makes we want to go out and buy some coffee.

But the Lotte Company sold its golf course to the Government of South Korea so that they could put up the THAAD, the terminal high altitude area defense anti-missile system. And then the Chinese said, well, we will make an example out of them. They shuttered their stores, a traditional type of response. They then took down the Lotte website with a denial of service attack, so a cyber attack. And then the Chinese retailers dropped Lotte products from their sites. And all of this just as there was a new prime minister in South Korea—a new president who then sent an emissary to President Xi of China. And in short order, Lotte was unblocked and South Korea suspended the THAAD program.

Is it your understanding that really the suspension of the THAAD program came directly as a response to the Chinese cyber attack on South Korea?

Dr. RAVICH. Well, I do not know if it was a direct result or it is part of a larger pattern of Chinese coercion against the South Koreans in this context. When China looks at all of the different muscles that it can flex when it has that type of trading arrangement with the South Koreans and know that the South Koreans have that much product that they are selling into China, China holds a lot cards. And this was clearly a shot across the bow in Seoul. You do this. These are the types of effects you are going to feel. The DDoS attack was a small attack monetarily-wise but clearly these things are all part of a pattern. I do not think it goes too far to say that this was something that the Chinese lifted when the South Koreans——

Senator MERKLEY. Have we seen China enact similar patterns of retaliation against companies that are engaged in things it does not like? Or is this kind of a new test?

Dr. RAVICH. No. We see pattern—I see Eric shaking his head yes—after pattern. There was an example in Vietnam not too long ago, actually after the Hague decision for the Philippines and against China. It appears that China wanted to send a specific message to Vietnam. Don't you get any ideas in those territorial waters. And there were certain trade actions taken against Vietnam.

Senator MERKLEY. I wanted to turn to North Korea because here in the United States, we have the NSA full of some of the brightest computer minds to be found certainly throughout our country and probably beyond. And I think about so here is North Korea that does not have a lot of contact with the outside world. What is our assessment on how they developed such enormous capability? Are they benefiting from cyber expertise being shared from the Chinese? Or have they simply made this such a priority for their country that they are harvesting every great mathematical computer code mind to go to work on this project?

Dr. RAVICH. So the answer is certainly the latter, but how they effect that—they have made this a clear priority. They know that this is one of their greatest asymmetric strengths to be able to go after the economy in South Korea.

But the North Korean scientists do travel the world. They do go to conferences. They do have access to journals and online resources. They are not growing up in a bubble, so to speak. They are learning from potentially other hostile state and non-state actors.

Senator MERKLEY. Here is a question then. So we have seen North Korea with the WannaCry ransomware attack, the Sony attack, the DarkSeoul attack, the Bangladesh account, attempted $1 billion heist. And I am sure there is a much longer list than that. So why is North Korea not concerned about extensive retaliation? And is it because in part that their own economy is not computerized in a way that makes it very vulnerable to such retaliation?

Dr. RAVICH. I think they have learned a valuable lesson over the last 20 years, that they can get away with a lot without facing any punishment that they feel the pain. Even with the sanctions regime they keep getting layered and layered over them, they continue with their nuclear missile programs. The elite still get to live like elites. The burden falls on the average person. So they continue to do what they want to do when they want to do it, and they have not had enough of a persuasion to change their pathway.

Senator MERKLEY. So in conventional warfare, one thing that deters folks is if I attack them, they will attack back. So my time is running out, so I will just ask you two pieces of this question.

Should we send a message that we are going to respond ferociously if we are attacked in a cyber manner, if attacked by North Korea again?

And second of all, should we take sanctions against their computer scientists traveling the world and attending conferences, if you will, a privilege that you have noted that they still enjoy?

Dr. RAVICH. Taking the second part first, absolutely. It gets to understanding who is in the command and control apparatus of North Korea's cyber and who is operationalizing it. And absolutely that should be clearly on the docket.

On the first, we do need and will need to respond more forcefully but we better ensure that our castle walls are strong enough, and that is of great concern.

Senator MERKLEY. Which they are not even close.

Thank you.

Senator GARDNER. Senator Kaine?

Senator KAINE. Thank you, Mr. Chair.

And thanks to the witnesses.

Mr. Rosenbach, in your written testimony, you quote from a Department of Defense document, a cyber strategy document, dated 2015. And the quote is about deterrence, and it says it works by "convincing a potential adversary that it will suffer unacceptable costs if it conducts an attack on the United States and by decreasing the likelihood of a potential adversary's attack will succeed."

Reporting today suggests that as part of the growing facts that are available about the Russian cyber attack on the election, that 39 State boards of elections were hacked in some way by the Russians. So clearly we did not convince a potential adversary that it will suffer unacceptable consequences.

Have you delved into why we did not? I think the testimony is that President Obama in September told Vladimir Putin to, quote, knock it off, and then there was even a use of the red phone right before the election to reach out and say, hey, we know what you are doing. Why was more not done and why was more not done publicly to discuss the fact of this Russian incursion into our elections?

Mr. ROSENBACH. Senator, that is a really hard question for me because I was so involved in all of the deliberations about that. And so I would just say this that I personally believe that we should have done much more, that we should have done much more sooner to send a signal that this is not something that would be acceptable to the United States, recognizing that an attack on our democracy in the way that it happened is probably the most serious attack on a vital U.S. national interest. It is hard for me to imagine that we should not have been more muscular in our response.

But I will have to tell you at the time that this was going on, there were different ideas about what the outcomes might be and that sometimes influences foreign policy decisions as well.

Senator KAINE. And regardless of the outcomes, an attack is an attack, and the integrity of the system is something we should protect one way or other. Correct?

Mr. ROSENBACH. Yes, sir. I think the thing I am most concerned about now is even after the fact, we still have not responded to the Russians in a way that the rest of the world sees that you cannot get away with doing this to the United States. So I am concerned now that in the next election—the North Koreans—they definitely watch that. So do the Iranians.

Senator KAINE. Would you not think the rest of the world would also potentially draw the message, wow, if the U.S. would not act vigorously to defend itself, what is the likelihood that they would defend us against an attack?

Mr. ROSENBACH. Yes, sir. Absolutely. I think that is a great point. And this is not a political thing. I know there is a lot of stuff going on associated with issues political right now. But we, as a country, need to raise above the political fear about it and do something about cyber and information attacks against the democracy, or otherwise in the years to come, it is just going to get worse.

Senator KAINE. I mean, I will just say kind of to my surprise in the aftermath of the election, I was amazed how much of it was known by folks with the administration and how little was done. Calculations, as you say. I know a lot more after November 8, but I was amazed how much of that was known long before November 8 with little action.

And I contrast it—and I am not sure it is a completely fair comparison but with the French experience. So when they were aware that there was a Russian effort to suck data and emails away from candidates, they made that very public. And then when there started to be the dumping of such data, they also made that very public. They made a very different calculation than we did. And that may be the ability to take advantage of learning. And a Sony attack is early, then involvement in a Brexit vote, and then involvement in the U.S. election. And by now there is an opportunity, wow, this is really happening. We better talk about it. But they really made a different calculation as a nation, not any particular party. As a nation, they made the calculation Russia is doing this. We are going to call them out on it on the actual attack and taking of data and emails, and then as soon as they start to dump them, we are also going to call them out on it, which led voters to at least maybe have a little sense of skepticism about what they might hear. That is not the only way to respond to an attack, but being transparent to the public about what is going on, that would seem to be in accord with our own values as well. Would you not agree?

Mr. ROSENBACH. I really strongly agree, Senator. I think the way the French handled it was very sophisticated. They did have the huge advantage of seeing that it was probably coming because of things that the Russians had done. However, they were not afraid to go out there. And then they also did things that were kind of creative with information ops themselves. Those are things that we should learn from and that we should watch out for with our allies. Again, the point here is we need to think about this domain in a more creative way and realize that it has grave consequences for the country if we are not going to be tough and think about it in a sophisticated way like other foreign policy issues.

Senator KAINE. And, Mr. Chair, if I could just say one thing. It is not really a question. But I really appreciated that aspect of Dr. Ravich's testimony because it kind of challenged my own thinking. I am on the Armed Services Committee too and in Foreign Relations. Virtually everything we talk about, military operation, we talk about our allies, what are we going to do together with our allies. But often when we have cyber discussions, we have cyber discussions, you know, just what should the U.S. do, and we do not talk about it so much with respect to allies other than intelligence sharing. But in terms of what we might do together with allies, we talk about that in other realms of defense, not in cyber defense. And your notion of cyber co-ops and why are we not doing more with the UK and Israel kind of reminds us, oh, yes, if this is a domain of warfare, we should be thinking about alliances just as we do whether we are talking about training exercises, European Reassurance Initiative, and others. And I really appreciated that aspect of your testimony.

Thank you, Mr. Chair.

Senator GARDNER. Please go ahead.

Senator MARKEY. Mr. Vice President—Senator, do not believe the fake news. [Laughter.]

Senator MARKEY. I think the warning that you are giving us just by sitting here is something that we have to heed, and the consequences can be historic if you ignore the lessons of this last election and what happened in these other places. Such things can turn the whole arc of history. So thank you for being here. Thank you for your leadership on the issue.

Senator GARDNER. Thank you, Senator Kaine.

And if you do not mind, we will just go back and forth with continued conversation, if that is all right with you if you do not have anything else going on right now.

We started this conversation off—I think there are a lot of things that we could follow up on. You know, South Korea and China. I think it is unacceptable. What China has done to South Korea is basically a schoolyard bully when it comes to retaliating against South Korea's decision that they would make for its self-protection and the placement of THAAD. That is an alliance decision. Obviously, we continue to work to strengthen that alliance with South Korea and the United States. But that was an important decision that we have to make sure remains part of that alliance framework.

By the way, China has cost South Korea in South Korean estimates $7 billion in economic damage as a result of their retaliation over South Korea's self-defense efforts.

Going back to the question that we talked about, who is in charge, the cyber coordinator at the State Department, the Defense Department offices, the White House offices—you know, China has a cyber administration. President Xi placed himself on the cyber committee, this super cyber committee. Other countries may be doing other things. Is there a different construct that we should be looking at? Do we need a cyber administration? I do not want to create bureaucracy for the sake of creating a bureaucracy. Do we need an envoy, ambassador-level position at the State Department? How do we get to the point where we have somebody that is the identifiable lead when it comes to a whole-of-government cyber policy?

Dr. RAVICH. Well, one thing that you might want to consider—harkening back to the Eisenhower administration and their Solarium Project with how do we actually prevail in a battlespace that is going to last into the future and looking at the hard choices of containment, of deterrence, you know, the big muscle movements of a government, how do we do targeting, and who is part of it. These were taken on very specifically and focused.

So right now, in answer to your question, I do not think there is any place in the U.S. Government that could undertake a Solarium Project, drawing in the right people to be able to do it. Whether that first sits on the outside, and the knowledge gained from that exercise is then imported onto a functioning process on the inside, or whether those things happen simultaneously needs to be kind of parsed out. But it is needed and it is needed immediately.

Senator GARDNER. Mr. Rosenbach?

Mr. ROSENBACH. You know, I honestly think that we are at the point now where most of the known answers are there and available, and the biggest problem is implementation and finding people to get stuff done, particularly in the government. So I like the idea that there could be a very senior person in the White House driving this in the interagency, interacting with the private sector, doing some things internationally, but it would have to be someone who has gravitas, has clout, and also who has the backing of the President.

Senator GARDNER. Can a coordinator do this, or does it need to be a cabinet-level official?

Mr. ROSENBACH. I would say the coordinator, as has it has been in this iteration—Rob Joyce is a great guy, very smart, very capable, but he does not have the stature and the backing probably to really move things, I think similar to Michael Daniels. It is not a political thing. I think it needs to be something that it is a more senior-level position, and it cannot be within one of the departments I do not think.

Senator GARDNER. President Xi, of course, came to Washington last year, and the Obama administration and President Xi came to some kind of an agreement as it relates to China's cyber efforts against the United States. This is an outgrowth of the OPM breach. Is China living up to its end of the bargain from the conversations it had here in Washington last year?

Dr. RAVICH. It seems that there was a dip at first, but the anecdotes that are coming in because—Eric and I were talking about this—the lack of a comprehensive database on cyber incidents against our private sector is not there. It looks like business as usual, meaning the wholesale theft of IP on the private sector side. I will let others talk about the infiltration on the government side of the house. There is a little bit of we do not know what we do not know, but again, anecdotally, it looks like they are back to business.

Senator GARDNER. Mr. Rosenbach?

Mr. ROSENBACH. I hate to sound cynical but Chris Painter and I were the two representatives to go and negotiate with the Chinese on issues like this back in the day. And they would tell us every single time that we met with them that they were not doing economic espionage, that it was not the Chinese. There was no way to know that. So I do not want to sound cynical, but I believe they are now just better at doing what they were doing before and they found new ways and that their leadership told them don't you dare get caught again.

Senator GARDNER. So a quick question for the two of you. And you may not feel like you can answer this question. I do not know. But I had a meeting with the CEO of a major tech company in the United States, and he brought up five points: multi-factor authentication, strong encryption of data, micro-segmentation, consistent and automatic patches and upgrades, and consistent education and testing of the workforce. Pretty simple and basic hygiene points. And his point was that these five things, had they been implemented, would have prevented the OPM breach, would have prevented the Sony breach, would have prevented the ransomware spread.

Do you feel comfortable in answering that question? Is that true? Is that something as simple as requiring vendors to do this kind of thing? Would that solve a significant portion of this threat?

Dr. RAVICH. I think it solves a portion of it, but I think what the answer to you completely misses is that state adversaries, very, very aggressive, very technologically sophisticated state adversaries, are looking to hollow out portions of our economy. And while the five steps will go very nicely to locking doors, maybe getting a guard dog if the state actor wants to get in there, it is not going to suffice. And the action has to be taken against the state actor themselves to push back on them.

Senator GARDNER. Mr. Rosenbach, just a last question and then I will turn it over to Senator Markey.

Do we have a nuclear deterrent in cyber?

Mr. ROSENBACH. We do, of course. So just like in any other domain, if there were a cyber attack against the United States that resulted in death or significant destruction, the nuclear option would be on the table.

Senator GARDNER. I do not mean an actual use of a nuclear bomb. I mean is there a sort of theoretical digital version of a nuclear deterrent within the cyber realm should somebody do something so bad to the United States that we can send something back as a so-called cyber umbrella. And I think Dr. Ravich has written about this.

Mr. ROSENBACH. I do not think from everything I have done that I have ever seen the cyber nuke, so to speak. And the issue is it takes a lot of preparatory work to get everything in place to be able to take something down. But it would be great if there were such a thing, and you would have to use it in conjunction with other military options I believe.

Dr. RAVICH. No, but these are the kind of policy options that we definitely do need to develop, along with a very clear declaratory policy. Where are we in terms of if a country takes an action or allows for an action to be taken from their domain? Right? It kind of harkens back to the declaratory policy that was created after 9/11. You sponsor terrorism, you actually do it, or you allow others to use your territory to do it. I do not think that either we or our adversaries understand our declaratory policy. I think we need to work on that. I think we need to have one. And again, it goes to not just the adversary themselves but if they are sponsoring proxies, we see it the same way as if they did it themselves to us.

Senator GARDNER. Thank you and I apologize.

Senator Markey?

Senator MARKEY. I think it is very important.

Like Stuxnet, we probably have some capacity which has been developed that we could paradox the Russians' or any other country's electrical grid system if they really wanted us to have to prove to them that we could reciprocate. Do you not think, Dr. Ravich?

Dr. RAVICH. Could we? Would we?

Senator MARKEY. What Senator Gardner was asking is if we get attacked, can we attack back. You knock down our electricity system. Can we knock down their electricity system?

Dr. RAVICH. I assume, but do not know, that we have those capabilities.

Senator MARKEY. Thank you.

Do you agree with that, Mr. Rosenbach?

Mr. ROSENBACH. I think this is a really important question. So the worst case would be that someone thought the United States was an emperor that had no clothes when it came to cyber capability. And so when I was overseeing cyber things at the Department of Defense, I was very worried that we did not have enough capability and often would talk bigger than what the capability warranted. So I think it is a really important question that you are all are asking to push the country to have that type of real capability that you could use quickly and is not wrapped in all kinds of bureaucracy.

Senator MARKEY. So in the spy versus spy world that we live, the fact that the National Security Agency lost control of powerful cyber weapons to the group known as Shadow Brokers raises questions about our own government, about our own NSA. Who do you think Shadow Brokers are?

Mr. ROSENBACH. You know, Senator, I have read a lot of intelligence on this topic, so I just cannot talk about that.

Senator MARKEY. How about you, Dr. Ravich?

Dr. RAVICH. Kind of the same. I am not comfortable talking about the——

Senator MARKEY. So we probably need a discussion about that. If there is some group out there that can crack into the NSA and steal our cyber weapons and then we cannot talk about who they are, it is hard to have a public policy response in terms of what our paradox of them would be, you know, what we would be trying to create as public policy. So that is a conundrum for us.

Mr. ROSENBACH. There is one thing that is important I was not able to say orally but is in my statement is that if we are going to build these type of cyber weapons, it is very, very important that we take care of them. So I was an Army officer. When you are in the Army, if you have an accidental discharge even with a single round, there is accountability for that. The company commander will be relieved. I am not sure we have that same kind of accountability right now.

Senator MARKEY. So you are saying that these are powerful cyber weapons, and they were not properly protected by the NSA. That is what you are saying. You used the metaphor for your gun.

Mr. ROSENBACH. I will use a metaphor because I cannot comment specifically——

Senator MARKEY. I understand.

Mr. ROSENBACH. There are ongoing legal things, but I think you all understand.

Senator MARKEY. Yes.

So if the United States is going to develop capabilities that allow our military and intelligence community to penetrate widely-used commercial software like Microsoft Windows, then we need to be far more vigilant to ensure that these tools are not stolen, much like we take steps, as you said, to make sure that other weapons arsenals are safe from theft and misuse, and we have to do the same for these tools. In fact, I do not think it overstates the severity of the risk we face to suggest that it is time for the intelligence community to develop features akin to the permissive action links that ensure that our nuclear weapons cannot be used except when authorized by the President. Do you agree with that, Mr. Rosenbach?

Mr. ROSENBACH. I think that is a very interesting idea and something that is technically completely possible. And I only wonder why we have not done it already.

Senator MARKEY. Dr. Ravich, do you agree with that?

Dr. RAVICH. I do agree with it with the proviso that—there is a disconnect that has developed between the operators and senior policymakers in the last administration and this administration in terms of the operators not being able to fully, adequately, comprehensively explain what they need to do and the ramifications of it, leaving the policymakers to say do not do anything. There is a dangerous kind of gap in understanding that has arisen I believe leading us to not take actions when we could for fear from the senior leadership that it will have unintended consequences which many times it will not.

Senator MARKEY. So do you have any other ideas for us in terms of tools that the NSA and other law enforcement agencies should adopt in order to ensure that tools such as those used in WannaCry are not stolen and misused by bad actors? Any other suggestions?

Mr. ROSENBACH. Senator, this is less specific to the U.S. Government and us taking care of our cyber arsenal, so to speak. In particular, because you are the Foreign Relations Committee, there is an analogy to the proliferation security initiative where if you were to work on a bilateral basis on building the capacity of nations to stop the proliferation of destructive malware, I think that is something that can make a difference. There is a little bit of deterrence aspect in that as well because a lot of countries buy those type of capabilities on the black market with bitcoin or straight out cash. It is sometimes hard to develop. If we were able to do something about that, I think it can make a difference.

Senator MARKEY. Thank you, Mr. Chairman.

Senator GARDNER. Senator Kaine?

Senator KAINE. I will come back to Dr. Ravich on allies and cyber co-ops. I think that is a fascinating part of your testimony. And you are with the Foundation of Defense of Democracies, and one of the analogous challenges we are grappling with on the Armed Services—I am kind of interested in putting it into this context—is the battle against ISIS.

So in the summer of 2014, ISIS had its biggest advance of real estate. And the U.S. and the coalition effort to defeat ISIS on the battlefield has been pretty successful, squeezing them down, painful, slow, but they are losing. And they know it and we know it, and they know that we know it. But ISIS now has decided, okay, if we are losing space on the battlefield, then what we probably should do is focus more on one-off attacks, whether it is an airliner in the Sinai, a mausoleum in Tehran, Manchester, London, San Bernardino. They are going to try to inspire attacks.

You do not beat those attacks with a battalion. You beat those attacks with intelligence sharing. So kind of again, this is a kind of warfare where the quality of your alliances and the quality of the information that you share is probably the most important thing to defeat the attacks.

So now I am putting myself into the cyber realm. It may be that, as we think about cyber defense, the quality of these alliances will end up being very critically important to whether we can defend our own democracies, protect our own internal democracy.

How should we gauge the—it is one thing to judge the capacity of another nation to be a battlefield, you know, fighting force alongside with us, choose them to be a partner because we trust their on-the-ground combat capacity. How about gauging allies in the cyber realm for working cooperatively? The one that I am thinking about is under P.M. Modi, they have shed a little bit of the Congress' party nonalignment philosophy and they do more military training exercises with the United States than any other nation. And it is also a nation with a strong technological capacity. Just to use them as an example, analyzing India as a potential—this is the region we are talking about analyzing India as a potential ally in a cyber co-op arrangement as you describe in your testimony.

Dr. RAVICH. It is very interesting. How we are thinking about it is so the easiest hurdle to cooperate is probably on the R&D agenda because sharing of intelligence gets a little bit tricky, and different countries have different trust levels. So the idea was, well, let us walk into this in a way that we can actually good news, not a talk shop, but actually create something. We all have comparative advantages. When I started out looking at the United States, the Israelis, the UK, we have different comparative advantages technologically to go forward on that.

But then as you start to kind of broaden out, other countries, while they may not be technological super stars, have particular windows into a certain threat. Ukraine has a window into a threat. They can understand a certain actor. There are other countries in the world that are also good friends or partners or allies with us on other things that have a window into a threat. Do they share the similar goals with us? So in terms of where India places, I think high and evolving on the technology, certainly a window into a threat from where they are, and certain shared goals going ahead.

Senator KAINE. And I guess another area of shared interest you might want to look at is if they are facing a problem similar to us. So there might be a threat like a country, but there also could be is there a particular sector where you are facing challenges and we are facing challenges in the same sector. And that might suggest not cooperation on all of cyber defense, but at least let us strengthen our utility sector or our financial sector—those that are at risk—so that for purposes of R&D or other things, we could focus on a sector and make each of our nations stronger. So that would be probably another area that we should look at.

Dr. RAVICH. I agree.

Senator KAINE. Thank you. That is very helpful.

Senator GARDNER. Thank you. And, Senator Kaine, thanks to referring to India. I had hoped to use this committee to adversely possess India as jurisdiction for the Indo-Pacific——

Senator KAINE. I am on the committee that oversees India. I am always grasping. [Laughter.]

Senator GARDNER. Thank you.

Senator Markey?

Senator MARKEY. Thank you, Mr. Chairman.

I want to follow up on Senator Kaine because following the WannaCry attack, Microsoft's President, Brad Smith, called the attack a wakeup call for the world's governments, and Smith called for a digital Geneva Convention in which governments would agree not to retain vulnerabilities for cyber weapons development and would, instead, reveal those vulnerabilities to software developers to protect consumers against attack. In essence, Smith was calling for a kind of cyber arms control comparable to the arms control regimes we have developed in the nuclear weapons domain.

Of course, the analogy only goes so far. Nuclear weapons are physical objects. Cyber weapons are digital objects which can be hidden far more effectively. Cyber arms control would face far greater difficulties when it comes to verification and enforcement, but that does not mean that governments have no interest in cooperating. For example, if a country's hospitals are vulnerable to cyber attacks, that could impact global health. If a country's airports are vulnerable, that could impact travelers from beyond its borders. And if a country's stock market can be manipulated, that could affect the global financial system.

Can you both discuss your thoughts on global cooperation intended to improve cybersecurity? What are the limits of cyber arms control? And are there remaining opportunities for international cooperation that we have not fully explored?

Dr. RAVICH. I have reservations about a push towards broader cyber norms and these large-scale elements that you are discussing that they can rapidly turn into a lot of wonderful language with lofty goals but crumble because of two things: one, because too many people are in it with too many different visions of what they want to do and capabilities to actually do them; and the second being that somebody opens the door to hostile adversaries being part of the discussion.

So I kind of fall back on some of the earlier discussions. Let us start with a small group of likeminded countries that can actually put real technology to starting to solve some of these problems and have the wherewithal and the will to take actions when needed, show great results in that front and then slowly open up to who else do we want to protect under our cyber umbrella.

Senator MARKEY. Thank you.

Senator GARDNER. Thanks, Senator.

Mr. ROSENBACH. You remember how President Reagan said trust but verify when he was talking about arms control? I think that trust part with the Russians right now in particular would be very difficult when it comes to cyber arms control.

So I think it is an interesting idea. Personally I think we should go for more practical projects, for example, like trying to stop proliferation working together and doing that with the private sector as well. Down the road, I think it is an interesting idea but I am not sure, in particular from the Department of Defense perspective, where I used to sit, that that is something we would be that supportive of.

Senator MARKEY. Thank you, Mr. Rosenbach. And I appreciate this Russia-U.S. tension. It is not quite Broncos-Patriots, but I appreciate your living in Cambridge in the era of Tom Brady in football. So thank you both for your testimony.

Senator GARDNER. Yes. And thank you both for being here.

And I think one of the things the Senate should look at soon is the PATCH Act. It is legislation that would address some of the efforts and vulnerabilities that we have seen. If the U.S. Government knows of a patch and it is not a national security issue, then we ought to be making sure that that patch is available and out there. So there are a number of ways that we can work to make sure that we address some of these issues. I think it is interesting questions that we have to continue to build upon, understanding how our global alliances work when it comes to issues of cyber, understanding who is in charge, and understanding that perhaps Russia and China are not going to—will not hold the same kind of interest that we do as it relates to these issues. And so how do we move forward with common interests around the globe to develop the kinds of norms that we need to and not wait to convince people who we may not be able to convince.

So I want to thank all of you, thanks to both of you for your testimony today. Very interesting and actionable. Thanks to all the Senators who attended today's hearing. And the witnesses, again thank you.

For the information of the members, the record will remain open until the close of business on Thursday, including for members to submit questions for the record.

This is your homework assignment. I would just ask kindly that the dog not eat your homework, and you return the homework as quickly as possible. I ask the witnesses to respond as promptly as possible, and your responses will be made a part of the record.

And again, with the thanks of the committee, the hearing is now adjourned.

[Whereupon, at 4:00 p.m., the hearing was adjourned.]

Prepared Statement of Samantha F. Ravich, Ph.D.

CONGRESSIONAL TESTIMONY: FOUNDATION FOR DEFENSE OF DEMOCRACIES

Senate Foreign Relations Committee
Subcommittee on East Asia, the Pacific, and International Cybersecurity

State-Sponsored Cyberspace Threats:

Recent Incidents and U.S. Policy Response

SAMANTHA F. RAVICH, PH.D.

Senior Advisor
Foundation for Defense of Democracies

Board of Advisors
Center on Sanctions and Illicit Finance,
Foundation for Defense of Democracies

Former Deputy National Security Advisor
Vice President Dick Cheney

Former Co-Chair
National Commission for the Review of
Research and Development Programs in the
United States Intelligence Community

Washington, DC
June 13, 2017

FDD
FOUNDATION FOR
DEFENSE OF DEMOCRACIES

www.defenddemocracy.org

Chairman Gardner, Ranking Member Markey, distinguished members of the subcommittee, thank you for inviting me to participate in this important hearing on state-sponsored cyber threats. My testimony today focuses on an area that I believe is woefully underappreciated yet cannot be more important for our country. And that is the use of cyber means by adversarial states to purposefully undermine our economy in order to weaken us military and politically.

Both traditional economic warfare and, more recently, cyber warfare have been extensively studied. What is much less understood, however, is the *intersection* between these two subjects: The contemporary evolution of economic warfare within the new realities of cyberspace has not received the focused, comprehensive scrutiny and policy attention that it warrants. The questions we must be asking and answering are: Within the escalating cyber attacks on U.S. public and private organizations, is there lurking a new type of action – some form of *concerted adversarial strategy* – to undermine the U.S. economically? Are some adversaries' strategies designed to cause economic harm that would weaken or significantly debilitate U.S. security capabilities? To what extent, and when, are they sponsoring proxies to achieve these nefarious goals? Is the U.S. prepared to identify and address such hostile strategies effectively? Does the U.S. government need new collection and analysis platforms to perform this critical function?

It is my contention that the threats are real, the warfare is ongoing, and that the U.S. government is **inadequately structured to properly and comprehensively** detect, evaluate, and address cyber-enabled economic threats. The U.S. government has made great strides in organizing itself to protect and defend the .gov and .mil realms.[1] But our nation's greatest vulnerability may lie with adversarial attacks on the U.S. private sector. And in this regard, the private sector believes it is on its own, a position that is untenable when the adversary is a state actor such as China or North Korea.

Background of the Evolving Battlespace

As we think through our ability as a nation to protect ourselves and our allies, and advance our core interests overseas, the greatest strength we have is our economy. It is our free market, with its ability to efficiently move capital, protect intellectual property, distribute goods, and provide the running room for new ideas and technology to flourish, that creates the most powerful and fearsome military the world has ever known. It is the confidence of the American people that our $18.5-trillion GDP will continue to thrive that provides our leaders the confidence to fund our defense budget. And it is not just the defense industrial base but the broader national security industrial base that underpins it all. Specifically, it is not just the big defense contractors and the big telecommunication companies but everything from the technology startups; to the banks and investment houses that supply capital; to the cars, trucks, trains, and planes that move men and materiel; to the pharmaceuticals and food supplies that care and feed those who protect the free world. Moreover, an April report from the Defense Science Board Task Force on the Cyber Supply Chain warned that the Pentagon can be crippled through maliciously inserted

[1] Vicki Michetti, "DoD's Defense Industrial Base Cybersecurity (DIB CS) Program," *U.S. Department of Defense*, August 24, 2016. (https://www.fbcinc.com/e/cybertexas/presentations/Room_302_Wed_1-145PM_Vicki_Michetti_DIB_101_Cyber_Texas_Aug15.pdf)

vulnerabilities into the weapons and goods that power the U.S. military through entry points in private sector companies.[2]

It is true that the business of America is business. And the business of America is at risk of being hollowed out from the inside by everything from theft of intellectual property to the malicious infection of the supply chain to the degradation of confidence in our commerce, banking, and transportation sectors. The papers are filled with articles about cyber attacks against the private sector to gain profit. No doubt, this is a serious and growing problem. British insurance company Lloyds estimated that cyber attacks cost global businesses as much as $400 billion per year.[3] The internet and its related networked systems provide overwhelming advantages that help an economy to learn, share, and grow, but as we increase our reliance on the electronic movement of data, money, goods, and services, we also increase our vulnerability.[4]

What the $400 billion amount, large as it seems, ignores is the corrosive effect cyber attacks against the private sector can have on a country's military readiness or political sovereignty. The theft of defense-related intellectual property and the corruption of the defense supply chain has been widely reported, and the possible damage these hostile actions could inflict upon our weapons systems has raised alarms throughout the Pentagon and on Capitol Hill.[5] The more pernicious, and less recognized, effect is the degrading of the entrepreneurial motivation that occurs with the systematic and wholesale theft of intellectual property from its creators and owners. As a result of sustained cyber attacks, startups may not get financing because their IP is stolen and established companies may be forced to shut down for days because of malware incidents, projects may get cancelled, and people may get laid off. And it is the small- and medium-sized enterprises – the very companies where the most innovative work is being done that eventually finds its way into our military – that are often hit hardest by cyber attacks.[6] A 2012 U.S. Patent and Trademark Office report aptly summed it up this way: "Every job in some way produces, supplies, consumes, or relies on innovation, creativity, and commercial distinctiveness. Protecting our ideas and intellectual property (IP) promotes innovative, open, and competitive markets."[7] With estimates of the annual costs of trade secret theft in the U.S. ranging from $180 billion to $540 billion, the long-tailed drag on the economy must be recognized for the crisis it is, with a disproportionate burden falling on the very startups and

[2] U.S. Department of Defense, Defense Science Board, "Cyber Supply Chain," April 2017. (http://www.acq.osd.mil/dsb/reports/2010s/DSBCyberSupplyChain_ExecSummary_Distribution_A.PDF)

[3] Stephen Gandel, "Lloyd's CEO: Cyber attacks cost companies $400 billion every year," *Fortune*, January 23, 2015. (http://fortune.com/2015/01/23/cyber-attack-insurance-lloyds/)

[4] Steve Morgan, "IBM's CEO On Hackers: 'Cyber Crime Is The Greatest Threat To Every Company In The World,'" *Forbes*, November 24, 2015. (https://www.forbes.com/sites/stevemorgan/2015/11/24/ibms-ceo-on-hackers-cyber-crime-is-the-greatest-threat-to-every-company-in-the-world/#1db8a3473f07)

[5] Ellen Nakashima, "Confidential report lists U.S. weapons system designs compromised by Chinese cyberspies," *The Washington Post*, May 27, 2013. (https://www.washingtonpost.com/world/national-security/confidential-report-lists-us-weapons-system-designs-compromised-by-chinese-cyberspies/2013/05/27/a42c3e1c-c2dd-11e2-8c3b-0b5e9247e8ca_story.html?utm_term=.afe441d46dc3)

[6] According to the 2012 Verizon Breach report, 71 percent of companies with less than 100 employees have suffered a cyber attack. "2012 Data Breach Investigations Report," *Verizon*, 2012, page 11. (http://www.verizonenterprise.com/resources/reports/rp_data-breach-investigations-report-2012_en_xg.pdf)

[7] "Economics and Statistics Administration and U.S. Patent and Trademark Office, "Intellectual Property and the U.S. Economy: Industries in Focus," March 2012. (https://www.uspto.gov/sites/default/files/news/publications/IP_Report_March_2012.pdf)

innovation leaders that the U.S. and other developed nations credit with building the future economy, enhancing military readiness, and safeguarding sovereignty.[8] As the U.S. government better develops systems to cooperate with and defend the private sector, protecting these types of startups and innovative companies should be a priority given the disproportionate role they play in determining future national power.

The very well-researched IP Commission Report from the National Bureau of Asian Research discusses at length the follow-on effects from IP theft, including advantaging our adversaries both in the market and on the battlefield as well as chilling the innovative spirit that creates the technological breakthroughs upon which our economy and military rely.[9] Therefore, it is not the pure cyber criminal that should keep this committee up at night. Rather, it is the hostile state actor who recognizes that while it may not be able to compete directly with America's strength of arms, it holds a significant asymmetric advantage in attacking our economic wherewithal and, by so doing, weaken us militarily or politically.

We call this purposeful strategy Cyber-Enabled Economic Warfare (CEEW).

Cyber-enabled economic warfare is distinct from cyber crime and cyber terrorism – although both may be part of a larger CEEW campaign. What distinguishes CEEW attacks from other types of cyber attacks is the motivation and strategy. A CEEW campaign is driven by strategic intent to degrade the military and political capabilities of an adversary. States can now use cyber means as just one more part of their economic warfare toolbox.

Economic warfare goes back as far as the Bible and was used throughout history in the form of blockades, trade embargoes, blacklists, sanctions, tariff and/or quota discrimination, sabotage of economic targets, preclusive purchase of scarce critical resources, and expropriation. During World War II, Britain created the Ministry of Economic Warfare "to so disorganize the enemy's economy as to prevent him from carrying on the war."[10] In more recent times, economic warfare has also encompassed the freezing of capital assets, counterfeiting, suspending foreign aid, and restricting foreign investment and capital flows. Over the last few decades, the U.S. has relied heavily on economic sanctions (a form of economic warfare) to curtail the illicit, illegal, and dangerous actions and behaviors of rogue countries such as Saddam Hussein's Iraq, the Islamic Republic of Iran, and, of course, the Kim family's DPRK.

[8] "Update to the IP Commission Report: the Theft of American Intellectual Property: Reassessments of the Challenge and United States Policy," *National Bureau of Asian Research* on behalf of the *Commission on the Theft of American Intellectual Property*, 2017. (http://www.ipcommission.org/report/IP_Commission_Report_Update_2017.pdf); "Economic Impact of Trade Secret Theft: A Framework for Companies to Safeguard Trade Secrets and Mitigate Potential Threats," *Center for Responsible Enterprise and Trade* and *PricewaterhouseCoopers*, 2014. (https://create.org/resource/economic-impact-oftrade-secret-theft)

[9] "Update to the IP Commission Report: the Theft of American Intellectual Property: Reassessments of the Challenge and United States Policy," *National Bureau of Asian Research* on behalf of the *Commission on the Theft of American Intellectual Property*, 2017. (http://www.ipcommission.org/report/IP_Commission_Report_Update_2017.pdf)

[10] W.N. Medlicott, *The Economic Blockade (Volume I)*, (London: His Majesty's Stationery Office, 1952). (https://archive.org/stream/economicblockade012328mbp/economicblockade012328mbp_djvu.txt)

But in the past quarter century, there has emerged a vitally important new potential form of economic warfare. The advent of the Information Age and its accompanying "virtual" world of cyberspace has produced the potential for the use of cyber-enabled attack methods to cause an adversary economic harm that is far disproportionate to the size, resources, or efforts of the attacker.

To rise to the level of Cyber-Enabled Economic Warfare, the attack must:

- Be cyber-enabled.
- Cause, or be intended to cause, economic harm.
- Be significant enough to potentially degrade national security capabilities.
- Be motivated by the strategic intent to erode national security capabilities.[11]

Cyber-enabled economic warfare (CEEW)

Refers to a hostile strategy involving attack(s) against a nation using cyber technology with the intent to weaken its economy and thereby reduce its political and military power.

An attack, or collection of attacks, constitutes CEEW if it meets the following four requirements:

It must be cyber-enabled.

It must cause, or be intended to cause, economic harm.

The economic damage must be significant enough to potentially degrade national security capabilities.

The attack(s) must be motivated by the strategic intent to erode national security capabilities.

State Adversaries

Ten years ago this past April, the small country of Estonia suffered a Russia-supported cyber invasion.[12] The ostensible cause of the invasion was the anger of ethnic Russians and their

[11] For a more fulsome discussion of what constitutes a cyber-enabled economic warfare attack, see Samantha F. Ravich and Annie Fixler, "Framework and Terminology for Understanding Cyber-Enabled Economic Warfare," *Foundation for Defense of Democracies*, February 22, 2017. (http://www.defenddemocracy.org/content/uploads/documents/MEMO_CyberDefinitions_07.pdf)

[12] Emily Tamkin, "10 Years After the Landmark Attack on Estonia, Is the World Better Prepared for Cyber Threats?" *Foreign Policy*, April 27, 2017 (http://foreignpolicy.com/2017/04/27/10-years-after-the-landmark-attack-on-estonia-is-the-world-better-prepared-for-cyber-threats/); Joshua Davis, "Hackers Take Down The Most Wired Country In Europe," *Wired*, August 21, 2007. (https://www.wired.com/2007/08/ff-estonia/); Christian Lowe,

Moscow backers over the relocation of a World War II memorial in the Estonian capital. The larger setting was that Vladimir Putin deeply resented Estonia's accession to NATO and decided to inflict great harm on that country's economy and public sector by cyber means. The first round began on April 26, 2007 when the initial attacks brought down the Estonian government's websites. The prime minister's office as well as the offices of the minister of defense, political parties, and the parliament were all crippled by distributed denial of service (DDoS) attacks. The attack undermined the ability of the government to communicate with the people. The next round of attacks brought down press outlets covering the crisis, making it harder to inform both the Estonian citizenry and the outside world about what was happening. Waves and waves of denial of service and malware attacks on all aspects of Estonian life, culture, civil society occurred over the next two weeks.

What made this cyber attack even more alarming was that, on May 9, the financial system was figuratively brought to its knees. Hansabank, Estonia's largest bank, experienced a sustained attack and had to cease operations, cutting off nearly all Estonians from accessing their capital. ATMs would not dispense money. People panicked. The citizenry lost faith in its banking sector. Apparently having gotten their message across that they could attack where and when they chose and then recede into the darkness, the aggressors stopped the attacks on May 19 as quickly as they had begun.

It is important to recognize the likely effect of similar actions if taken against the United States, where nearly 50 percent of Americans live paycheck to paycheck. If those Americans could not access their ATMs or get their paycheck in time, a hundred million of our citizens would quickly have no money to buy food for their families, diapers for their babies, or their much-needed medicine.

Estonia suffered a large-scale but relatively unsophisticated Russian cyber attack. While most Russian cyber attacks seem aimed at political institutions and more direct military targets, it is not a stretch to envision Russia retaliating for any new sanctions against it by going after our own economic wherewithal. It was only five years ago, we should recall, when an Iranian cyber attack brought down the state-owned Saudi Arabian oil company Aramco's network, destroying 35,000 computers and putting 10 percent of the world's oil at risk. In one day, Aramco bought 50,000 new hard drives – a cost that would have bankrupted most companies.[13]

While it is important to understand the strategies of all U.S. adversaries and competitors, two of the most active players in the field of cyber-enabled economic warfare are the Chinese and North Koreans. Often the discussion focuses on how China steals trade secrets to advantage its own industries and Pyongyang steals money because North Korea has no real economy. While these motivations may explain part of what is occurring, it appears that both of these actors may have a much broader strategy in play.

"Kremlin loyalist says launched Estonia cyber-attack," *Reuters*, March 13, 2009. (http://www.reuters.com/article/us-russia-estonia-cyberspace-idUSTRE52B4D820090313)

[13] Nicole Perlroth, "In Cyberattack on Saudi Firm, U.S. Sees Iran Firing Back," *The New York Times*, October 23, 2012. (http://www.nytimes.com/2012/10/24/business/global/cyberattack-on-saudi-oil-firm-disquiets-us.html?_r=0); Jose Pagliery, "The inside story of the biggest hack in history," *CNN*, August 5, 2015. (http://money.cnn.com/2015/08/05/technology/aramco-hack/)

China: Beginning as early as the 1970s, China has been engaged in a massive, prolonged campaign of intellectual property theft against U.S. firms.[14] Over time, China has increasingly been conducting this campaign via cyber-enabled technologies, targeting nearly every sector of the U.S. economy. While the exact amount such theft has cost U.S. companies in dollars and American citizens in jobs is unknown, it has been estimated to be as high as hundreds of billions of dollars and more than two million jobs.[15] In the aggregate, the effects on the U.S. private sector include, according to the IP Commission: "Lost sales; lost brand value; reduced scope of operations; lost jobs and reduced ability to provide employee benefits; reduced ability to conduct R&D; increased IP protection expenses for prevention, remediation, and enforcement; increased costs from dealing with malware acquired from unlicensed software; [and] reduced incentive to innovate."[16]

China's IP theft campaign constitutes a large, if not the largest, part of what appears to be Beijing's overall cyber-enabled economic warfare strategy against the U.S. and the West more generally. Illustrative of this intention are the words by PLA Colonels Qiao Liang and Wang Xiangsui in their book *Unrestricted Warfare*, where they describe CEEW as "a form of non-military warfare which is just as terribly destructive as a bloody war, but in which no blood is actually shed."[17]

However, Washington and its allies have been slow to comprehend the threat, primarily because they view each attack individually as a separate incident instead of collectively as elements in an overall coordinated campaign. For example, in May 2014, the Department of Justice charged five Chinese hackers who targeted American companies in the nuclear power, metals, and solar industries with only computer crimes and espionage.[18] Similarly, accusations against China for theft of U.S. Steel's proprietary information claim only that Beijing is focused on market share,[19] without understanding how this fits into the larger collective pattern.

[14] Christopher Cox, "Report of the Select Committee on U.S. National Security and Military/Commercial Concerns with the People's Republic of China," *U.S. House of Representatives*, May 1999. (https://www.congress.gov/105/crpt/hrpt851/CRPT-105hrpt851.pdf)

[15] Lesley Stahl, "The Great Brain Robbery," *CBS News*, January 17, 2016. (http://www.cbsnews.com/news/60-minutes-great-brain-robbery-china-cyber-espionage/); "The IP Commission Report: The Report of the Commission on the Theft of American Intellectual Property," *The National Bureau of Asian Research* on behalf of the *Commission on the Theft of American Intellectual Property*, 2013. (http://www.ipcommission.org/report/ip_commission_report_052213.pdf)

[16] "The IP Commission Report: The Report of the Commission on the Theft of American Intellectual Property," *The National Bureau of Asian Research* on behalf of the *Commission on the Theft of American Intellectual Property*, 2013, page 29. (http://www.ipcommission.org/report/ip_commission_report_052213.pdf)

[17] Qiao Liang and Wang Xiangsui, *Unrestricted Warfare*, Trans. Foreign Broadcast Information Service (Beijing, China: PLA Literature and Arts Publishing House, February 1999), page 51. (http://www.terrorism.com/documents/unrestricted.pdf)

[18] U.S. Department of Justice, Press Release, "U.S. Charges Five Chinese Military Hackers for Cyber Espionage Against U.S. Corporations and a Labor Organization for Commercial Advantage," May 19, 2014. (https://www.justice.gov/opa/pr/us-charges-five-chinese-military-hackers-cyber-espionage-against-us-corporations-and-labor)

[19] John W. Miller, "U.S. Steel Accuses China of Hacking," *The Wall Street Journal*, April 28, 2016. (http://www.wsj.com/articles/u-s-steel-accuses-china-of-hacking-1461859201)

Of late, Beijing has flexed its cyber-enabled economic powers of coercion and intimidation more overtly. In July 2016, loudspeakers and screens of Vietnam Airlines in that country's two largest airports were hacked, and flight and safety information was overridden by offensive messages about Vietnam's claims to the South China Sea. Although there is some debate regarding the ultimate culprit, the cyber attack did come on the heels of the Hague's Permanent Court of Arbitration's ruling against China and in favor of the Philippines in their territorial dispute. The Vietnam Security Information Association said that the attacks were "deliberate" and "well-planned" and appeared to be part of an escalating pattern by China that took a more formal shape in the immediate aftermath of China's placement of an oil rig in Vietnam's exclusive economic zone.[20] The particular attack did little damage aside from inconveniencing passengers who had to wait for the analog system to kick in, but if replicated and expanded, it could shake the trust in the airline and transportation system of that country. Already, Vietnamese companies are worried about the toll Chinese cyber-enabled economic warfare will take on their own businesses. A 2014 survey found that "20 percent of respondent firms expressed concerns that the East Sea/South China Sea tensions could threaten their information security."[21]

South Korean firms have also begun to feel China's cyber-enabled economic wrath. When Beijing was informed that the United States was accelerating the deployment of its Terminal High Altitude Area Defense (THAAD) system to South Korea as a response to North Korea's latest missile tests, the PRC immediately began to bring pressure on South Korean private firms operating in China. Lotte, a South Korean conglomerate that sold its government a golf course to be used for THAAD, felt the pain almost immediately. Chinese authorities shuttered nearly two-dozen Lotte stores on the mainland,[22] using the flimsy excuse that the government only just discovered that the stores did not comply with existing fire regulations.[23] Additionally, the website for the Lotte Group was brought down by a denial-of-service (DDoS) attack originating from Chinese internet addresses,[24] and a number of Chinese e-commerce sites halted sales of Lotte goods. Estimates of lost business and damage are in the hundreds of thousands of dollars.[25] Although the damage is a small dollar figure compared to Lotte's total income from 150 chemical plants, supermarkets, and other facilities operating in China, the move has prompted deep concern in Seoul. South Korea exported over $120 billion to China last year, about a quarter of the country's total exports, and is particularly vulnerable to Chinese coercion.

[20] Helen Clark, "The Alleged Chinese Hacking at Vietnam's Airports Shows That the South China Sea Battle Isn't Just in the Water," *The Huffington Post*, accessed June 7, 2017. (http://www.huffingtonpost.com/helen-clark1/china-hack-vietnam-south-china-sea_b_11357330.html)

[21] "Vietnam vulnerable to cyber attacks but agencies poorly equipped," *Than Nien News* (Vietnam), December 10, 2014. (http://www.thanhniennews.com/tech/vietnam-vulnerable-to-cyber-attacks-but-agencies-poorly-equipped-34980.html)

[22] Javier Hernandez, Owen Guo, and Ryan McMorrow, "South Korean Stores Feel China's Wrath as U.S. Missile System Is Deployed," *The New York Times*, March 9, 2017. (https://www.nytimes.com/2017/03/09/world/asia/china-lotte-thaad-south-korea.html?_r=2)

[23] Jethro Mullen and Sol Han, "One company is bearing the brunt of China's anger over U.S. missile system," *CNN*, March 7, 2017. (http://money.cnn.com/2017/03/07/news/china-lotte-thaad-south-korea-tensions/)

[24] Joyce Lee and Heekyong Yang, "South Korea's Lotte Duty Free says website crashed after attack from Chinese IPs," *Reuters*, March 2, 2017. (http://www.reuters.com/article/us-lotte-china-idUSKBN1690HR)

[25] Shin Ji-hye, "Cyberattacks open new front in Korea, China THAAD spat," *The Korea Herald* (South Korea), March 9, 2017. (http://www.koreaherald.com/view.php?ud=20170309000792)

In one of his first issues taken up upon entering office, the new South Korean president, Moon Jae-in, sent an emissary to meet with Chinese President Xi. In the aftermath of the meeting, Lotte's website was unblocked. Days later, President Moon suspended the deployment of THAAD.[26]

***North Korea*:** As early as 2009, North Korea was already initiating malicious cyber attacks on its adversaries. That summer there was a wave of destructive denial of service attacks perpetrated against "websites of the Departments of Homeland Security, Treasury, Transportation, the Secret Service, the FTC, the New York Stock Exchange, and NASDAQ, as well as dozens of South Korean banks, affecting at least 60,000, and possibly as many as 160,000 computers."[27]

In March 2013, North Korean hackers attacked South Korean banks and media companies using malware dubbed "DarkSeoul," destroying tens of thousands of computers, deleting data from hard drives and overwriting Master Book Records, and rendering many banking services inoperable.[28] North Korea's intentions in the March 2013 attacks were not purely economic or commercial – that is, Pyongyang was not interested in advantaging its own media companies and financial institutions within the South Korean market by taking out their competitors. Rather, North Korea attacked South Korea's economic resources in order to threaten its economy and affect Seoul's national security decision-making. North Korea engaged in a systematic operation, which continues today, to disrupt elements of the South Korean economy in order to sap the strength of the country – financially and militarily. Indeed, South Korean police cyber investigators stated in 2016 that North Korea had operationalized a long-term plan involving the seeding of malicious code in more than 140,000 computers at over 160 South Korean firms and government agencies.[29] The police concluded that the DPRK likely "aimed to cause confusion on a national scale by launching a simultaneous attack after securing many targets of cyber terror, or intended to continuously steal industrial and military secrets."

More recently, it was reported that North Korean hackers most likely initiated the WannaCry ransomware attack that spread to hundreds of thousands of computers worldwide.[30] The monetary haul from the scheme was minimal, leading some analysts to question if the effort was a test for a larger attack. Similar assessments have been made about the 2016 cyber bank heist

[26] Paul Mcleary, "In Nod to China, South Korea Halts Deployment of THAAD Missile Defense," *Foreign Policy*, June 7, 2017. (http://foreignpolicy.com/2017/06/07/in-nod-to-china-south-korea-halts-deployment-of-thaad-missile-defense/)

[27] Fred Kaplan, *Dark Territory: The Secret History of Cyber War* (New York: Simon & Schuster, 2016), page 213.

[28] Choe Sang-Hun, "Computer Networks in South Korea Are Paralyzed in Cyberattacks," *The New York Times*, March 20, 2013. (http://www.nytimes.com/2013/03/21/world/asia/south-korea-computer-network-crashes.html); K.J. Kwon, "Smoking Gun: South Korea uncovers northern rival's hacking codes," *CNN*, April 22, 2015. (http://www.cnn.com/2015/04/22/asia/koreas-cyber-hacking/); "Four Years of DarkSeoul Cyberattacks Against South Korea Continue on Anniversary of Korean War," Semantec Security Response, June 26, 2013. (https://www.symantec.com/connect/blogs/four-years-darkseoul-cyberattacks-against-south-korea-continue-anniversary-korean-war)

[29] Jack Kim, "North Korea mounts long-running hack of South Korea computers, says Seoul," *Reuters*, June 13, 2016. (http://www.reuters.com/article/us-northkorea-southkorea-cyber-idUSKCN0YZ0BE)

[30] Choe Sang-hun, paul Mozur, Nicole Perlroth, and David Sanger, "Focus Turns to North Korea Sleeper Cells as Possible Culprits in Cyberattack," *The New York Times*, May 16, 2017. (https://www.nytimes.com/2017/05/16/world/asia/north-korea-cyber-sleeper-cells-ransomware.html?smid=tw-nytimes&smtyp=cur&_r=2)

that attempted to withdraw $1 billion from Bangladesh's account at the New York Federal Reserve. Assessments now tie this attack back to the North Korean cyber group Lazarus. While some in the U.S. government have remarked that, if true, it appears that the North Koreans are now robbing banks, it is more chilling to consider that, if true, the North Koreans are now targeting our banking sector.[31]

With a GDP per capita of barely $1,000 and its single largest source of foreign currency coming from sales of coal to China, North Korea has an obvious need to rob foreign banks. But Kim Jong Un is not simply a Korean Willie Sutton. In a military confrontation with the U.S. and South Korea, Kim would look to any capability that could help even out the overwhelming military advantage of the allies. Attacking our economies, which he has already proven he can and will do, may be the quickest way to gain battlefield advantage since it could potentially cause panic in our markets and on our streets.

Policy Recommendations: Without a concerted effort, the United States economy will become increasingly vulnerable to hostile adversaries seeking to undermine our military and political strength. The U.S. government, both the Congress and the executive branch, need to immediately undertake a number of actions to prevail in this new battlespace, including:

- **Understanding the Adversary:** There should be sustained attention within the U.S. intelligence community to understanding the capabilities and intentions of adversarial leadership to engage in cyber-enabled economic warfare. This effort should focus both on staying one step ahead of what cyber tools the enemy is creating and fielding (by using U.S intelligence collection platforms to target adversarial science and technology), but also on mapping the command-and-control hierarchy of the enemy's leadership which directs such campaigns, recognizing any internal frictions or vulnerabilities that can be exploited. It is critical to know as much as possible about the man *behind* the man *behind* the computer – because decisions are made by decision-makers, not bots and bits. At least not yet. In the same vein that the U.S. intelligence community studied Soviet leadership through Kremlinology, so too is it time to map the organizational leadership charts for CEEW within the most dangerous enemy states.

- **International Cyber Co-op:** The U.S. cannot go it alone in its endeavor to safeguard the networks and systems upon which our economy depends. We must take steps to formalize the cyber partnerships that already exist with the other free-market democracies that are leaders in cyber science and technology. Such a "co-op" should begin with the U.S., the UK, and Israel, building on the fact that the UK and Israel are world leaders in cyber and already have cyber attachés stationed in Washington. There is growing evidence that the "bad guys" (China, Russia, Iran, and North Korea) cooperate,[32] and the

[31] Jim Finkle, "Cyber security firm: more evidence North Korea linked to Bangladesh heist," *Reuters*, April 3, 2017. (http://www.reuters.com/article/us-cyber-heist-bangladesh-northkorea-idUSKBN1752I4)

[32] Alex Grigsby, "The Next Level For Russia-China Cyberspace Cooperation?" *Council on Foreign Relations*, August 20, 2015. (https://www.cfr.org/blog/next-level-russia-china-cyberspace-cooperation); Riley Waggaman, "Iran and Russia announce plans for cyber security cooperation," *Press TV* (Iran), March 14, 2017. (http://www.presstv.ir/Detail/2017/03/14/514354/Iran-Russia-cyber-security-cooperation); Yeganeh Torbati and Roger Atwood, "Iran, North Korea agree to cooperate in science, technology," *Reuters*, September 1, 2012. (http://www.reuters.com/article/us-korea-north-iran-idUSBRE88005H20120901)

"good guys" must also build better cooperation not only at the declaratory level, but on the strategic and tactical level.

- **Cyber R&D:** While the private sector plays a key role in the creation of new technologies for the ultimate securing of the systems and networks upon which our economic livelihood rests, government R&D is needed to supply certain types of research which the private sector is not likely to advance. As then-Federal Reserve Chair Ben Bernanke commented, the "argument [for government funding of R&D] which applies particularly strongly to basic or fundamental research, is that the full economic value of a scientific advance is unlikely to accrue to its discoverer, especially if the new knowledge can be replicated or disseminated at low cost. For example, James Watson and Francis Crick received a minute fraction of the economic benefits that have flowed from their discovery of the structure of DNA. If many people are able to exploit, or otherwise benefit from, research done by others, then the total or social return to research may be higher on average than the private return to those who bear the costs and risks of innovation. As a result, market forces will lead to underinvestment in R&D from society's perspective, providing a rationale for government intervention."[33] Initial candidates for government CEEW R&D could include everything from protections for legacy supervisory control and data acquisition systems (SCADA) to assessing if and how a new internet protocol needs to be built. Optimally, the "cyber co-op" discussed above could be established with its first task being to create a cyber R&D agenda, with partner countries leveraging their comparative advantage in certain fields while not duplicating the work likely to be produced in the private sector.

- **Understanding the Scale, Scope, and Evolution of the Threat:** As we better understand the strategies of our adversaries and build better cooperation with our allies, we must also understand the evolution of the threats. An open-source database, searchable by tags such as targeted industry and type of attack, should be funded and made available to the government, researchers, and the private sector. While both the Cyber Threat Intelligence Integration Center, housed in the Office of Director of National Intelligence, and the National Cybersecurity and Communications Integration Center (NCCIC) of the Department of Homeland Security exist in some form or fashion to increase the sharing of cyber security-related information within federal and, in the case of NCCIC, non-federal entities, neither funds a comprehensive database of cyber attacks and incidents across the private sector. Consequently, most of U.S. policy and operations are built on anecdotal observations from single cases, which are then used to speculate about attack patterns and potential. We are virtually blind to the context and setting of cyber conflict unless we have a macro-level data source that provides this key information.[34] Such a database could shed much needed light on the scale, scope, and evolution of the threat against our economic foundation as well as serve as a way to gauge whether actions taken against the adversary are succeeding in deterring malicious behavior.

[33] Federal Reserve Chairman Ben Bernanke, "Promoting Research and Development: The Government's Role," *Speech at the Conference on "New Building Blocks for Jobs and Economic Growth,"* May 16, 2011. (https://www.federalreserve.gov/newsevents/speech/bernanke20110516a.htm)

[34] From a research proposal submitted to the author by Brandon Valeriano and Christopher Whyte.

- **Creating a Whole of Government CEEW OODA Loop.** Using the platforms above, the U.S. government should create a whole of government OODA (observe, orient, decide, and act) loop so that it can properly assess the enemy's escalatory ladder and better recognize if our defensive and offensive actions are actually minimizing and deterring hostile activity. Without such an informed assessment, we run the risk of being too timid to use our capabilities against the enemy on the one hand or potentially exacerbating a fraught situation on the other. In practice, this would mean more coordination across the government on everything from the tasking of the collection of the relevant CEEW intelligence to a better understanding of how the threat is evolving to the sharing of hard data on what is being attacked to the analysis of theories and practice for deterring and responding to the enemy.

While the analogies to the dawn of the nuclear age can be overdrawn when laid over the challenges we now face in cyber-enabled economic warfare, today's legislators, decisionmakers, and operators can learn a lot from the rigorous thought that went into assessing the types of intelligence collection platforms, targeting processes, and analytic methods created to deal with that challenge. In this new threat environment, we are akin to the late 1940s or early 1950s in how to organize ourselves as a government. We have much work to do.

Thank you for the opportunity to testify. I look forward to your questions.