Stenographic Transcript
Before the

COMMITTEE ON
ARMED SERVICES

UNITED STATES SENATE

HEARING TO RECEIVE TESTIMONY ON UNITED STATES CYBERSECURITY POLICY AND THREATS

Tuesday, September 29, 2015

Washington, D.C.

ALDERSON REPORTING COMPANY
1155 CONNECTICUT AVENUE, N.W.
SUITE 200
WASHINGTON, D.C. 20036
(202) 289-2260

HEARING TO RECEIVE TESTIMONY ON

UNITED STATES CYBERSECURITY POLICY AND THREATS

Tuesday, September 29, 2015

U.S. Senate

Committee on Armed Services

Washington, D.C.

The committee met, pursuant to notice, at 9:30 a.m. in Room SD-G50, Dirksen Senate Office Building, Hon. John McCain, chairman of the committee, presiding.

Committee Members Present: Senators McCain [presiding], Inhofe, Sessions, Wicker, Ayotte, Fischer, Cotton, Rounds, Ernst, Tillis, Sullivan, Lee, Reed, Nelson, McCaskill, Manchin, Gillibrand, Donnelly, Hirono, Kaine, King, and Heinrich.

OPENING STATEMENT OF HON. JOHN McCAIN, U.S. SENATOR FROM ARIZONA

Chairman McCain: Good morning. The committee meets today to receive testimony from Deputy Security of Defense Robert Work, Director of National Intelligence James Clapper, and Admiral Mike Rogers, the Commander of U.S. Cyber Command, Director of the National Security Agency, and Chief of the Central Security Service. We thank each of the witnesses for their service and for appearing before the committee.

We meet at a critical time for the defense of our Nation from cyberattacks. In just the past year, we all know the United States has been attacked by cyberspace -- in cyberspace by Iran, North Korea, China, and Russia. Indeed, since our last cyber hearing in March, the attacks have only increased, crippling or severely disrupting networks across the government and private sector, and compromising sensitive national security information.

Recent attacks against the Joint Chiefs of Staff, the Pentagon, and the Office of Personnel Management are just the latest examples of the growing boldness of our adversaries in their desire to push the limits of acceptable behavior in cyberspace. New intrusions, breaches, and hacks are occurring daily. The trends are getting worse. But, it seems the administration has still not mounted an adequate

response. They say they will, quote, "respond at the time and manner of our choosing," unquote, but then either take no action or pursue largely symbolic responses that have zero impact on our adversaries' behavior.

Not surprisingly, the attacks continue, our adversaries steal, delete, and manipulate our data at will, gaining a competitive economic edge and improving their military capability. They demonstrate their own means to attack our critical infrastructure. And they do all of this at a time and manner of their choosing. More and more, they are even leaving behind what Admiral Rogers recently referred to as, quote, "cyber fingerprints," showing that they feel confident that they can attack us with impunity and without significant consequences.

Just consider the recent case with China. After much hand-wringing, it appears the President will not impose sanctions in response to China's efforts to steal intellectual property, pillage the designs of our critical weapon systems, and wage economic espionage against U.S. companies. Instead, last week's state visit for the President of China simply amounted to more vague commitments not to conduct or knowingly support cyber-enabled theft of intellectual property.

What's worse, the White House has chosen to reward China with diplomatic discussions about establishing norms

of behavior that are favorable to both China and Russia. Any internationally agreed-upon rules of the road in cyberspace must explicitly recognize the right of self-defense, as contained in Article 51 of the U.N. Charter, along with meaningful human rights and intellectual property rights protections. The administration should not concede this point to autocratic regimes that seek to distort core principles of the international order, to our detriment.

Make no mistake, we are not winning the fight in cyberspace. Our adversaries view our response to malicious cyberactivity as timid and ineffectual. Put simply, the problem is a lack of deterrence. As Admiral Rogers has previously testified, the administration has not demonstrated to our adversaries that the consequences of continued cyberattacks against us outweigh the benefit. Until this happens, the attacks will continue, and our national security interests will suffer.

Establishing cyberdeterrence requires a strategy to defend, deter, and aggressively respond to the challenges to our national security in cyberspace. That is exactly what the Congress required in the Fiscal Year 2014 National Defense Authorization Act. That strategy is now over a year late, and counting. And, while the Department of Defense's 2015 cyberstrategy is a big improvement over previous such efforts, it still does not integrate the ends, ways, and

means to deter attacks in cyberspace.

Establishing of cyberdeterrence also requires robust capabilities, both offensive and defensive, that can pose a credible threat to our adversaries, a goal on which the Congress, and specifically this committee, remains actively engaged.

The good news here is that significant progress has been made over the past few years in developing our cyberforce. That force will conclude -- will include a mix of professionals trained to defend the Nation against cyberattacks, to support the geographic combatant commands in meeting their objectives, and to defend DOD networks. This is good. But, the vast majority of our DOD resources have gone toward shoring up our cyberdefenses. Far more needs to be done to develop the necessary capabilities to deter attacks, fight, and win in cyberspace. Policy indecision should not become an impediment to capability development.

We do not develop weapons because we want to use them. We develop them so as we do not have to. And yet, in the cyberdomain, as Admiral Rogers testified in March, quote, "We're at a tipping point." He said, quote, "We've got to broaden our capabilities to provide policymakers and operational commanders with a broader range of options." We must invest more in the offensive capabilities that our

cybermission teams need to win on the cyber battlefield. The fiscal year 2016 NDAA seeks to address this challenge in a number of ways, including a pilot program to provide the Commander of Cyber Command with limited rapid acquisition authorities.

Finally, we know the Defense Department is in the process of assessing whether the existing combatant command structure adequately addresses the mission of cyberwarfare, and whether to elevate Cyber Command to a unified command. There are worthwhile arguments on both sides of this debate. I look forward to hearing Admiral Rogers' views on this question and his assessment of how an elevation of Cyber Command might enhance our overall cyberdefense posture.

I also look forward to hearing from our witnesses what, if any, progress has been made on addressing disagreements within the interagency on the delegation and exercise of authority to use cyber capabilities.

I thank the witnesses again for appearing before the committee. I look forward to their testimony.

Senator Reed.

STATEMENT OF HON. JACK REED, U.S. SENATOR FROM RHODE ISLAND

Senator Reed: Thank you very much, Mr. Chairman. And let me commend you for scheduling this very important hearing. It's an appropriate to discuss a number of important cyber issues with our witnesses, especially in light of the cyber agreements announced last Friday between President Obama and the President of China.

I want to thank Director Clapper, Deputy Security Work, and Cyber Command Commander Admiral Rogers for their testimony today and for their service to the Nation. Thank you, gentlemen, very much.

Let me start with a series of cyber agreements with China. The apparent commitment by China to cease stealing U.S. intellectual property for their economic gain is notable. And I expect we will have a robust discussion about China's compliance and our course of action if it does not. China's leaders must be aware that its reputation and standing in the eyes of the American people will continue to decline if this piracy does not stop, which ultimately will have a tremendously negative impact on our relations with China.

I would also emphasize potential importance of China embracing a set of international norms in cyberspace developed by the United Nations which includes a commitment

to refrain from attacks on other nations' critical infrastructure.

Next, I would highlight that we are facing the recurring issue of whether or when to elevate Cyber Command from a sub-unified command to a full unified command, and whether to sustain the current dual-hat arrangement under which the Commander of Cyber Command also serves as the Director of NSA. I understand that the Department may be nearing a recommendation to the President that the next unified command plan elevate Cyber Command to a unified command.

The committee, in the past, has questioned whether Cyber Command is mature enough to warrant elevation to a unified command, and whether the dual-hat arrangement should continue when a decision is made to elevate the Command. Put simply, if Cyber Command is so reliant on NSA that common leadership is still necessary, is the Command ready to stand on its own as a unified combatant command? This is an issue that Senator McCain has drawn attention to, and it's something that I think is very critical, going forward, for this committee.

Directly related to that question of the maturity of Cyber Command is the status of the military cyber mission units that the Department only began fielding over the last 2 years. Commendably, the Department is meeting its

schedule for standing up these units with trained personnel; but, by its own admission, the equipment, tools, and capabilities of these forces will remain limited. Indeed, the committee's proposed FY16 National Defense Authorization Act includes a mandate that the Secretary of Defense designate executive agents from among the services to build a so-called "unified platform," persistent training environment, and command-and-control systems that are necessary for these forces to operate effectively. It will take a number of years to build these -- capability.

We are behind in developing these military capabilities for our cyber forces because the Defense Department was persuaded that the systems and capabilities that NSA already has would be adequate and appropriate for use by Cyber Command. This is an important example of an assumed critical dependency on NSA and an assumed commonality between intelligence operations and military operations in cyberspace that, in some cases, has turned out to be inaccurate.

For a number of years, this committee has been urging the executive branch to work diligently to identify all practical methods to deter malicious actions in cyberspace and to articulate a strategy for implementing them. Some believe that retaliation in kind in cyberspace is a necessary and effective component of such a strategy. I

look forward to hearing the views of our witnesses on this matter.

As my colleagues and our witnesses are well aware, the Senate went into recess for the August break having reached an agreement for bringing the cyber information-sharing bill to the floor for debate. I know the Chairman is in full agreement on the need to debate, amend, and pass that legislation this year in the interest of national security, and so am I.

We must also recognize the Defense Department and intelligence community are not operating alone to protect America's cyber infrastructure, most notably rely on the Department of Homeland Security for protection of America's critical infrastructure. The use of overseas contingency operations funding to avoid the Budget Control Act caps in defense does nothing to help the DHS or other nondefense partners avoid the effects of sequestration. This is yet another argument for why we need a comprehensive solution to the problem of sequestration.

Finally, I think it is important that we hear from our witnesses on the subject of encryption. Post-Snowden, U.S. technology companies fearful of losing business at home and abroad are encrypting communications and offering encryption services for which even the companies themselves have no technical capability to unlock. FBI Director Comey has

given multiple speeches warning the law enforcement agencies and intelligence agencies that they will be going dark, with serious consequences for public safety and national security.

These and other questions, gentlemen, are vitally important. And I look forward to your testimony.

Chairman McCain: I thank the witnesses.

Director Clapper, I've tried to impress on members of this committee to show deference to old age, and so we'd like to begin with you.

STATEMENT OF HON. JAMES R. CLAPPER, DIRECTOR OF NATIONAL INTELLIGENCE

Director Clapper: Chairman McCain, Ranking Member Reed, members of the committee, when I testified on the intelligence community's worldwide threat assessment at the end of February, cyberthreats again led our annual threat report for the third year in a row. We're here today to respond to the several requests in your invitation letter, and I will focus on an overview of cyberthreats, briefly, that face our Nation, and their attendant national security implications. And then Secretary Work, Admiral Rogers will follow, as well.

We will, as you understand, perhaps run into some classified aspects that we won't be able to discuss as fully in this open televised hearing.

I do want to take note of and thank the members of the committee who are engaged on this issue and have spoken to it publicly, as the two of you just have.

So, by way of overview, cyberthreats to the U.S. national and economic security are increasing in frequency, scale, sophistication, and severity of impact. Although we must be prepared for a large, Armageddon-scale strike that would debilitate the entire U.S. infrastructure, that is not, we believe, the most likely scenario. Our primary concern now is low- to moderate-level cyberattacks from a

variety of sources which will continue and probably expand. This imposes increasing costs to our business, to U.S. economic competitiveness, and to national security.

Because of our heavy dependence on the Internet, nearly all information, communication technologies, and IT networks and systems will be perpetually at risk. These weaknesses provide an array of possibilities for nefarious activity by cyberthreat actors, including remote hacking instructions, supply-chain operations to insert compromised hardware or software, malicious actions by insiders, and simple human mistakes by system users.

These cyberthreats come from a range of actors, including nation-states, which fall into two broad categories, those with highly sophisticated cyberprograms, most notably Russia and China, are our peer competitors, and those with lesser technical capabilities, but more nefarious intent, such as Iran and North Korea, who are also more -- but who are also much more aggressive and unpredictable. Then there are non-nation-state entities -- criminals motivated by profit, hackers or extremists motivated by ideology.

Profit-motivated cybercriminals rely on loosely networked online marketplaces, often referred to as the "cyber underground" or "dark web," that provide a forum for the merchandising of illicit tools, services, and

infrastructure and stolen personal information and financial data. The most significant financial cybercriminal threats to U.S. entities and our international partners come from a relatively small subset of actors, facilitators, and criminal forums.

And terrorist groups will continue to experiment with hacking, which could serve as the foundation for developing more advanced capabilities.

Cyber espionage criminal and terrorist entities all undermine data confidentiality. Denial-of-service operations and data-deletion attacks undermine availability. And, in the future, I think we'll see more cyberoperations that will change or manipulate electronic information to compromise its integrity. In other words, compromise its accuracy and reliability instead of deleting it or disrupting access to it.

As illustrated so dramatically with the OPM breaches, counterintelligence risks are inherent when foreign intelligence agencies obtain access to an individual's identity information -- of course, a problem that the Department of Defense has encountered. Foreign intelligence agencies or nonstate entities could target the individual, family members, coworkers, and neighbors, using a variety of physical and electronic methods, for extortion or recruiting purposes.

And speaking of the OPM breaches, let me say a couple of words about attribution. It is not a simple process, involves at least three related but distinct determinations: the geographic point of origin, the identity of the actual perpetrator doing the keystrokes, and the responsibility for directing the act. In the case of OPM, we have differing degrees of confidence in our assessment of the actual responsibility for each of these three elements.

Such malicious cyberactivity will continue and probably accelerate until we establish and demonstrate the capability to deter malicious state-sponsored cyberactivity. And establishing a credible deterrent depends on reaching agreement on norms of cyberbehavior by the international community.

So, in summary, the cyberthreats to U.S. national and economic security have become increasingly diverse, sophisticated, and harmful. There are a variety of Federal entities that work the cyber problem in DHS, FBI, NSA, and other law enforcement, intelligence, and sector-specific agencies, like Treasury and Energy. Every day, each of these centers and entities get better at what they do individually. I believe now we've reached the point where we think it's time to knit together all the intelligence these separate activities need to defend our networks, because, while these entities may be defending different

networks, they are often defending against the same threats. So, that's one reason the President directed me to form a small center to integrate cyberthreat intelligence. And I strongly believe the time's come for the creation of such a center to parallel the centers that we operate for counterterrorism, counterproliferation, and counterintelligence and security.

With that, let me turn to Deputy Security Work.

[The prepared statement of Director Clapper follows:]

STATEMENT OF HON. ROBERT O. WORK, DEPUTY SECRETARY OF DEFENSE

Mr. Work: Chairman McCain, Ranking Member Reed, distinguished members of the committee, thank you very much for inviting us here this morning to talk about the threats of cyber. This committee has led the way in discussing the threats and the response to these threats, and the Department looks forward to working with the committee to get better in this regard.

As DNI Clapper has said, cyberintrusions and attacks by both state and nonstate actors have increased dramatically in recent years, and particularly troubling are the increased frequency and scale of state-sponsored cyberactors breaching U.S. Government and business networks. These adversaries continually adapt and evolve in response to our cyber countermeasures, threatening our networks and systems of the Department of Defense, our Nations' critical infrastructure, and U.S. companies and interests globally.

The recent spate of cyberevents, to include the intrusions into OPM, the attacks on Sony, and the Joint Staff networks by three separate state actors, is not just espionage of convenience, but a threat to our national security. As one of our responses to this growing threat, we released, in 2015, the DOD Cyber Strategy, which will guide the development of our cyberforces and strengthen our

cybersecurity and cyberdeterrence posture. That is its aim.

The Department is pushing hard to achieve the Department's three core missions as defined in the strategy. The first and absolutely most important mission is to defend DOD network systems and information. Secretary Carter has made this the number-one priority in the Department, and we are really getting after it now. Second, to defend the Nation against cyberevents of significant consequence. And third, to provide cybersupport to operational and contingency plans. And, in this regard, the U.S. Cyber Command may be directed to conduct cyberoperations, in coordination with other government agencies, as appropriate, to deter or defeat strategic threats in other domains.

Now, my submitted statement, Mr. Chairman, contains additional detail on how we're moving out to achieve these three strategic goals, but I'd like to highlight the particular focus on deterrence, especially since I know this is key in the minds of most of the members here.

I want to up -- acknowledge, up front, that the Secretary and I recognize that we are not where we need to be in our deterrent posture. We do believe that there are some things the Department is doing that are working, but we need to improve in this area, without question. And that's why we've revised our cyberstrategy.

Deterrence is a function of perception. It works by

convincing any potential adversary that the costs of conducting the attack far outweigh any potential benefits. And therefore, our three main pillars of our cyberdeterrence strategy, in terms of deterrence, are denial, resilience, and cost imposition. Denial means preventing the cyberadversary from achieving the -- his objectives. Resilience is ensuring that our systems will continue to perform their essential military tasks, even when they are contested in the cyber environment. And cost imposition is our ability to make our adversaries pay a much higher price for their malicious activities than they hoped for.

I'd like to briefly discuss these three elements:

To deny the attacker the ability to adversely impact our military missions, we have to better defend our own information networks and data. And we think the investments we have made in these capabilities are starting to bear fruit. But, we recognize that technical upgrades are only part of the solution. Nearly every single one of the successful network exploitations that we have had to deal with can be traced to one or more human errors which allowed entry into our network. So, raising the level of individual cybersecurity awareness and performance is absolutely paramount. Accordingly, we're working to transform our cybersecurity culture, something that we ignored for a long time, by -- the long term, by improving human performance

and accountability in this regard.

As part of this effort, we have just recently published a cybersecurity discipline implementation plan and a scorecard that is brought before the Secretary and me every month. And they are critical to achieving this goal of securing our data and our networks and mitigating risk to DOD missions. This scorecard holds commanders accountable for hardening and protecting their end points and critical systems, and also have them hold accountable their personnel, and directs, as I said, the compliance reporting to the Secretary and me on a monthly basis. The first scorecard was published in August of this year, and it is being added to and improved as we go.

Denial also means defending the Nation against cyberthreats of significant consequence. The President has directed DOD, working in partnership with our other agencies, to be prepared to blunt and stop the most dangerous cyberevents. There may be times where the President and the Secretary of Defense directs DOD and others to conduct a defensive cyberoperation to stop a cyberattack from impacting our national interests, and that means building and maintaining the capabilities to do that -- just that.

This is a challenging mission requiring high-end capabilities and extremely high-trained teams. We're

building our cyber mission force and deepening our partnership with law enforcement and the intelligence community to do that.

The second principle is improving resiliency by reducing the ability of our adversaries to attack us through cyberspace and protecting our ability to execute missions in a degraded cyber environment. Our adversaries' view DOD cyber dependency as a potential wartime vulnerability. Therefore, we view our ability to fight through cyberattacks as a critical mission function. That means normalizing cybersecurity as part of our mission assurance efforts, building redundancy whenever our systems are vulnerable, training constantly to operate in a contested cyber environment. Our adversaries have to see that these cyberattacks will not provide them a significant operational advantage.

And the third aspect of deterrence is having the demonstrated capability to respond, through cyber or noncyber means, to impose costs on a potential adversary. The administration has made clear that we will respond to cyberattacks in a time, manner, and place of our choosing. And the Department has developed cyber options to hold aggressor at risk in cyberspace, if required.

Successfully executing our missions requires a whole-of-government and whole-of-nation approach. And, for that

reason, DOD continues to work with our partners and the other Federal departments and agencies and the private sector and our partners around the world to address the shared challenges we face.

Secretary Carter has placed particular emphasis on partnering with the private sector. The Department doesn't have all of the answers and is working with industry. We think it will be very, very critical.

Finally, our relationship with Congress is absolutely critical. The Secretary and I very much appreciate the support provided to DOD cyberactivities throughout, from the very beginning, and we understand, and we are looking forward to the National Defense Authorization Act to see if there are other improvements that we have -- we can do.

I encourage continued efforts to pass legislation on cybersecurity information-sharing -- we think that is absolutely critical -- data breach notification, and law enforcement provisions related to cybersecurity, which were included in the President's legislative proposal submitted earlier this year.

I know you agree that the American people expects us to defend the country against cyberthreats of significant consequence. The Secretary and I look forward to working with this committee and Congress to ensure we take every step possible to confront the substantial risks we face in

the cyber realm.

Thank you again for inviting us here today and giving the attention that you have always given to this urgent matter.

I'd like to pass it off now to Admiral Rogers, if that's okay, Mr. Chairman.

[The prepared statement of Mr. Work follows:]

STATEMENT OF ADMIRAL MICHAEL S. ROGERS, USN, COMMANDER, U.S. CYBER COMMAND; DIRECTOR, NATIONAL SECURITY AGENCY; CHIEF, CENTRAL SECURITY SERVICES

Admiral Rogers: Chairman McCain, Ranking Member Reed, and distinguished members of the committee, I am honored to appear before you today to discuss U.S. cyber policy and the state of cyberthreats worldwide. I'd like to thank you for convening this forum and for your efforts in this important area.

I'm also honored to be sitting alongside Director Clapper and Deputy Secretary of Defense Work.

It gives me great pride to appear before you data -- today to highlight and commend the accomplishments of the uniformed and civilian personnel of U.S. Cyber Command. I'm both grateful for and humbled by the opportunity I have been given to lead our cyber team in the important work they do in the defense of our Nation and our Department.

We are being challenged as never before to defend our Nation's interests and values in cyberspace against states, groups, and individuals that are using sophisticated capabilities to conduct cybercoercion, cyberaggression, and cyberexploitation. The targets of their efforts extend well beyond government and into privately-owned businesses and personally identifiable information. Our military is in constant contact with agile, learning adversaries in

cyberspace, adversaries that have shown the capacity and the willingness to take action against soft targets in the United States.

There are countries that are integrating cyberoperations into a total strategic concept for advancing their regional ambitions. They use cyberoperations both to influence the perceptions and actions of states around them and to shape what we see as our options for supporting allies and friends in a crisis. We need to deter these activities by showing that they are unacceptable, unprofitable, and risky for the instigators.

U.S. Cyber Command is building capabilities that can contribute to cross-domain deterrence, and thus, make our commitments even more credible. We are hardening our networks and showing an opponent cyberaggression won't be easy. We are creating the mission force, trained and ready like any other maneuver element that is defending DOD networks, supporting joint force commanders, and helping to defend critical infrastructure within our Nation. We are partnering with Federal, foreign, and industry partners, and exercising together regularly to rehearse concepts and responses to destructive cyberattacks against critical infrastructures. We are generating options for commanders and policymakers across all phases of the conflict, and particularly in phase zero, to hold at risk what our

adversaries truly value.

The demand for our cyberforces far outstrip supply, but we continue to rapidly mature, based on real-world experiences and the hard work of the men and women of U.S. Cyber Command and our service cybercomponents, as well as our broader partners.

I'd like to assure the committee that U.S. Cyber Command has made measurable progress. We are achieving significant operational outcomes, and we have a clear path ahead.

With that, thank you again, Mr. Chairman and members of the committee, for convening this forum, inviting all of us to speak. Our progress has been made possible in no small part because of the support from this committee and other stakeholders. Unity of effort within our Department and across the U.S. Government in this mission set is essential. And I appreciate our continued partnership as we build our Nation's cyberdefenses. And I welcome your questions.

[The prepared statement of Admiral Rogers follows:]

Chairman McCain: Well, thank you, Admiral. And thank the witnesses.

Director Clapper, recently former Chairman of the Joint Chiefs Dempsey was asked about various threats to the United States security, and he said that, in a whole range of threats, we have a significant advantage, except in cyber. Do you agree with that assessment?

Director Clapper: It's probably true. We haven't, I guess, exhibited what our potential capability there is, so I think that's one of the implicit reasons why I have highlighted cyberthreats in the last 3 years of my worldwide threat assessments.

Chairman McCain: I thank you. And you have done that, I think, at least great effect before this committee. As a result of the leader -- the Chinese leader in Washington, there was some agreement announced between the United States and China. Do you believe that that will result in a elimination of Chinese cyberattacks?

Director Clapper: Well, hope springs eternal.

Chairman McCain: Yeah.

[Laughter.]

Director Clapper: I think we will have to watch what their behavior is, and it will be incumbent on the intelligence community, I think, to depict -- portray to our policymakers what behavioral changes, if any, result from

this agreement.

Chairman McCain: Are you optimistic?

Director Clapper: No.

Chairman McCain: Thank you.

Admiral Rogers, you recently stated, quote, "There's a perception," there is, quote, "little price to pay for engaging in some pretty aggressive behaviors, and, because of a lack of repercussions, you see actors, nation-states, indeed, willing to do more." And that was what you stated. What is required? What action is required to deter these attacks, since there's little price to pay? What do we have to do to make it a heavy price to pay?

Admiral Rogers: So, I think we have to clearly articular, in broad terms, what is acceptable and unacceptable, norms, if you will, of behavior. I think we have to clearly articulate that, as a nation, we are developing a set of capabilities, we are prepared to use those capabilities if they're required. They're not necessarily our preference. We clearly want to engage in a dialogue with those around us. But, on the other hand, we do have to acknowledge the current situation we find ourselves in. I don't think there's anyone who would agree that it is acceptable and that it is in our best long-term interest as a Nation.

Chairman McCain: Well, I say with respect, I

understand it's not acceptable, but, in other words, what would enact a price? Would it be relations in other areas? Would it be counterattacks? What -- in other words, what actions would be in our range of arsenals to respond?

Admiral Rogers: So, I think it's potentially all of those things. The first comment I would make, I think Sony is a very instructive example. One of the things I always remind people of, we need to think about deterrence much more broadly, not just focus within the cyber arena. I thought the response to Sony, where we, for example, talked about the economic options as a Nation we would exercise, was a good way to remind the world around us that there's a broad set of capabilities and levers that are available to us as a Nation, and that we're prepared to do more than just respond in kind, if you will.

Chairman McCain: One of the -- Director Clapper, one of the things that's been disappointing to the committee is that, in the fiscal year defense authorization bill, as you know, it required the President to develop an integrated policy. The strategy is now a year late. Can you tell us where we are in that process and what you feel is -- what might bring the administration in compliance?

Director Clapper: You're asking me about policy development?

Senator Reed: Yes.

Director Clapper: I think I would defer to Secretary Work on that.

Mr. Work: Well, Mr. Chairman, as we have said over an over, we believe our cyberdeterrence strategy is constantly evolving and getting stronger.

Chairman McCain: I'm talking about a policy, not a strategy, Mr. Secretary. It required a policy, the Fiscal Year '14 National Defense Authorization Act.

Mr. Work: The policy is still in development. We believe we have a good cyberstrategy. The policy has been outlined in broad strokes by the --

Chairman McCain: Not broad enough, I would think. Does it describe what our -- whether we deter or whether we respond or whether we -- in other words, as far as I know and the committee knows, that there has been no specific policy articulated in compliance with the requirement to -- in the Defense Authorization Act. If you believe that it has, I would be very interested in hearing how it has.

Mr. Work: I believe the broad strokes are, we will respond to --

Chairman McCain: I'm not asking broad strokes. Suppose there is an attack -- a cyberattack like the one on OPM. Do we have a policy as to what we do?

Mr. Work: Yes, we do.

Chairman McCain: And what is that?

Mr. Work: The first is to try -- first, we deny and then we would -- we first find out -- we do the forensics --

Chairman McCain: I'm not asking the methodology. I'm asking the policy. Do you respond by counterattacking? Do you respond by trying to enact other measures? What do we do in case of a cyberattack?

Mr. Work: We respond in a time, manner, and place of our choosing.

Chairman McCain: Does that mean that we counterattack?

Mr. Work: That may be one of the options. It's as --

Chairman McCain: That's not a policy, Secretary Work. That is a -- that is an exercise in options. We have not got a policy. And for you to sit there and tell me that you do, "a broad-stroke strategy," frankly, is not in compliance with the law.

Senator Reed.

Senator Reed: Well, thank you very much, Mr. Chairman.

Director Clapper, we are constantly engaged in, euphemistically, information operations with many other nations, and they're involved with information operations, trying to, as you indicated in your testimony, influence the opinion, disguise activities, disrupt, et cetera. What agencies are -- under your purview or outside your purview, are actively engaged in information operations to the United States in the cyberworld?

Director Clapper: Actually, sir, in -- from an intelligence perspective, we would feed that, in that we don't, at last in what I can speak to publicly, engage in that as a part of our normal intelligence activity. So, we feed other arms, support other arms of the government, not only the State Department and those responsible for messaging.

Senator Reed: Right.

Director Clapper: The National Counterterrorism Center has an office that is devoted to, in a countering-violent-extremism context, helping to develop themes or recommending themes based on what we glean from intelligence as -- for potential vulnerabilities and messages that would appear to various groups, to obfuscate the message, disrupt it, or compete with it. But, generally speaking, intelligence, writ large, doesn't actively engage in information operations.

Senator Reed: From your perspective, are these other agencies that you provide information to adequately resourced and staffed so they can use it effectively, or are they getting a lot of good insights and sitting around wondering what they can do --

Director Clapper: If I were king, which I am not, I think I would have a much more robust capability from the standpoint of the resource commitment to countermessaging.

Senator Reed: And that would fall with -- outside the purview of intelligence, more the State Department and some other agencies.

Director Clapper: Correct.

Senator Reed: And I think we're all going to remember the Voice of America, when it was a -- you know, a pretty dominant sort of -- source of information.

Director Clapper: Well, personal opinion only, not company policy, I would, I think perhaps, you know, a USIA on steroids that would address these messages more broadly and more robustly. But, that's strictly personal opinion.

Senator Reed: But, I think, in terms of what you're observing, particularly some of our competitors have a -- extraordinarily robust operation. They don't lack for resources or personnel, and they're constantly engaged in these types of information operations -- enhancing their image, discrediting their opponents, actively engaging local groups in other countries of interest, et cetera -- and we're sort of on the sidelines more.

Director Clapper: I think that's quite right. And our -- in contrast to us, the Russian intelligence services are very active and very aggressively engaged in messaging.

Senator Reed: Thank you.

Admiral Rogers, to this issue of encryption that Director Comey pointed to, I think your thoughts would be

very helpful.

Admiral Rogers: So, the issue that we find ourselves -- this is less for me, on the U.S. Cyber Command side and much more on the NSA side -- is -- communications in the world around us increasingly going to end-to-end encryption, where every aspect of the path is encrypted, and the data and the communication is protected at a level that, with the current state of technology, is difficult to overcome. Clearly, that's in the best interests of the Nation, in broad terms. And strong encryption is important to a strong Internet defense, and a well-defended Internet is in our best interests as a Nation and the world's best interests.

Within that broad framework, though, the challenge we're trying to figure out is -- realizing that that communication path is used by very law-abiding citizens, nation-states, and companies engaged in lawful activity, it is also being used by criminals, terrorists, nation-states who would attempt to generate advantage against the United States and against our allies and partners. And so, we're trying to figure out, How do we balance these two important imperatives of privacy and security? And realizing that it's a technical world around us, and it's changing in a foundational way. And so, we're trying to come to grips, broadly, with, How do we deal with the reality of the technical world around us, and yet the broader legal and

social imperatives we have?

I'm the first to acknowledge we do not have a defined way ahead here. In the end, I think this is about, How do we get the best minds together as a nation to address this? Because, when I look at our capabilities as a nation, there is no problem we can't overcome when we work together in an integrated way to -- in the private sector, industry, business, the academic world. I think that's the way ahead here, in broad terms.

Senator Reed: Thank you very much.

Thank you, Mr. Chairman.

Chairman McCain: Senator Sessions.

Senator Sessions: Thank you, Mr. Chairman.

Senator Inhofe is chairing an EPW Committee. That's why he couldn't be here today.

You've given us a good summary on the threats that we face and the threats that are actually occurring today. And I appreciate that.

Senator McCain asked you about reporting on other policy that Congress has asked you to report on, and that not having been done. Mr. -- Secretary Work, in the 2014 NDAA, the Senate and House agreed on a provision that required the services to report on the cyber vulnerabilities of weapons and communication systems connected by networks. That's something that came out of our Strategic Subcommittee

on a bipartisan basis, and was eventually expanded to include all weapon systems, not just satellites and missiles and national missile defense. We don't have that final report. I believe it's overdue. This budget, I believe, has 200 million in it to help fund this effort. What can you tell us about that?

First, let me say, it may take some time. If it does, that's -- I understand. But, I don't think we've had any report from the DOD to state that -- what progress you've made and how much longer it will take.

Mr. Work: Well, again, on both of the points -- on the policy, we expect that is in the final deliberations. It's an interagency effort. You know, generally, trying to establish norms and deterrence is central to the policy. Again, it's the denial, resilience, and cost-imposition. I'm the first to admit that we are the farthest ahead on the denial and the resilience part. Those are the areas where we are moving faster. The cost-imposition part, because we have elected to retain the retaliatory mechanism of cyberattacks at the national level, just like nuclear weapons, because of the risk of escalation --

Senator Sessions: What about the --

Mr. Work: As far as the -- oh, I'm sorry, sir.

Senator Sessions: -- the other --

Mr. Work: Yes, sir. As far as --

Senator Sessions: -- the vulnerabilities of our weapon systems?

Mr. Work: It is a big, big problem. Most of the -- many of the weapon systems that we have now were not built to withstand a concerted cyberthreat. So, going through every single one of the weapon systems, what Frank Kendall has done is, he's prioritized the weapon systems, and he is working through very carefully. And I expect this work to be done very soon. We now have new requirements in our KPPs, our key performance parameters --

Senator Sessions: So, you have assigned a -- an individual --

Mr. Work: Absolutely.

Senator Sessions: -- to be responsible for this?

Mr. Work: Yes. Frank Kendall is the one who is going through all of the different -- working with, obviously, our CIO, also the Cyber Command, and the -- all of our cyber experts. But, he's responsible for taking a look at the weapon systems and also requiring KPPs, key performance parameters, for new weapon systems so that, when we build them, they will have cyberdefenses built in from the beginning.

Senator Sessions: What about our defense contractors, Admiral Rogers? They maintain and build these systems and have highly sensitive information. Are we satisfied they're

sufficiently protected?

Admiral Rogers: So, we certainly acknowledge there's a vulnerability there. We've been very public about our concerns about foreign nation-states trying to access some of our key operational technology through penetrations in the clear defense contract arena for us. We've made changes to the contractual relationships between us and those companies, where they have to meet minimum cybersecurity requirements, they have to inform us, now, of penetrations. We're clearly not where we need to be, but we continue to make progress.

Senator Sessions: Well, I think it's a bipartisan commitment on Congress to help you with that.

Secretary Work, if it takes more money, let us know. We'll have to evaluate it. And I also understand that some of the protections can be done without much cost; some may require considerable cost. So, we hope that you will complete that.

Admiral Rogers, you, I believe, last week, reported, in the Los Angeles Times, about the threat from China. You note one thing, that they are involved in obtaining U.S. commercial and trade data in a foreign nation, advanced nation, ally of ours. I was told that they -- one of their companies bid on a contract, and that the Chinese had got all the bid data from the Web. And his comment was, "It's

hard to win a bid when your competitor knows what you're bidding."

Admiral Rogers: Yes, it is.

Senator Sessions: Is that kind of thing happening?

Admiral Rogers: It has been. We've very -- been very public of it. I think that's reflected in the agreement that you saw raised during the President of China's visit last week, where we were very explicit about that concern.

Senator Sessions: Well, my time is up, but I would just ask --

You're not allowed -- if you saw an American business being damaged through improper action, you're not allowed to advise them or share any information with them, while our adversaries do assist their businesses. Is that basically correct?

Admiral Rogers: The way this works right now is, I would provide information and insight both in my intelligence hat as the Director of NSA, as well as the Commander of U.S. Cyber Command. If, under that authority, I became aware of activity, I would share the insights with DHS and the FBI, who have a mission associated with interfacing with the private sector in a much more direct way than I do.

Chairman McCain: Senator Manchin.

Senator Manchin: Thank you, Mr. Chairman.

And thank all three of you for your service and for being here today.

Admiral Rogers, if -- I'll start with you. Which country is the most committed, determined, and successful hacker of the U.S.?

Admiral Rogers: Could you say that one more time, Senator?

Senator Manchin: Which country do you believe is the most committed, successful hacker of the U.S.?

Admiral Rogers: If you look at volume, nation-statewide -- nation-state-wides, I would -- China, the PRC, has been the one that we've been the most vocal about. They're not the only one, by any stretch of the imagination.

Senator Manchin: I thought the last time you were here you said that -- I recall you saying that you had more concerns over Russia having more of the ability or the expertise to do us damage.

Admiral Rogers: I thought your question was really focused more on volume. If your -- if the perspective is capability, if you will, then we have been very public about saying I would probably put the Russians --

Senator Manchin: Russians.

Admiral Rogers: -- in a higher capability.

Senator Manchin: But, it seems like that China is more committed and determined to do it.

Admiral Rogers: They certainly do it at a volume level --

Senator Manchin: Gotcha. I understand.

And, Director Clapper, if I may, I know that you just said no -- emphatically no, you don't believe that this agreement that the President of China and our President has made last week will work. With that saying -- what are the -- is there any penalties in this agreement if one or the other violates it? Or is it just basically, well, we have agreed, and let it go at that?

Director Clapper: The terms that I --

Senator Manchin: As you understand it.

Director Clapper: The terms that I have seen, I don't think it treats, specifically, penalties. There certainly are implied penalties. I think the threat of economic sanctions that -- which brought Minister Mung to this country, I think is illustrative of what would mean something to the Chinese if they transgress or violate this agreement.

And I think, as Admiral Rogers was discussing earlier, there -- with respect to sanctions, there certainly whole-of-government possibilities here. Don't have to do, necessarily, a cyber eye for an eye. It can be some other form of retaliation.

But, I don't think -- to answer your question, at least

what I'm aware of -- that there are specific penalties if the agreement is violated.

Senator Manchin: And that's why I think you were pretty quick in saying you don't think it'll work. You said no to that, I think, when the Chairman asked you.

Director Clapper: Well, the reason I said no, of course, is -- the extent to which Chinese purloining of our data, our intellectual property, is pretty pervasive. I think there's a question about the extent to which the government actually orchestrates all of it, or not. So, I think we're in the -- to model -- to borrow a President Reagan term, "trust but verify" mode, at least as far as intelligence is concerned. And we are inherently skeptics.

Mr. Work: Sir, could I add something?

Senator Manchin: If I could -- I have a question for you, Secretary, and then you can go ahead and add to that.

There's a news -- the recent news article that examined similarities between China's J-31 fighter and our F-35 strike finder and what they're been able to do in such a rapid period of time, without any R&D. Do you believe that that gives them a competitive advantage? I mean, you can -- I understand there might be some differences as far as in the software or in the weaponry and this and that, but they're making leaps, which are uncommon, at the behest of us. And we know this, I understand, but we're not taking

any actions against them.

Mr. Work: Well, I'd like to work this in to your --

Senator Manchin: Yes.

Mr. Work: -- and follow up with your --

Senator Manchin: You go ahead.

Mr. Work: -- first question.

At the highest levels, we have made it clear that we believe that Chinese actions in the cybersphere are totally unacceptable as a nation-state. And we made that clear in a wide variety of different ways. And I would characterize the agreement that we have as a confidence-building measure with the Chinese, where we are asking them to prove to us that they are serious about what they say about what they will do to control these efforts.

So, we -- there were really four things that we agreed to do. First, we would give timely responses to information when we say, "Hey, we believe that there is a problem here" -- and we have agreed to exchange information on cybercrimes, we have agreed to possibly collect electronic evidence and to mitigate malicious cyberactivity if it's occurring on our soil. We both agree that we would not knowingly conduct cyber-enabled theft of intellectual property, which, as you say, Senator, has been a problem. We have told them it's a problem, that it's unacceptable. They have said that they will work to curb that. Then we've

agreed to have common effort to promote international norms. And the final thing is, we'll have a high-level joint mechanism, where we can meet at least twice a year and say, "Look, this is just not working. You are not coming through with what you've said."

So, this isn't a treaty or anything like that. It's a confidence-building measure for us to find out if China is going to act responsibly. I agree totally with Director Clapper. They've got to prove to us. And we know that they have stolen information from our defense contractors.

Senator Manchin: Right.

Mr. Work: And it has helped them develop systems. And we have hardened our systems through the Defense Industrial Base Initiative. And we're trying to make --

Senator Manchin: But, I'm saying we know the J-20 is pretty much mirroring our F-22. We know that their J-31 is pretty much mirroring our F-35. When we know this and the cost to the American taxpayers, and let them get -- I mean, why wouldn't we tale hard actions against them? Or why wouldn't we come down -- I just don't understand why we wouldn't retaliate --

Mr. Work: Well --

Senator Manchin: -- from a financial standpoint.

Mr. Work: There are a wide variety of cost-imposition options that we have. They are developed through the

interagency. And again, it's not necessarily kind -- I mean, tit-for-tat. It is proportional response. And we're working through all of those right now.

Senator Manchin: My time is up, sir.

And if I could just follow up on that later, if we can meet with you later, I'd --

Mr. Work: Absolutely, sir.

Senator Manchin: -- very much appreciate it.

Director Clapper: Senator, if I may just add a word here about -- this is a point Admiral Rogers has made in the past about, you know, terminology, lexicon, nomenclature definitions are important. And so, what this represents, of course, is espionage -- economic --

Senator Manchin: Absolutely.

Director Clapper: -- cyber espionage. And, of course, we, too, practice, cyber espionage. You know, in a public forum to, you know, say how successful we are, but we're not bad at it. So, when we talk about, "What are we going to do for -- to counter espionage or punish somebody or retaliate for espionage," well, we -- I think it's a good idea to at least think about the old saw about people who live in glass houses --

Senator Manchin: Gotcha.

Director Clapper: -- shouldn't throw rocks.

Chairman McCain: So, it's okay for them to steal our

secrets that are most important --

[Laughter.]

Director Clapper: I didn't say that --

Chairman McCain: -- including our fighter, because --

Director Clapper: I didn't say that, Senator.

Chairman McCain: -- because we live in a glass house. That is astounding.

Senator Ayotte.

Director Clapper: I did not say it's a good thing. I'm just saying that both nations engage in this.

Senator Ayotte: I want to thank all of you for being here.

With regard to the Chinese, I want to follow up on -- we've talked about the stealing of the highest secrets, in terms of our weapon system, but what about the 21 million people whose background check and personal information has been, of course, associated publicly with the Chinese, and the fact that we know that 5 million sets of fingerprints, as well, leading to potential vulnerability for our citizens? And if you put that in the context of these other issues that we've raised, it seems to me -- I looked very carefully, for example, Secretary Work, at some of the language you've been using. You gave a speech at the Royal United Services Institute in London. You said, "Deterrence must be demonstrated to be effective."

Secretary Clapper, in your prepared statement, you said, "The muted response by most victims to cyberattacks has created a permissive environment."

So, I'm trying to figure out, based on what you've said, how we're not in a permissive environment, in light of what they've stolen on our weapon systems, but also this huge infringement on 21 million people in this country.

And also, could you comment on the vulnerability of that data and where we are, in terms of how it could be used against us?

Director Clapper: Well, first, that is an assessment of what was taken. We actually don't know, in terms of specific -- specifics. But, that's -- I think frames the magnitude of this theft. And it is potentially very serious -- has very serious implications, first, close to home, from the standpoint of the intelligence community and the potential for identifying people who may be under covered status, just one small example. And, of course, it poses all kinds of potential -- and, unfortunately, this is a gift that's going to keep on giving for years.

So, it's a very serious situation. What we've tried to do is educate people what to look for and how to protect themselves. But, again, this is a huge threat -- theft, and it has, potentially, damaging implications for lots of people in the intelligence community and lots of people in

the Department of Defense and other employees of the government.

Senator Ayotte: So, I think what you're hearing from some of us up here is just a -- "Now what are we going to do about it?" is the issue, as opposed to a shared agreement on generic principles with the Chinese. This is a pretty significant issue that is going to impact millions of Americans. I'm not hearing what we're going to do about it, but that may be a higher-level decision, going up to the President. But, seems to me if we're going to talk about deterrence, if we don't follow up with action, and if you look at that, combined with the testimony we heard last week about the artificial islands being built by the Chinese, and the fact that we won't even go within, I believe it's 12 nautical miles of those islands -- if you put that all from the Chinese perspective, I think you think, "Hmmm, we can pretty much do what we want to do, because we haven't seen a response."

Now, I'm not asking for -- from all of you -- to answer that, because it probably needs to be answered by the President and his national security team, but it seems to me that they aren't seeing a response right now from us, and therefore, we're going to see -- continue to see bad behavior from the Chinese.

Before I go, I have an important question on another

topic, Secretary Work, and that is: Yesterday, we heard public reports about a potential violation of the INF Treaty by the Russians, and that, essentially, Russia tested -- flight tested a new ground-launched cruise missile this month that U.S. intelligence agencies say further violates the 1987 INF Treaty. And, of course, this is going back, also, to the reports, as early as 2008, of the -- Russia conducting tests of another ground-launched cruise missile, in potential violation of the INF Treaty that we've raised with them. And, when Secretary Carter came before our committee, on his confirmation, he listed three potential responses to these INF violations. So, now we have the Russians violating the INF Treaty yet again. And I guess my question is: Secretary Carter rightly identified that we should respond, either through missile defense, counterforce, or countervailing measures. What are we doing about it?

Mr. Work: Senator, this is a longstanding issue that we have been discussing with the Russians. The system that you're talking about is in development, it has not been fielded yet. We are -- we have had different discussions with them on our perception of the violation of the INF, and they have come back. This is still in discussions, and we have not decided on any particular action at this point.

Senator Ayotte: So, are you saying that you don't

think they violated the INF Treaty?

Mr. Work: We believe very strongly that they did.

Senator Ayotte: That's what I thought. So, what are we going to do about it? Because they're claiming that they haven't, going back to the 2008 violations, and now here we have another situation.

Mr. Work: It's still under -- because they have not fielded the system, we are still in the midst of negotiating this position. We are giving ours. But, if they do field a system that violates the INF, I would expect us to take one of the three options that Secretary Carter outlined before the committee.

Senator Ayotte: So, my time is up, but I see two consistent themes here, both with the Chinese and the Russian: a lot of talk, no action, unfortunately. And people take their cues from that. And that worries me.

Thank you all.

Chairman McCain: Senator Hirono.

Senator Hirono: Thank you, Mr. Chairman.

Director Clapper, you testified before the House Intelligence Committee recently that the -- while the United States makes distinctions between cyberattacks conducted for economic purposes or to gain foreign intelligence, I would -- that's the espionage arena, I think, that you're referring to -- or to cause damage, our adversaries do not.

Would you consider the OPM breach, to the extent that we believe it is a state actor who did that, that that would be in the category of espionage?

Director Clapper: Yes.

Senator Hirono: The --

Director Clapper: That was the tenor of the discussion at the HTSC hearing that Admiral Rogers and I engaged in. And, of course, that has to do with the -- as I mentioned earlier to Senator Manchin, the importance of definition, nomenclature, and terms. So -- and the definition of these terms -- and so, what -- the theft of the OPM data, as egregious as it was, we wouldn't necessarily consider it as an attack. Rather, it would --

Senator Hirono: Yes.

Director Clapper: -- be a form of --

Senator Hirono: Well, and --

Director Clapper: -- theft or espionage.

Senator Hirono: And, as you say, other countries, including our own, engages in such activities.

My understanding of the recent agreement between the United States and China, though, has to do with commercial cybertheft. And I think that's a very different category that has to do with obtaining information about corporations, et cetera. And therefore, that that is in the category of economic attacks. So, Director Clapper, would

you consider that kind of an agreement to be helpful? I realize that you are skeptical, but, to the extent that we are defining a particular kind of cyberattack, and that we're contemplating, through this agreement, an ability of our two countries to engage in high-level dialogue regarding these kinds of attacks, is that a helpful situation?

Director Clapper: Well, it would be very helpful if, of course, the Chinese actually live up to what they agreed to. So, if -- and what the agreement pertained to was theft of data for economic purposes to give Chinese commercial concerns an advantage, or their defense industries an advantage, as opposed to -- I don't believe they -- that we've agreed with the Chinese to stop spying on each other.

Senator Hirono: Yes.

Director Clapper: And so, there is a --

Senator Hirono: The --

Director Clapper: -- for purely espionage purposes -- and there is a distinction.

Senator Hirono: Mr. Secretary, you can weigh on this also. To the extent that we've created an -- a potential for a dialogue or an environment where there's a process to be followed, and the cases where we suspect commercial cyberattacks, that at least we have a way that we can talk to the Chinese. Because you also mentioned, Director Clapper, that attribution is not the easiest thing, although

we are getting better at figuring out who actually were the actors who that did these cyberattacks. So, one hopes that, even with a great deal of skepticism, going forward, that this agreement may create the space for us to have a -- more than a conversation, but one that would lead to some kind of a change in behavior on the part of these state actors.

Mr. Secretary, feel free to give us your opinion.

Mr. Work: Senator, I think that's exactly right. I mean, as Director Clapper said, first you have to find out the geographical location from the -- where the attack came from. Then you have to identify the actor, and then you have to identify whether the government of that geographic space was either controlling --

Senator Hirono: Recognize that's not the easiest to do, yes.

Mr. Work: And what we have done is, we have confronted China, and China, in some cases, has said, "Look, this was a hacker that was inside our country, but we had no control over him." What this allows us to do is say, "Okay, well, what are you going to do about that? That's a cybercrime. Are you going to provide us the information we need to prosecute this person? Are you going to take care of it on your own?" So, I believe this type of confidence-building measure and this way to discuss these things will -- the proof will be in the pudding, how the Chinese react to this

--

Senator Hirono: Mr. Secretary, I think you mentioned that this particular agreement allows -- contemplates meeting at least twice a year.

Mr. Work: Yes.

Senator Hirono: Is there anything that prevents more frequent dialogue between our two countries in suspected cases of commercial cyberattacks?

Mr. Work: Senator, I believe, if there was a significant cyber event that we suspected the Chinese of doing or they suspected us, that we would be able to meet this. This is going to be a high-level joint dialogue. They'll -- the Chinese will have it at the ministerial level. Our U.S. Secretary of Homeland Security and the U.S. Attorney General will co-lead on our part. We're going to have the first meeting of this group by the end of this calendar year, and then at least twice a year. So, I believe that, as Director Clapper is, I think all of us have some healthy skepticism about this, but I believe it's a good confidence-building measure and a good first step, and we will see if it leads to better behavior on the part of the Chinese.

Senator Hirono: Thank you.

Chairman McCain: Mr. Secretary, I can't help but comment. We have identified the PLA, the building in which

they operate. Now, please don't deceive this committee as if we don't know who's responsible for it. That's just very disingenuous. There have been public reports that we've identified the PLA building in which these cyberattacks come from.

Senator Ernst.

Senator Ernst: Thank you, Mr. Chair.

Thank you, gentlemen, for joining us today.

Admiral Rogers, I'll start with you, sir.

Admiral Rogers: Okay.

Senator Ernst: Two of the President's nine lines of effort in defeating ISIL are, first, exposing ISIS's true nature and, second, disrupting the foreign fighter flow. And, over the weekend, the New York Times reported that 30,000 recruits joined ISIS over the past year, and that's double the previous recruitment year.

Earlier this month in reference to ISIS recruiting, the State Department's Ambassador-at-Large and Coordinator for Counterterrorism said that ISIS's recruiting trend is still upward, and this information came of no surprise to her. The Ambassador also said the upward trend was primarily due to Internet and social media.

So, sir, do you believe the administration's efforts have so far succeeded on these two lines of effort in cyberspace and social media? Just, please, simple yes or

no.

Admiral Rogers: No.

Senator Ernst: Okay. In light of that, with the record recruiting numbers for ISIS, how would you then assess the effectiveness of the U.S. Government's counter-ISIS effort in cyberspace? So, what specifically is your assessment of the State Department's "think again, turn away" program in support of efforts to disrupt ISIS's online recruiting effort?

Admiral Rogers: Senator, I'm not in a position to comment on State Department -- the specifics of their program. I honestly am just not knowledgeable about it. I will say this, broadly, to get to, I think, your broader point. I have always believed that we must contest ISIL in the information domain every bit as aggressively as we are contesting them on the battlefield, that the information dynamic is an essential component of their vision, their strategy, and ultimately their success. And we have got to be willing to attempt to fight them in that domain, just like we are on the battlefield. And we clearly are not there yet.

Senator Ernst: I agree. I think we are failing in this effort. And some of the programs that we have seen obviously are not working. So, are there areas in -- where you could recommend how the U.S. Government better partner

with various NGOs or private entities to more effectively counter the ISIS propaganda?

Admiral Rogers: Again, the contesting-the-propaganda piece, much broader than Cyber Command's mission. I will say, from a technical and operational perspective, we, broadly within the DOD, Cyber Command, Strategic Command, and CENTCOM, are looking at, within our authorities, within our capabilities, what's with -- in the realm of the possible, in terms of, What can we do to help contest them in this domain?

Senator Ernst: Okay.

We have a larger problem coming forward, too, in regards to ISIS and ISIL in the Middle East. We seem to see the emergence of a trifecta between Syria, Iran, and Russia. And now it seems that Iraq has begun information-sharing with Russia, with Iran, with Syria. Director Clapper, can you speak to that and the broader implications of Russia emerging as a leader in the Middle East while we seem to be frittering away our opportunity with ISIL?

Director Clapper: Well, that's certainly their objective. I think they have several objectives, here, one of which is that -- I think, protect their base, the -- their presence in Syria, ergo their buildup in the northwest part of Syria; clearly want to prop up Assad; and, I think, a belated motivation for them is fighting ISIL.

As far as the joint intelligence arrangement is concerned, I can't go into detail here in this forum, but I will say there are -- each of the parties entering into this are a little bit suspicious of just what is entailed here, so we'll have to see just how robust a capability that actually provides.

Senator Ernst: Okay, I appreciate that.

And, Secretary Work, do you have any thoughts on the emergence of Russia with the intelligence-sharing, how that might impact the operations that we have ongoing in Iraq against ISIS?

Mr. Work: Well, I think we were caught by surprise that Iraq entered into this agreement with Syria and Iran and Russia. Obviously, we are not going to share intelligence with either Syria or Russia or Iran. So, we are in the process -- our -- we are in the process of working to try to find out exactly what Iraq has said. Certainly, we're not going to provide any classified information or information that would help those actors on the battlefield. Really what we're trying to do is deconflict, and that is the primary purpose of the discussion between President Obama and President Putin yesterday -- is, "If you are going to act on this battlefield, we have to deconflict."

The other thing we have made clear is -- they would

like to do a military first, followed by a political transition. We need -- we believe those two things have to go in parallel, and that has been our consistent message. This is early days. We're still in the midst of discussing what exactly this means, so I don't have any definitive answers for you at this point, Senator.

Senator Ernst: Well, I am very concerned that we have abdicated our role in the Middle East as -- and in so many other areas, as has been pointed out earlier. Grave concern to all of us. And I think we need to be working much more diligently on this.

Thank you, Mr. Chair.

Chairman McCain: Senator Nelson.

Senator Nelson: Thank you, Mr. Chairman.

Gentlemen, thank you for your public service.

Admiral, I'm concerned about all of these private telecoms that are going to encrypt. If you have encryption of everything, how, in your opinion, does that affect Section 702 and 215 collection programs?

Admiral Rogers: It certainly makes it more difficult.

Senator Nelson: Does the administration have a policy position on this?

Admiral Rogers: No, I think we're still -- I mean, we're the first to acknowledge this is an incredibly complicated issue with a lot of very valid perspectives.

And we're still, I think, collectively, trying to work our way through, "So, what's the right way ahead, here?" -- recognizing that there's a lot of very valid perspectives.

But, from the perspective, as Cyber Command and NSA, that I look at the issue, there's a huge challenge us -- for us, here, that we have got to deal with.

Senator Nelson: A huge challenge. And I have a policy position, and that is that the telecoms better cooperate with the United States Government, or else it just magnifies the ability for the bad guys to utilize the Internet to achieve their purposes.

Speaking of that, we have a fantastic U.S. military. We are able to protect ourselves. It's a -- it's the best military in the world. But, we have a vulnerability now, and it's a cyberattack. Do you want to see if you can make me feel any better about our ability to protect ourselves, going forward?

Admiral Rogers: So, I would tell you the current stated capability in the Department, if I just look at where we were 18 months ago, 2 years ago, is significantly improved. We currently defeat probably 99-point-some-odd percent attempts to penetrate DOD systems on a daily basis. The capability, in terms of both the amount of teams, their capability, just continues to improve. Our speed, our agility. The challenge for us, fundamentally, to me, is, we

are trying to overcome decades of a thought process in which redundancy, defensibility, and reliability were never core design characteristics for our networks, where we assumed, in the development of our weapon systems, that external interfaces, if you will, with the outside world were not something to be overly concerned with. They represented opportunity for us to remotely monitor activity, to generate data as to how aircraft, for example, or ships' hulls were doing in different sea states around the world. All positives if you're trying to develop the next generation, for example, of cruiser/destroyer for the Navy. But, in a world in which those public interfaces, if you were, increasingly represent also potential points of vulnerability, you get this class of strategies, if you will. And that's where we find ourselves now.

So, one of the things I try to remind people is, it took us decades to get here. We are not going to fix this set of problems in a few years. This takes dedicated prioritization, dedicated commitment, resources, and we've got to do this in a smart way. We've got to prioritize, and we've got to figure out what's the greatest vulnerability and where's the greatest concern for us?

Mr. Work: Senator, is it okay if I jump in here for a second?

Senator Nelson: Yes. I just want to add to that. And

for us to let our potential enemies understand that we have the capability of doing to them what they do to us. However, that gets more complicated when you're dealing with a rogue group of a dozen people stuck in a room somewhere that are not part of a nation-state.

Yes, sir. Mr. Secretary.

Mr. Work: Well, I was just going to echo what Admiral Rogers said. When Secretary Carter came in, he said, "Look, we are absolutely not where we need to be," and he made job number one defense of the networks. So, we're going from 15,000 enclaves to less than 500. We're going to have -- we're going from 1,000 defendable firewalls to less than 200, somewhere between 50 and 200. So, you are absolutely right, we have recognized this is a terrible vulnerability. We are working, first, to defend our networks, as we talked about earlier. We're looking at our systems. And we're also trying to change the culture. Right now, if you discharge a weapon, you are held accountable for that. That's a -- you know, negligent discharge is one of the worst things you can do. What we need to do is inculcate a culture where a cyber discharge is considered just as bad, and make sure that that culture is inculcated throughout the force.

Senator Nelson: I agree. But, now the Admiral is assaulted by the telecoms, who want to tie his hands behind

his back by doing all of the encryption.

Thank you, Mr. Chairman.

Chairman McCain: Senator Donnelly.

Senator Donnelly: Thank you, Mr. Chairman.

In our State, Naval Surface Warfare Center Crane has taken the lead on much of our efforts to protect against the threat of counterfeit electronics. And so, Secretary Work and Director Clapper, the global supply chain for microelectronics presents a growing challenge for cybersecurity. One of the things we saw recently, IBM sold its chipmaking facilities with DOD "trusted foundry" status to a foreign-owned competitor. So, I was wondering your top priorities in managing the risk posed by the globalization of our microelectronics manufacturing capabilities and our abilities to protect our systems in that area.

Mr. Work: That's a big question, Senator. In fact, it's going to be one of the key things we look at in this fall review, because of the recent -- as you said, the recent sale of the IBM chips.

Now, there are two schools of thoughts on this. Secretary Carter personally has jumped into this. And some say you do not need a trusted foundry. Another group says you absolutely have to have it. Having confidence in the chips that we put in our weapon systems is important. And I would expect that, come February, we'll be able to report

out the final decisions through the fall review on how we're going to tackle this problem.

Senator Donnelly: Who within DOD's leadership has primary responsibility for overseeing the supply chain risk management?

Mr. Work: That would be Frank Kendall and also DLA. DLA has the supply chain, and Frank Kendall is really focused on the trusted chip, the fabrication of trusted chips.

Senator Donnelly: One of the areas that we look at in regards to cyber -- and, in some ways, you know, technology in particular parts of it not advancing has been a good thing in this respect -- is in the nuclear area. And so, are there any specific groups that are focused just on protecting our nuclear efforts against cyber?

Mr. Work: There's the National -- the NNSA. And also, we have a Nuclear Weapons Council, which is cochaired by, again, Frank Kendall, our Under Secretary of Defense for AT&L, and the Vice Chairman of the Joint Chiefs. They are the ones that work with DOE to make sure that our weapon system components are reliable and trusted, and to make sure that we have a safe, reliable, and effective nuclear deterrent.

Senator Donnelly: Admiral, when we look at building a force of cyber warriors, a cyber team, how can we use the

National Guard and Reserves to help do that? Because it strikes me that that can help us in retaining highly qualified individuals who want to devote part of their life to helping their country. And it would seem to almost be a perfect fit for us.

Admiral Rogers: So, we have taken a total-force approach to the force that we're building out. That includes both Guard and Reserve. Every service slightly different, not the least of which because different services have different Reserve and Guard structures. So, that is a part of it.

I'd say one of the challenges that we're still trying to work our way through is under the Title 32 piece, how we coordinate what Guard and Reserve are doing, how we generate capacity and bring it to bear with maximum efficiency. The one thing -- the two things, in partnering with my Guard teammates and my Reserve teammates -- because we're taking a total-force approach to this, we need one standard for this. We don't want a place where the Guard and Reserve are trained in one standard and the Active side is trained to a different. That gives us maximum flexibility in how we apply the capability across the force. And the Guard and Reserve has done great in that regard. And then, secondly, we need one common unit structure. We don't want to build unique, one-of-a-kind structures in the Guard or Reserves

that don't match the Title 10 side. Again, we want to treat this as one integrated force. And again, I would give the Guard and the Reserves great kudos in that regard. We've got a common vision about the way we need to go, and we've got a great exercise series, CYBERGUARD, that we're using every year, where we bring together the Guard, the private sector, the Active component, and government, and work our way through the specifics about how we're going to make this work.

Senator Donnelly: Thank you.

Director Clapper -- and I apologize if you already answered this -- what is the one cyber challenge you are most concerned about?

Director Clapper: Well, obviously, the one that I think about is -- would be a massive Armageddon-like-scale attack against our infrastructure. That is not -- we don't consider that the most likely probably right now, that the greater threat -- or the low-to-moderate sort of threats that we're seeing. And what I have seen in the 5 years I've been in this job is a sort of progression, where these get more aggressive and more damaging. And, as I indicated in my oral statement at the outset, what I will see -- I think what we can expect next are data manipulation, which then calls to question the integrity of the data, which, in many ways, is more insidious than the kinds of attacks that we've

suffered thus far.

So, you know, the greater -- the specter is this massive attack, although it's not likely.

Senator Donnelly: Thank you.

Thank you, Mr. Chairman.

Chairman McCain: Senator Lee.

Senator Lee: Thank you, Mr. Chairman.

Annex 3 of the recently signed Iran Nuclear Agreement calls for the participating countries to work with Iran to, quote, "strengthen Iran's ability to protect against and respond to nuclear security threats, including sabotage, as well as to enable effective and sustainable nuclear security and physical protection systems," close quote.

Secretary Clapper, do you read this portion of the Iran Nuclear Agreement, the Annex, to include cyberthreats, meaning that the P5+1 countries, who are part of this agreement, will be expected -- will be deemed to have an obligation under the agreement to assist Iran in developing systems to prevent other countries from using cyber capabilities to acquire information about, or to disrupt the operations of, Iran's nuclear capabilities -- Iran's nuclear programs?

Director Clapper: Well, in this environs, I will say that I trust that this is not going to prevent us from gleaning intelligence from our traditional sources, in the

interests of verifying the agreement, which will be principally monitored by international organization, IAEA. So, I'm not aware of any strictures on our ability to collect on their behavior and their components.

Senator Lee: But, why would we want to give Iran the ability to defend against cyberweapons that we, or perhaps some of our allies, might one day want to use against Iran?

Director Clapper: Well, sir, in this open environment, there are some aspects here that I can't discuss. I'm happy to talk with you privately or in a classified environment about that.

Senator Lee: Okay. Okay. But, you're not disputing the fact that the agreement says that, that we would have to --

Director Clapper: No.

Senator Lee: Okay.

Now, can you tell me, in this environment, what specific technical assistance we'll be offering Iran in this portion of the agreement?

Director Clapper: I honestly don't know the answer to that question. I've -- have to have that researched. I don't know exactly what would -- what's in mind there.

Senator Lee: Now, would any of these capabilities, once acquired by Iran, prevent or inhibit the United States or any of our allies, any other enemy of Iran, from using

any cybermeasure against Iranian nuclear facilities?

Director Clapper: Again, I -- I'm reluctant to discuss that in this setting.

Senator Lee: Were you consulted by U.S. negotiators during the nuclear negotiations in connection with this portion of the agreement, the agreement --

Director Clapper: Well, the intelligence community was deeply involved in -- throughout the negotiations.

Senator Lee: Can you describe the nature of any consultation you had with them as to this portion of Annex 3?

Director Clapper: With the Iranians?

Senator Lee: Yes.

Director Clapper: I -- no, I did not engage with the Iranians on --

Senator Lee: No, no, that's not what I'm asking. I'm asking if you can describe your discussions with U.S. negotiators as they came to you and consulted with you on the implications of this portion of Annex 3.

Director Clapper: I didn't actually -- my lead for this was Norm Roule, who was the -- known to many of you on this committee, the National Intelligence Manager for Iran. And he was the direct participant. And I -- I don't want to speak for him as -- to the extent to which he was involved or consulted on that provision. I'd have to ask him.

Senator Lee: Okay. But, you would have been aware of consultation going on. I mean, I'm sure he came to you and said, "Look, this is going to impact our ability, the ability of the United States, to do what we need to do with respect to Iran." That -- would that not have been something --

Director Clapper: Well, again, sir, I would rather discuss what the potential response of ours could be in a closed setting.

Senator Lee: Okay.

Secretary Work, how is the Department working to ensure that the hardware and software on some of these major programs that we're developing to future contingencies and technological advances so they can continue to address emerging cyberthreats well into the future without major overhauls of the entire system?

Mr. Work: Senator, as I said, we are now putting into our KPPs, our key performance parameters, on any new systems, specific cyber-hardening requirements, much like during the Cold War, when we had EMP requirements for many of our systems. The problem that we face is that many of the old systems that are still in service were not built to the -- to respond to the cyberthreats that we see today. So, we're having to go back through all of those older systems, determine which ones are most vulnerable,

prioritize them, and make fixes. So -- and it also goes back to Senator Donnelly's question on the trusted foundry. We're trying to determine what is the best way to assure that we have reliable and trust microelectronics.

Senator Lee: Okay. Thank you.

I see my time's expired.

Thank you, Mr. Chairman.

Chairman McCain: Senator King.

Senator King: Thank you, Mr. Chairman.

Secretary Work, if there's a catastrophic attack tonight on the fiscal infrastructure or the financial infrastructure of this country, I do not want to go on cable news in the morning, if there is cable news in the morning, and say, "The administration told us that the policy is still in development." We've got to get on this. We've been talking about it for years. And, as the Chairman pointed out, this was an essential part of our National Defense Authorization Act, a year ago, And the idea that we can continue to simply defend and never have an offensive capability, I just think is ignoring this enormous threat, which we all agree --

So, let me ask a one-word-answer question to each of you. Do we need an offensive capability in the cyber realm in order to act as a deterrent?

Secretary Work.

Mr. Work: We need a broad range of response options, to include --

Senator King: Do we need a offensive cybercapability to act as a deterrent?

Mr. Work: I would say yes, sir.

Senator King: Secretary -- Director, go ahead.

Director Clapper: Absolutely.

Senator King: Admiral Rogers.

Admiral Rogers: Yes.

Senator King: Thank you.

The second part of that is that it can't be secret. Our instinct is to make everything secret. And the whole point of a deterrent capability is that it not be secret. So, I think we need to establish what we have -- I suspect we do have some significant offensive capability, but part of a -- making it a deterrent is that it has to be made -- it has to be made public.

I think another question that needs to be addressed -- and I don't necessarily think it -- in this hearing this morning, but in this -- terms of the policy -- we need to define what an act of war is in the cyber area, whether hitting Sony pictures is an act of war, or the OPM. And how do you draw those lines? And I would suggest that that's got to be part of this policy definition.

And I don't mean to imply, Secretary Work, that this is

easy. But, it's urgent. That's the -- and we just simply can't defend ourselves by saying, "Well, it was complicated and we didn't get to it."

Changing the subject slightly. Admiral Rogers, do you believe that the dispersion of responsibility in the Federal Government for cyber is a potential problem? It strikes me we've got agencies and departments and bureaus -- I suspect you could name 15 of them if you tried -- that all have some responsibility here. Do we need to strengthen Cyber Command and make that the central repository of this policy?

Admiral Rogers: I would not make Cyber Command or the Department of Defense the central repository. This is much broader than just the DOD perspective. But, I will say this. I have been very public in saying we have got to simplify this structure for the outside world, because if you're on the outside looking in -- and I hear this from the private sector fairly regularly -- "Who do you want me to go to? Is it -- I should talk to the FBI. Should I talk to DHS? Why can't I deal with you? Do I need to talk to the" -- if I'm a financial company, "Should I be talking to the sector construct that we've created?" We have got to try to simplify this for the private sector.

Director Clapper: If I might add to that, Senator King, it's one of the reasons why I had a very brief commercial for -- just within the intelligence community --

of integrating the cyber picture, the common operating picture simply from within intelligence, let alone, you know, what we do to react or protect. And that, to me, is one important thing that I have come to believe. We need along the lines of a mini-NCTC or NCPC.

Senator King: I would hope that that would also -- and that -- the leadership and decisionmaking on that has to start with the White House, it has to start with the administration, for an all-of-government approach to dealing with this dispersion-of-responsibility problem.

I would point out, parenthetically, that -- you know, we're -- there's been a lot of talk about China and our ability to interact with China and to respond and hold China responsible. And it's not the subject of this hearing, but the fact that we owe China trillions of dollars compromises our ability to interact with China in a firm way. It's a complicated relationship, and that's one of the things that makes it difficult.

Director Clapper, do you have any idea what brought the Chinese to the table for this recent agreement with the President?

Director Clapper: Well, it appears that the threat of potential economic sanctions, particularly imposing them right before the visit of President Xi, I think, got their attention. And that's why they dispatched Minister Maung to

try to come to some sort of agreement, which is what ensued subsequently.

Senator King: And I agree that it's not a definitive agreement or a treaty, but I do agree, Secretary Work, that it's a step in the right direction. At least these issues are being discussed. But, countries, ultimately, only act in their own self-interest, and we have to convince the Chinese that it's in their interest to cut out this activity that's so detrimental to our country.

Thank you, gentlemen, for your --

Mr. Work: Senator, could I just make --

Senator King: Yes, sir.

Mr. Work: -- one real quick comment?

Just because we have not published our policy -- it is so broad and encompassing, going over things like encryption -- What are the types of authorities we need? -- does not mean that, if we did have an attack tonight, we would not -- we do not have the structure in place right now with the national security team to get together to try to understand who caused the attack, to understand what the implications of the attack were and what response we should take. Those are in place right now.

Senator King: But, the whole point of being able to respond is deterrence so that the attack won't occur. Dr. Strangelove taught us that if you have a doomsday machine

and no one knows about it, it's useless. So, having a secret plan as to how we'll respond isn't the point I'm trying to get at. The deal is, we have -- they have to know how we will respond, and therefore, not attack in the first place.

Thank you.

Thank you all, gentlemen, for your testimony.

Senator Reed [presiding]: On behalf of the Chairman, let me recognize Senator Fischer.

Senator Fischer: Thank you, Senator Reed.

Following up a little bit where Senator King was going on this, many of you talked about establishing norms in cyberspace. Do you think it's possible to establish or maintain that norm without enforcement behaviors? When we look at publicly identifying those who are responsible for an activity or imposing costs on them, can we do that? I'll begin with you, Mr. Secretary.

Mr. Work: Well, I believe that trying to establish these norms are very, very helpful. In the Cold War, for example, there was a tacit agreement that we would not attack each of our early-warning missile -- I mean, warning satellites. And so, establishing these norms are very important. But, they will be extremely difficult, because the enforcement mechanisms in cyber are far more difficult than -- because it's much more easy to attribute missile

attacks, et cetera. So, I believe that this agreement with China is a good first step, that we should strive to establish norms, especially between nation-states -- and establish norms which we believe are beyond the bounds, and to try to establish mechanisms by which we can work these through. But, this will be very, very difficult, Senator, because it's -- because of the -- just the -- it's much more difficult.

Director Clapper: And we have the added problem, of course, of -- the norms are, as Secretary Work said, really applicable to nation-states. And, of course, you have a whole range of non-nation-state actors out there who wouldn't necessarily subscribe to these norms and would be a challenge to deal with even if we -- if there were nation-state mutual agreement.

Senator Fischer: Admiral?

Admiral Rogers: I would echo the comments of my two teammates. I'm struck by -- we're all captives of our own experience. In my early days as a sailor, well before I got into this business, at the height of the Cold War out there, we knew exactly how far we -- between the Soviets and us -- we knew exactly how far we could push each other. And we pushed each other, at times, right up to the edge. I mean, very aggressive behaviors. But, at the -- we developed a set of norms. We had a series of deconfliction mechanisms

in the maritime environment. We actually developed a set of signals over time so we could communicate with each other. But, the -- so, I'm comfortable that we're going to be able to achieve this over time in the nation-state arena, but, as my teammates have said, it's the nonstate actor that really complicates this, to me. It's going to make this difficult.

Senator Fischer: So, when we're attacked in cyberspace, how do we impose costs on those who are attacking us? Do we respond in cyberspace, or can we look at other ways to, I think, respond in an appropriate manner, say with sanctions? What would you look at, Admiral?

Admiral Rogers: So, what we have talked about previously is, we want to make sure we don't look at this just from one narrow perspective, that we think more broadly, we look across the breadth of capabilities and advantages that we enjoy as a nation, and we bring all of that to bear as we're looking at options as to what we do, and that it's a case-by-case basis. There's no one single one-size-fits-all answers to this. But, fundamentally, think more broadly than just cyber. Not that cyber isn't potentially a part of this. I don't mean to imply that.

Senator Fischer: Correct.

Mr. Secretary, would you agree with the Admiral on that? Do you see a variety of options out there? And wouldn't it be more beneficial to us as a country to be able

to have a policy that is a public policy on what those options could be, and the consequences that would be felt when we are attacked?

Mr. Work: Absolutely. And that is what I say about a broad policy, where we will respond in a time manner -- time, place, and manner of our own choosing. In this case, there's an asymmetry with our nation-state potential adversaries. They are all authoritarian states. The attack surfaces that they have are far smaller than what we have as a free nation. And we value that. We do not want to close down the Internet. But, we are more vulnerable to a wide variety of attack surfaces than our adversaries. So, we may sometimes have to respond proportionally, but in a different way than a simple cyber response. It might be sanctions. It might be a criminal indictment. It might be other reactions. So, we believe very strongly that this is something where it's an interagency process. The process is established where they are taken care of --

Senator Fischer: And --

Mr. Work: -- handled on a case-by-case basis.

Senator Fischer: And does the administration have a definition on what constitutes a cyberattack?

Mr. Work: Well, any type of malicious activity which causes either damage or theft of information or IP, all of those are under either cyber -- malicious cyberactivities.

It might be espionage. In each case, there's no defined red line for what would constitute --

Senator Fischer: What's --

Mr. Work: -- act of war.

Senator Fischer: What would be the difference between a cyberattack and cybervandalism?

Director Clapper: Well, I would have to make a -- again, a case-by-case determination. And, of course, important consideration here would -- in terms of our reaction, would be attribution. And that -- again, it would be case-by-case.

Mr. Work: And cybervandalism, ma'am, do you -- is that stealing information or IP or --

Senator Fischer: The attack by North Korea on Sony was described by the President as cybervandalism. I was just wondering on how you distinguish that definition from a cyberattack.

Director Clapper: Well, it didn't affect a national security entity, but it certainly did cause damage to the company. And, in that case -- and this is an important illustration of when we could attribute very clearly and there was uniform agreement across the intelligence community to attribute that attack to the North Koreans, and we did sanction them.

Senator Fischer: Okay, thank you.

Thank you, Mr. Chairman.

Chairman McCain [presiding]: Senator Heinrich.

Senator Heinrich: Thank you, Mr. Chair.

Gentlemen, thank you for your service and for joining us here today.

And, Director Clapper, before I start on -- begin to focus on cyberpolicy, I think we're all very concerned about the allegations that leadership at Central Command deliberately distorted the assessments of intelligent officers related to the fight against ISIL. And I understand that there is an ongoing investigation, and I'm going to wait for the results of that investigation. But, I want to say that, as a member of both this committee and the Intelligence Committee, I want to, in the strongest terms possible, impress upon you the importance for all of us to receive absolutely objective and unbiased assessments. And I look forward to the results of the IG investigation, and I expect that you will hold accountable anyone who has failed in their duty in the intelligence community, no matter how high up the chain that may go.

Director Clapper: Well, Senator, I -- you brought up a very important consideration here, which is a great concern to me. I'm a son of an Army intelligence officer who served in World War II, Korea, and Vietnam. And I have served in various intelligence capacities for over 52 years, ranging

from my first tour in Southeast Asia in the early '60s to my service now as the longest tenured DNI. And it is a almost sacred writ in intelligence -- in the intelligence profession never to politicize intelligence. I don't engage in it. I never have. And I don't condone it when it -- it's identified.

Having said that, I -- and I completely agree with you -- in spite of all the media hyperbole, I think it's best that we all await the outcome of the DOD IG investigation to determine whether and to what extent there was any politicization of intelligence at CENTCOM.

I will also say that the intelligence assessments from CENTCOM or any other combatant command come to the national level only through the Defense Intelligence Agency. That is the main conduit and, I will say, to the extent evaluater and filter for what flows into the national intelligence arena.

Senator Heinrich: Thank you, Director.

Turning to you, Admiral Rogers. As the director of U.S. Cyber Command, your responsibilities include strengthening our cyberdefense and our cyberdeterrence posture. And I want to return to a line of questioning several of my colleagues have begun this morning.

As you know, the breach of OPM computers resulted in an enormous loss of sensitive personal information. Thus far,

to my knowledge, the U.S. has not responded. And to put it in the words of Deputy Secretary Work's language this morning, we haven't imposed a cost, which raises questions about whether we truly have developed the mechanisms for proportionate response to cyberattacks against the U.S. Government, even after the April 2015 publication of the DOD cyber strategy. We know that if a foreign agent had been caught trying to steal U.S. personnel files in a less digital age, we would either kick them out of the country, if they were a diplomat, or we'd throw them in jail, if they weren't a diplomat. That would be considered a proportionate response. But, in the case of the OPM breach, the U.S. Government seems uncertain about what a proportionate response would look like.

So, I want to ask you three questions, and I'll let you take them as you may: What constitutes an act of war in cyberspace? Has the United States decided on a proportionate response in the case of the OPM cyber espionage case? And what types of information-gathering by nation-states, by governments, are legitimate, and what types are not?

Admiral Rogers: Well, first, let me start out by saying, look, so I'm the operational commander here, and all three of the questions you've just asked me are much broader than that. I'm glad to give you an opinion, but I'm mindful

of what my role is.

In terms of the three things -- Have we defined what an active of war is? The bottom line is: clearly, we're still working our way through that. What are the parameters that we want to use to define what is an act of war? My going-in position is, we ought to build on a framework that we have developed over time in the more conventional domains. That's a good point of departure for it. It's got a broad legal framework. It's something that people recognize. And it's where we ought to start as a point of departure.

The second question was about -- just let me read my note to myself --

Senator Heinrich: Proportional response to the OPM case.

Admiral Rogers: Again, I think that what OPM represents is a good question about -- so, what are the parameters we want to use? Is it -- as the DNI has said, is it -- the intent is within the acceptable realm? Is it scale? Is it -- you can do espionage at some level, for example, but if you trip some magic threshold, hey, is 20 million records, is 10 million records -- is there some scale component to this? I think we're clearly still trying to work our way through that issue. And there is no one-size-fits-all answer. I think there's recognition. I think that's clearly -- is what has driven this broad discussion

between the United States and China, for example. That's been a positive, I would argue.

And the third, type -- what -- could you repeat again -- the types of information?

Senator Heinrich: Just -- you know, I'll -- my time is expired, so I'll cut to the chase. I think what you're hearing from all of us --

Chairman McCain: No, go ahead, Senator. This is an important --

Senator Heinrich: -- is --

Chairman McCain: -- line of questioning.

Senator Heinrich: We would like to see more transparency in being able to telegraph our deterrent, because we all know that -- looking back into the Cold War, that our deterrent was very important. But, the other side knowing what that deterrent was, was absolutely critical for it to be effective. And so, we need to be clear about what types of information-gathering by governments are considered legitimate and acceptable, and where those red lines are going to be.

Admiral Rogers: I agree. I think that's the important part of the whole deterrence idea. It has to be something that's communicated, that generates understanding and expectation, and then a sense of consequence.

Director Clapper: I think the contrast with the Cold

War is a good one to think about, in that -- well, I think what you're -- what -- the concern that people are raising is, Should there be red lines on spying? That's really what this gets down to. We didn't have red lines during the Cold War. It was freewheeling as far as us collecting intelligence against the Soviet Union, and vice versa. There were no limits on that. It was very difficult, for both -- well, more so for us.

And, of course, underlying -- the backdrop to all that was the deterrent, the nuclear deterrent, which, of course, restrained behavior even though it got rough at times, as the example that Admiral Rogers cited, in a -- just in a maritime context. But, there were ground rules that governed that.

We're sort of in the Wild West here with cyber, where there are no limits that we've agreed on, no red lines, certainly on collecting information, and -- which is what the OPM breach represented.

Chairman McCain: Director and Admiral, I would like to thank you for your forthright and candid assessment. And also, I think, the lesson that all of us are getting is that we really have to have some policy decisions. And you've been very helpful in fleshing that out for us.

Senator Cotton.

Senator Cotton: Secretary Work, I'd like to return to

an exchange you had with Senator Ayotte about the Intermediate-Range Nuclear Forces Treaty, also known as the INF Treaty. Is Russia in violation of their obligations under the INF Treaty?

Mr. Work: We believe that a system that they have in development would violate the treaty.

Senator Cotton: And you said, just now, "in development." I thought I heard you say, with Senator Ayotte, that it's not deployed, or it's not yet operationally capable. Is that correct?

Mr. Work: That's my understanding. I can have -- I can get back to you with a question for the record. But, it is in development, and we have indicated our concern with the Russians that, if they did deploy it, we believe it would violate the INF.

Senator Cotton: Thank you. Could you please do that in writing. And, if it's appropriate, in a classified writing, that's fine, as well.

[The information referred to follows:]

[COMMITTEE INSERT]

Senator Cotton: I'd now like to move to the Cyber Mission Force. At the Air Force Association Conference a couple of weeks ago, Major General Ed Wilson, the commander of the 24th Air Force, stated that DOD's Cyber Mission Force was halfway through its buildup. How difficult is it to establish the needed infrastructure and manning across the services to create the capability that we need to defend and deter cyberthreats?

Mr. Work: Well, I'd like to start, and then I'll turn it over to Admiral Rogers.

We're building to 133 total teams -- 68 are cyber protection teams that are focused on our number-one mission: defense of our networks. We have 13 national mission teams that we are building to help defend our Nations' critical infrastructure. And we have 27 combat mission teams that are aligned with the combatant commanders and assist them in their planning. To support those, we have 25 support teams which they can call upon, for a total of 133. We're building to 6200 military personnel, civilians, and some specialized contractors, and another 2,000 in the Reserves, so about 8400.

We expect to reach that in 2018, provided there is not another government shutdown. The last time, we had a government shutdown and sequestration, it put us behind by 6 months in building this. So, as of right now, we are -- I

think we're on track.

And I'd turn it over to Admiral Rogers to explain the -- how well we're doing in attracting talent.

Admiral Rogers: And, if I could, first let me accent, if you will, one particular portion of DEPSECDEF Work's comments, in terms of impact of a government shutdown or sequestration for us. The last time we went through this and we shut it down, we assessed that we probably lost 6 months' worth of progress, because we had to shut down the school system, we went to all stop, in terms of generation of capability in the -- like a domino, the layover effect of all of that, we think, cost us about 6 months of time. If we go to a BCA or sequestration level, that puts us even further behind in an environment in which we have all uniformly come to the conclusion we're not where we need to be and we've got to be more aggressive in getting there. And you can't do that if -- when you're shutting down your efforts, when you're cutting money.

To go specifically, Senator, to the question you asked, I would tell you the generation of the teams, in terms of the manpower and their capability -- knock on wood -- is exceeding my expectations. The bigger challenge, to me, has been less -- not that it's not an insignificant challenge, but the bigger challenge has been less the teams and more some of the enabling capabilities that really power them,

the tools, if you will, the platform that we operate from, the training environment that we take for granted in every other mission set. The idea that we would take a brigade combat team -- before it went to Iraq, before it went to Afghanistan, we'd put it out in the National Training Center, and we'd put it through the spectrum of scenarios we think they're likely to encounter in their deployment. We don't have that capability right now in cyber. We have got to create that capability. It's those enablers, to me, and the intelligence piece, let -- just like any other mission set, everything we do is predicated on knowledge and insights. No different for the CENTCOM Commander than it is for me. Those are the areas, to me, where the challenges are greater, if you will, than just the manpower. I'm not trying to minimize the --

Senator Cotton: Yeah.

Admiral Rogers: -- manpower --

Senator Cotton: And how important is it that we take advantage of the existing infrastructure and capabilities that we have as you're building out the entire mission force?

Admiral Rogers: I mean, that's what we're doing right now. But, I will say, one of our experiences -- Cyber Command has now been in place for approximately 5 years -- one of our insights that we've gained with practical

experience and as we're looking at both defensive response as well as potential offensive options, we need to create infrastructure that is slightly separate from the infrastructure we use at NSA. It's -- so, a unified platform, you've heard us talk about. It's supported in the funding. That's an important part of this. Experience has taught us this in a way that 5-6 years ago, we didn't fully understand.

Senator Cotton: Well, I'd like -- my time is up for questioning, but I'd just like to bring to your attention that Arkansas Attorney General Mark Barry has requested a cyber protection team at Little Rock Air Force Base. There is an 11,000-square-foot facility there. It has a SCIF of 8500 square feet. It's already had $3.5 million invested in it. One of these facilities, I understand, would cost about $4 million. It's a request that I support. I think it's harnessed resources that we've already invested, and it also -- it's a capability that they are ready to support, in addition to the professional educational center that does a lot of cybertraining for the National Guard, which is less than 30 minutes away.

Thank you.

Director Clapper: Mr. Chairman, I have to comment. I'm rather struck by the irony, here, of -- before I left my office to come for this hearing, I was reviewing the

directions that we're putting out to our people for shutting down and furloughing people. What better time for a cyberattack by an adversary when much of our expertise might be furloughed.

Chairman McCain: I think that's a very important comment, Director, and thank you for saying it. There are some of us who feel it's urgent that we inform the American people of the threats to our national security of another government shutdown. I believe that it was an Arkansas philosopher that said there is no education in the second kick of a mule. So, I thank you for your comment.

Senator McCaskill.

Senator McCaskill: It was probably a Missouri mule.

Director Clapper, earlier this year I introduced a bill that would give intelligence community contractors whistleblower protections as long as those complaints were made within the chain or to the Inspector General or the GAO. So, disclosures made to the press would not be protected. I -- as you probably know, Defense Department -- I know that Secretary Work knows this -- that we've already put into the law, in recent years, whistleblower protections for the contractors at the Department of Defense. And, to my knowledge -- and certainly correct me if I'm wrong, any of you -- I'm not aware of any classified or sensitive information that has made its way to a damaging place as a

result of these protections.

The 2014 intel authorization gave these protections to the government employees within intelligence. And one of the challenges we have in government is this divide between the contractors and government employees. And, frankly, whistleblower protections -- I can't think of a good policy reason that we would give whistleblower protections to employees and not give them to contractors. And so, I am hopeful today that you would indicate that you believe this is an important principle and that we should move forward with this legislation.

Director Clapper: Absolutely, Senator. And we have published, internal to the intelligence community, an intelligence community directive that includes whistleblowing protections for contractors. After all, that was the source of our big problem, here, with Mr. Snowden, who was a contractor. And so, our challenge -- you know, the additional burden we have, of course, is trying to prevent the exposure of classified information outside channels. So, that's why whistleblowers absolutely must be protected, so that they are induced or motivated to go within the channels, knowing that they will be protected. This is a program that is managed by the intelligence community Inspector General, who is, of course, independent as a Senate-confirmed official.

Senator McCaskill: Thank you. And I'm pleased to see that you would be supportive of that.

And, Secretary Work and Admiral Rogers, I assume that you would be supportive of giving whistleblower protections to intelligence community contractors?

Mr. Work: Absolutely. I agree totally with what Director Clapper said.

Admiral Rogers: Yes, ma'am, and I say this as the head of an intelligence agency.

Senator McCaskill: Thank you.

I want to follow up a little bit, Director Clapper, with your comment about a shutdown. Could you tell us what impact another government shutdown would have on your progress of getting the cyber mission force fully operational? Excuse me -- Admiral Rogers. I think that, in political isolation, shutdown appeals to a certain swath of Americans, and I understand why. Because sometimes it just feels good to say, "Well, let's just shut it down," because, obviously, government is never going to win popularity contests, certainly not in my State. On the other hand, there's a difference between responsible, in terms of public policy, and being irresponsible, in terms of recognizing -- I love it when some of my friends wave the Constitution in my face and then fail to read the part that we have a divided checks and balances in this country, unlike other

countries. The American people sent a party -- a President of one party to the White House and elected a Congress of a different party. And that means we have to figure out how to get along. So, could you talk a moment about what the impact would be to this important mission if once again we went down the rabbit hole of deciding the best thing to do is just to shut down government?

Admiral Rogers: So, if we use our experience the last time, first thing I had to do was shut down the school system. And training and education is a core component of our ability to create this workforce. Just shut it all down, because it was only mission essential.

The second thing I was struck for, all travel that was associated with training, all -- we had to shut all that down, so I couldn't send people to generate more insights, to gain more knowledge.

We had to shut down some of our technical development efforts because of the closure -- again, put that all on hold. At a time where we have talked about the need to develop more capability, the need to develop more tools, I had to shut that all down during the period of the last shutdown. We were forced to focus our efforts on the continued day-to-day defense, which is critical -- don't get me wrong. As Secretary Work has indicated, it is priority number one for us.

The other concern I have is -- and I have watched this play out now just in the last 10 days -- I've been in command 18 months, and I will tell you, the biggest thing I get from my workforce, prior to the last 10 days, "Sir, this happened to us once in 2013. Is this going to happen again? If it is, why should I stay here, working for the government? I can make a whole lot more money in the cyber arena on the outside." So, in addition to the threat piece that the DNI has highlighted, my other concern is -- if we do this again, is the amount of our workforce that says, "You know, twice in the course of 2 years? I've got a family, I've got mortgages, I've got to take care of myself. As much as I love the mission, as much as I believe in defending the Nation, I can't put myself or my family through this. I've got to go work in the commercial sector." That would be terrible for us. Because people -- despite all our technology, never forget, it is men and women who power this enterprise. That's our advantage.

Senator McCaskill: At the risk of sounding like a smart aleck, which I do from time to time, I would say maybe we need to open some of those schools so some of my colleagues could do some math and realize the votes are not there to overcome a presidential veto. And this is a recipe for dysfunction that does not help anyone in this country, and particularly our national security.

Thank you, Mr. Chairman.

Chairman McCain: Senator Tillis.

Senator Tillis: Thank you, Mr. Chairman.

I want to just echo the comments of my colleague Senator McCaskill. I think it's irresponsible. We've had this -- the Secretary come before this committee and say that the number and severity of threats have not been greater since 9/11. That should be enough said, in terms of what we need to do to keep continuity in funding the government. All the other things that I may have a problem with have to be second to that priority. I thank you all for your work. And, Director Clapper, I thank you for your comment.

Admiral Rogers, we've had briefings from you since you've taken the command. And one of the briefings I'm reminded of is the trend that you see, in terms of the gap between what tends to be still an American advantage, overall, narrowing, particularly with nations like China and Russia, and I think you may have even mentioned Iran being an emerging threat. Can you tell me, really in the context of maybe another 6 months reset on your training, but, more importantly, based on your current funding streams and your current plan, Are we going to be able to widen that gap again, or is this just a matter of staying slightly ahead of our adversaries?

Admiral Rogers: For right now, I think the most likely scenario is, we're staying slightly ahead of our adversaries, because we're trying to do so much foundational work, if you will, as I said previously, trying to overcome a very different approach over the previous decades. It's not a criticism of that approach. It was a totally different world. It led to a different prioritization. It led to a different level of effort and a different investment strategy. Clearly, we're going to have to change that. And we're changing that at a time when budgets are going down and threats -- not just in cyber, but more broadly -- are proliferating. I don't envy the choices that Secretary Carter and the leadership has to make. There's nothing easy here.

So, I think, in the near term, the most likely scenario for us is, How can we focus on the best investments that maximize your defensive capability while continuing to help us retain the advantage we do right now against most?

Senator Tillis: Thank you.

And this question may be for Secretary Work. The announcement about the agreement with China, that we're not going to, basically, attack each other, in the face of the compelling evidence that we have that China's done it in the past and they've denied it, why is this agreement a positive thing if, with the smoking-gun information we have right now

on prior attacks, theft of intellectual property, commercial data, that we have a pretty strong base of evidence to say that they're guilty of it, if they deny it, why does this agreement mean anything?

Mr. Work: On the buildup to this visit, we made it very clear, through a wide variety of efforts, that this was going to be something that was foremost in the discussions when President Xi came. We have made it as clear as we possibly can in every single level, from the President on down, that the Chinese cyberactivities are unacceptable. And we believe that this is a good first step as a confidence-building measure, where China can either demonstrate that they are serious about establishing some norms, and going after crimes, et cetera. But, the proof will be in the pudding. I agree with Director Clapper and Admiral Rogers, it's going to be up to the Chinese to demonstrate that they're serious about this.

Senator Tillis: Would the manipulation of commercial data fall within the definition of theft under this agreement?

Mr. Work: Well, specifically, one part of it is the theft of IP -- intellectual property -- for commercial advantage in, say, for example, a Chinese state enterprise. And we have agreed, at least at -- we have made a tentative agreement that we will not do those type of activities.

China has done those activities in the past. It will be up to them to prove that they won't do it in the future.

Senator Tillis: And then, the -- for anyone, and then I'll yield. I know the committee's gone on a while. But, at what point -- I think Senator Heinrich made some very important points about drawing red lines. But, at what point are we going to have clear definitions about malign activities in cyberspace being acts of war or acts of terrorism, and then have appropriate responses, whether they be through cyber, through sanctions, or other? When are we going to get that clarity? Because we don't have it today.

Mr. Work: Senator, I don't believe that we will ever have a definitive one-size-fits-all definition for these type things. Every single attack will be -- have to -- handled on a case-by-case basis, and you will have to judge the damage that was caused, who made the attack, was it just a nonstate actor or just a malicious hacker -- we'd have to go after that person, in terms of criminal activity. So, I don't believe we're ever going to have a specific definition that says, "If this happens, we will trigger this response." Each one will be handled in a case-by-case basis and be proportional.

Senator Tillis: Well, thank you. Mr. Chair, the --

I think the lack of clarity, though, the only concern that I have is, you're not establishing some level of known

deterrent. And that's why -- I understand the complexities of it. I've worked in the field. But, I think that, without that clarity, you're more likely to have more things that you're going to have to look at and figure out how to do a situational response.

Thank you, Mr. Chair.

Chairman McCain: Senator Sullivan.

Senator Sullivan: Thank you, Mr. Chairman.

And thank you, gentlemen, for your testimony today on a really important topic.

You know, I believe and I'm -- I was looking for the transcript, but -- at the joint press conference between President Xi and President Obama that -- President of China, I think, publicly stated that they don't engage in these kind of cyberactivities. Was that an accurate statement, if that was, indeed, what he said, in terms of cyberwarfare? It's pretty remarkable, if you're in a press conference with another head of state, and you just say something that seems to be pretty blatantly false.

Director Clapper: Well, it is. And I think, apart from the statements, at least for our part, it will be: What happens now, what is -- will there be a change in their behavior? And as I said earlier, well, hope springs eternal, but -- I personally am somewhat of a skeptic, but it will be our responsibility to look for the presence or

absence of the -- of their purloining of intellectual property and other information.

Senator Sullivan: And were any of you gentlemen, or all of you gentlemen, consulted on the terms of the agreement?

Director Clapper: We were aware of the negotiations, but, at least from -- normally, intelligence wouldn't be a voice or shaper of a policy agreement like this between two heads of state. It will -- I think our responsibility is to report what they do.

Mr. Work: We participated in the buildup of the visit, in terms of policy development, et cetera. But, in terms of what went on between the two leaders of the nations, we were not directly consulted.

Senator Sullivan: Admiral?

Admiral Rogers: And I was aware of the ongoing process, and, like Secretary Work, same thing, part of the broad effort in preparation for the visit.

Senator Sullivan: But, you weren't -- you didn't see the terms of this agreement before the --

Admiral Rogers: No.

Senator Sullivan: Did you, Mr. Secretary?

Mr. Work: No.

Senator Sullivan: Let's assume that, you know, kind of pass this prologue, here, and, you know, we were talking

about intellectual property. As you know, our country has been trying to get the Chinese from -- to stop stealing U.S. intellectual property for decades, really. And it hasn't really worked out very well. If -- let's assume that this agreement -- that there is some additional cybertheft that we can attribute to China. What would you recommend the actions of the United States should be, particularly in light of this agreement?

Mr. Work: I wouldn't be able to answer that, as I would have to know what the degree of the activity would be.

Senator Sullivan: Let's say another OPM kind of activity.

Mr. Work: I think we -- the Department of Defense would recommend a very vigorous response.

Senator Sullivan: And, Mr. Secretary, what would you -- I mean, just give me a sense of what that would be. Sanctions, retaliation --

Mr. Work: Could be any of those, Senator. Maybe all of the above. It will depend upon the severity of the activity. But, again, I know this is -- I know this is a big point of contention with the committee. It is -- we are serious about cost imposition, and our statement is, "If you participate in that -- this activity, we will seek some type of measure which imposes costs upon you." And we just do not think it's a proportional cyberattack for a cyberattack.

It might be something entirely different, like a criminal indictment or sanctions or some other thing.

Senator Sullivan: Let me ask kind of a related question for all three of you. How -- and I know you've been discussing this, and I'm sorry if I'm kind of going over areas that we've already discussed, but -- help us think through the issue of rules of engagement here. I mean, we have rules of engagement in so many other spheres of the military that are well established. How do we think through these issues, which I think in some ways are the fundamental aspects of what we do in response to cyberattacks?

Admiral, do you want to take a stab at that?

Admiral Rogers: So, if you look at the defensive side, I'm pretty comfortable that we've got a good, broad recognition of what is permissible within a rules-of-engagement framework.

Senator Sullivan: Do we? I mean, between us and other nations?

Admiral Rogers: I'm -- I wouldn't -- if you define it between us and other nations, I would -- no, I apologize. I thought your question was in a DOD kind of responsive framework.

If you want to expand it to a broader set of nations, then it's probably fair to say no.

Director Clapper: I would agree. I think, when it comes to offensive -- if you're thinking about offensive cyberwarfare, we probably don't -- do not have rules -- defined rules of engagement.

Mr. Work: I agree with what Director Clapper said earlier, Senator, that this really is the Wild West right now. There's a lot of activity going on, both from nation-state actors all the way down to criminals. And so, sorting through each of the different attacks and trying to attribute what happened and who it came from and who was responsible for it all demand specific responses on these attacks.

But, I agree totally with the committee that we need to strengthen our deterrence posture, and the best way to do that is continue to work through these things and make sure that everyone knows that there will be some type of cost.

Senator Sullivan: Thank you.

Thank you, Mr. Chairman.

Chairman McCain: The committee would also like to know when there's going to be a policy that would fit into these attacks and would then be much more easily responded to if we had a policy, as mandated by the 2014 defense authorization bill.

I thank the witnesses for a very helpful hearing. I know that they're very busy, and we -- the committee

appreciates your appearance here today.

Thank you.

[Whereupon, at 11:38 a.m., the hearing was adjourned.]