Stenographic Transcript
Before the

COMMITTEE ON
ARMED SERVICES

UNITED STATES SENATE

HEARING TO RECEIVE TESTIMONY ON CYBER POLICY, STRATEGY,

AND ORGANIZATION

Thursday, May 11, 2017

Washington, D.C.

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

HEARING TO RECEIVE TESTIMONY ON

CYBER POLICY, STRATEGY, AND ORGANIZATION

Thursday, May 11, 2017

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], Wicker, Fischer, Cotton, Rounds, Ernst, Tillis, Perdue, Sasse, Reed, Nelson, Shaheen, Gillibrand, Blumenthal, Donnelly, Hirono, King, Warren, and Peters.

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

Chairman McCain: Well, good morning. The committee meets today to receive testimony on cyber policy, strategy, and organization, of which there is very little.

We are fortunate to be joined this morning by an expert panel of witnesses: General Jim Clapper, who enjoys nothing more than testifying before Congress and is making his second appearance on the Hill this week. I hope you are scheduled for a couple more next week. Anyway, General Clapper, there is a reason why you are in demand and that is because of the incredible esteem in which you are held by Members of Congress. And I know that this is not your favorite activity, but I would argue that this issue deserves your input and your knowledge and background.

Jim Stavridis, who is the Dean of the Fletcher School of Law and Diplomacy at Tufts University and former Commander of U.S. European Command, in which he did an outstanding job. It is not his first appearance before this committee.

And Michael Hayden, Principal at The Chertoff Group and former Director of the Central Intelligence Agency and the National Security Agency. Again, a man of great credentials.

As Admiral Rogers told this committee earlier this week

-- and I quote -- we face a growing variety of advanced threats in cyberspace from actors who are operating with evermore sophistication, speed, and precision. Those are the words of Admiral Rogers.

As with every cyber hearing this committee has held in recent years, we heard how the lack of a strategy and policy continues to undermine the development of a meaningful deterrence in cyberspace. The threat is growing. Yet, we remain stuck in a defensive crouch, forced to handle every event on a case-by-case basis and woefully unprepared to address these threats.

Our hearing today brings together some of our Nation's most experienced and thoughtful national security leaders to help us better understand our cyber deficiencies but, even more importantly, to better understand how we can begin addressing these deficiencies.

A long list of fundamental policy questions remains unanswered.

What is our theory of cyber deterrence, and what is our strategy to implement it?

What is an act of war in cyberspace?

What are the rules of engagement for responding when attacked?

Who is accountable for this problem, and do they have sufficient authorities to deliver results?

Does over-classification undermine our ability to talk openly and honestly about cyber deterrence?

How should we address issues of sovereignty that may or may not apply to data as it moves from country to country?

What about cyber collateral damage?

Organizational questions are equally unresolved.

Should we have a cyber service?

What is the long-term relationship between Cyber Command and NSA?

How should we organize our efforts in the interagency?

Who are our cyber first responders?

No matter how well organized and prepared the Department of Defense may be, glaring gaps in our national cyber policy, strategy, and organization undermine our ability to defend the homeland and deter those seeking to undermine our national security in cyberspace.

While we remain stuck, others have made considerable progress in policy formulation and organizational alignment. For example, the United Kingdom recently established its National Cyber Security Centre, a centralized organization that brings the disparate organizations across the British Government under one roof sitting side by side with industry. I look to the views of our witnesses as to whether we should consider a similar organization in the United States.

Another model worth consideration is an organization akin to the U.S. Coast Guard with its flexible mix of law enforcement and military authorities.

Today we lack true cyber first responders. Neither the Department of Homeland Security nor the Department of Defense know who should arrive first on the scene to stabilize and assess a major cyber attack. We should consider developing a Coast Guard-like hybrid organization that can defend our territorial cyber boundaries, be our first responders, and if necessary, gracefully transition and support DOD, DHS, or FBI, depending on the situation.

Each of our witnesses have written or spoken extensively on how cyber has and will continue to shape our national security. We look forward to hearing more from each of you about the actions we can and should take to defend our Nation in cyberspace.

Senator Reed?

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

Senator Reed: Thank you very much, Mr. Chairman. And I want to join you in welcoming our distinguished witnesses and in holding this important hearing.

General Clapper, General Hayden, Admiral Stavridis all have significant experience and expertise in cyber from their service in the military, the intelligence community, the private sector, and academia. We thank you all, gentlemen, for your service to the Nation.

Russia's campaign last year to influence our election undermined faith in our democracy, and the objective truth of the news has been matched or surpassed by its years' long efforts to undermine democracy and the free press in Europe, the NATO alliance, and European unity in general. Russia's ambitious and aggressive use of information as a weapon adds a whole new dimension and urgency to the task of confronting and deterring hostile actions through cyberspace.

We heard testimony 2 days ago from Admiral Rogers that the Russians are still actively trying to influence our domestic politics and are very likely to attack our midterm congressional elections next year. There is not a moment to lose in addressing this challenge to our national security.

However, as Admiral Rogers also acknowledged earlier this week, Cyber Command's Cyber Mission Forces are neither

trained nor tasked to operate in this cognitive dimension of information warfare.

By the same token, the elements within the Defense Department that are responsible for information operations have no cyberspace responsibilities or expertise.

This disconnect is replicated across the other disciplines that make up the totality of information warfare and across multiple organizations in the Defense Department and the interagency process.

Additionally, I would like our witnesses to consider the advice of the Defense Science Board task force on cyber deterrence. Prominent former officials such as former Under Secretary of Defense for Policy Dr. James Miller served on this task force and have testified to this committee twice this year. They advocate rapidly developing the ability to conduct operations through cyberspace to threaten, quote, what key leaders on the other side value the most, close quote, which in the case of Russia could include their own financial wellbeing and status in order to deter influence operations and cyber attacks against us.

The threats that we face call for leadership and action. To date, however, despite the many large-scale and impactful cyber events of recent years, the executive branch has not acted to create an effective, whole-of-government capability to defend against and ultimately deter damaging

cyber attacks. Congress, challenged by the overlap of committee jurisdictions and concerns of numerous outside stakeholders, has also been unable to design and impose the comprehensive solutions that this problem requires.

However, it is imperative that there be a renewed effort. We must fashion an effective, integrated, and coordinated capability to detect and counter the kind of influence operations that Russia now routinely and continuously conducts. Likewise, we must act to ensure that our military and the government as a whole has a strategy and capability to deter such actions through the demonstrated ability conduct our own operations of this type. And we must also act to bolster the resilience of our society in the face of attempts to manipulate our perceptions and our decision-making.

I know that each of you think deeply about and have recommendations to address these critical issues. I look forward to your testimony and discussion of these urgent matters.

Thank you very much.

Chairman McCain: General Clapper?

STATEMENT OF HON. JAMES R. CLAPPER, JR., SENIOR FELLOW AT THE BELFER CENTER FOR SCIENCE AND INTERNATIONAL AFFAIRS, AND FORMER DIRECTOR OF NATIONAL INTELLIGENCE

Mr. Clapper: Chairman McCain and Ranking Member Reed and members of the committee, first I think I want to commend you for your sustained interest in this subject of cyber and cybersecurity and what we as a Nation should be doing about it.

It is certainly an honor to be on the same panel with the likes of Jim Stavridis and Mike Hayden, both old colleagues and friends.

I had some introductory comments about the threat, but I do not think I will dwell on that in the interest of time.

Chairman McCain: Before you leave the threat, though, General, would you say the threat is worsening, the same --

Mr. Clapper: I do. Since you have asked me, one of the themes that I have talked about in my former capacity at worldwide threat hearings, to include the last one we had here, was the fact that we in the past have taken some comfort in the fact that the entities which can do us the most harm, meaning Russia and China, probably have perhaps lesser intent, and then the entities which have more nefarious intent, meaning terrorists, criminals, et cetera, have lesser capability. The problem is that gap between the two is closing. And so the terrorists, criminals, et

cetera, hacktivists are going to exploit the technology. And so that comfort that we may have taken in the past I do not think is something we should count on. So that is an overall comment about the threat. So the short answer to your question is yes.

And the other comment I would make is I think what to do about all this transcends the Department of Defense and the intelligence community. We have a huge education challenge getting both institutions and individuals to practice common sense cybersecurity, sort of like the same way that we habitually lock our doors and windows, brush our teeth, or hopefully wear seat belts. And there is not that mindset certainly at the individual level or the institutional level.

And so in response to your request for thoughts on policy, strategy, and organization, I want to offer one overarching thought. To me, the first order of business is defense and resilience. We got to focus on this because without it, we will never be in a position to launch a counter-attack even if we can quickly and accurately attribute who attacked us which, by the way, is not in itself a trivial task. And we are always going to doubt our ability to withstand a counter-retaliation. And I saw examples of this during my time as DNI.

One case in point. When the Iranians launched a series

of denial of service attacks against our financial sector -- I think it was in 2013 or so -- the initial interagency impulse was to counter-attack but in a measured, precise way. What restrained us was lack of confidence in our ability to absorb a counter-retaliation. We could not be sure it would be similarly measured and proportional and legalistic, which is the way we do it, or what the second order or third order or unintended effects might be.

So we have to recognize and accept that it is inevitable that we are going to be attacked, and the real issue is how resilient can we be to recover. And in the absence of that resilience and the confidence it gives us, it will continue to inhibit our responses.

And this imperative on defense and resilience applies not just to the Federal Government at large and to DOD and the intelligence community but applies equally to people sitting in the White House situation room or board rooms. So defense and resilience must, in my view, be the pillars of whatever policies and strategy that we adapt. That to me is the very foundation for deterrence.

A related point -- and I have said this before -- is I think accordingly we should use all the tools potentially available to us, diplomacy, economic sanctions, and other forms of military power, when we consider responses to cyber threats. Just because someone attacks us using cyber should

not automatically mean that we should respond the same way. In fact, if the adversary chose cyber because it asymmetrically favored them, responding in kind means we are sort of letting them define the terms of the engagement and fighting on their terms. And, of course, intelligence, by the way -- I would mention this -- has a crucial role to play in identifying ways to leverage a cyber adversary.

With respect to the current posture of the U.S. Government, I would say -- my mild understatement -- it is not very good. Still, many organizations across the government have old, hard to defend IT architectures, and certainly the OPM breach got everybody's attention but it is probably the tip of the iceberg.

One trade publication recently reported that 34 percent of U.S. Government agencies surveyed experienced data breaches in the past year, and 65 percent reported experiencing a data breach at some time in their history. And these agencies cited old systems, lack of funding, and staffing shortages as the cause.

The Trump administration, I understand, is preparing a new executive order on strengthening the cybersecurity of federal networks and critical infrastructure. It emphasizes accountability, managing the government IT architecture as a federated enterprise, and all that. What I expect is, though, that the accompanying authorities and resources will

not match these bold goals.

This leads me to another crucial point. Even if the agencies in the government complied with this forthcoming executive order, both the spirit and substantively, we will still have no recognized standardized way to measure whether we are more secure or not. And to me, this is a major deficiency that must be addressed. The term "cyber metrics" applies to at least six different dimensions of cyber. Do we measure compliance with standards or how much we are spending or what functions we are performing or how we gauge the threat or calculate risk or measure return on investment? There is no consensus on any of these six ways or some combination thereof to measure whether we are actually improving cybersecurity.

On organizational things, you asked about the suitability of the Federal Government's organizational structure. And here I will probably, I am sure, present a contrarian view to my colleagues.

As a general comment, the older I have gotten, the less appealing reorganizations are to me. I say this both as a victim and an instigator of reorganizations. Big ones are hugely disruptive and distracting and take years to gel. The way the government is organized now can work provided that each component has the authorities clearly defined and the resources to perform its mission. So I do not have any

big, lofty ideas on reorganizing the government's approach to cyber.

I do, however, have two related organizational comments that are maybe less lofty but to me important.

First, I feel compelled to repeat something I said last January when I appeared here on the 5th of January, and that is my strong conviction about separating Cyber Command and NSA. If you invite me here to speak about cyber, I am always going to bring that up. NSA is a crucial component of the intelligence community, and I do not believe it is healthy for it to be essentially subordinated to a sub-unified command of DOD.

I was the Under Secretary of Defense for Intelligence when we came up with this arrangement and had a lot to do with it. I believed in it at the time. But it was never intended to be permanent. And this was 7 or 8 years ago.

So I would urge the establishment of a date certain to separate and then work to make it happen. NSA will always have to provide support to the command, but I believe an intelligence agency director should be focused full-time on the mission of their agencies. And again, I repeat NSA is a crucial part of the intelligence community.

The Commander of CYBERCOM and Director of NSA are each a full-time job. And if CYBERCOM is elevated to unified command status, which I believe it should be, then

separation is even more urgent. As the late Johnnie Cochran might say, if you elevate, you must separate.

Second, I do not support establishing a separate cyber service in the military, just as I am not a fan of having a separate space service. I think such proposals, if implemented, would create even more stovepipes, complicate personnel management, and I think make career progression for the people in it harder.

Finally, I have three brief comments on cyber issues in the intelligence community which maybe are a self-criticism.

First, the intelligence community needs to strengthen how it reports cyber intelligence to users with differing perspectives and needs. This means providing reporting to policymakers that is timely and relevant but not head-hurting technical and importantly identifies the so-what implications for action. Intelligence needs to move from reporting cyber anecdotes to a systematic framework that focuses on trends and the big picture.

Secondly, the IC needs to improve its support to State, local, tribal and private sector entities. This requires a better understanding of them and what their needs are. There are probably three kinds of customers for cyber intelligence, policymakers, line or core business people, and IT staffs, which are kind of like the military categories of strategic, operational, and tactical. I think

it would be useful if the IC kind of thought about how they relate to the various customer sets using that analogy.

Third, an always hardy perennial recommendation for the intelligence community is to enhance information sharing. This gets to your point about classification. Yes, we over-classify. No question about it. All I ask, though, is that when we look into this, we do consider the equities from the standpoint of the intelligence community. If we are going to declassify, transparency is always a double-edged sword. It is good but adversaries go to school on that transparency.

The other point I would make here is that information sharing has got to be a two-way street. The private sector is often the first to know of a cyber attack, and so rapid sharing must work both ways. Companies cannot depend on the government to provide just-in-time warning that its intellectual property clock is about to be cleaned. There are some understandable inhibitions on both sides that prevent this, but we must do better.

So with that, I will turn to, I guess, Admiral Stavridis. Thank you.

[The prepared statement of Mr. Clapper follows:]

[COMMITTEE INSERT]

STATEMENT OF ADMIRAL JAMES G. STAVRIDIS, USN, RETIRED, DEAN OF THE FLETCHER SCHOOL OF LAW AND DIPLOMACY AT TUFTS UNIVERSITY AND FORMER COMMANDER, UNITED STATES EUROPEAN COMMAND

Mr. Stavridis: Good morning. Chairman McCain, Ranking Member Reed, members of the committee, again thank you for asking me to come down and speak.

And I think we are facing potentially the most disruptive force in this cyber world, and we have a gaping vulnerability in my view.

I do want to mention that in the course of the panel, I think we are probably not going to agree on everything, but you will be pleased to know we coordinated our hairlines for disagreeing.

[Laughter.]

Chairman McCain: I know how you feel.

[Laughter.]

Mr. Stavridis: You look like a potential donor to me, Senator.

[Laughter.]

Mr. Clapper: Grass does not grow on a busy street. Or as my wife is quick to remind, nor out of a concrete block either.

[Laughter.]

Mr. Stavridis: So I will talk very briefly about kind

of three threat vectors. One is pretty obvious. It is national security. This is what General Clapper has outlined for us. I think the commercial sector is second, and then thirdly we should recall there is a very personal vector to cybersecurity that potentially influences each of us as you think about what that super computer you are carrying around in your pocketbook or purse say about you. So those three vectors I think are merging in a dangerous way today.

There are 7 billion people on the planet, probably 20 billion devices connected to the Internet of Things. And fairly recently we just saw an attack that turned the Internet of Things into an Internet of botnets, creating real havoc in a variety of crucial commercial sites. We have seen hundreds of millions of accounts hacked, most recently Yahoo. We have seen multiple actual thefts occur, $87 million from the Federal Reserve Bank trying to get money from Bangladesh to the Philippine Islands.

On the national security perspective, we see attacks, I would argue, from North Korea, Russia, certainly brushing up against attacks from China. Iran I would categorize an attack. These vulnerabilities come together in two fundamental points. We are deeply challenged. And as both the chairman and the ranking member have said, and as General Clapper has said, we are not particularly well

organized. Yet, we as the United States have the largest threat surface of any nation in the world.

So what do we do about it? I will launch a few ideas. All of these ought to be considered as modest proposals at this time. These are things we should think about doing and have more conversation about.

One I would say I am firmly in favor of -- and I am going to agree with General Clapper on this one -- I do believe that the NSA and Cyber Command should be separated. I have been speaking and writing about this for several years. To me, the jobs are too big. The missions are different. The span of control is a deep concern and rising. And I think Cyber Command should be elevated to being a full combatant command and, as the General says, separated, and I think probably two fundamentally different leaders are needed at those two commands.

Secondly, the idea of a cyber force. Here I am going to disagree with General Clapper. I think we should take a serious look at it. What I try and do at times is reach back into history, and I am mindful that I am flanked by two Air Force Generals. If we were having this hearing about 100 years ago, the Army and the Navy would be adamantly saying, hey, we do not need an Air Force. Why do we want that? We can handle that. Yet, today I do not think we could imagine our military functioning without all that the

Air Force brings to the table. I think cyber is kind of like that, and I think in 100 years we will look back and say, boy, were we really having a debate about whether or not to have some kind of cyber force?

So I would say let us take a serious look at this, whether it is a separate force in the same model as the Army, the Navy, the Air Force, the Marine Corps, perhaps not. A Coast Guard model I think is a very intriguing way to think about this. But I think at a minimum this would be something the Congress would be interested in hearing more views about and recognize, again, looking to the history of the creation of the U.S. Air Force, you are going to get enormous pushback from the Department, from the individual services. And I know Admiral Mike Rogers was just up testifying, disagreeing with the idea as well. Fair enough. Let us bring that debate on.

A second idea I think that is worth thinking about at least is being more demonstrative of our offensive cyber capabilities. I think that would help create more deterrence if we did so.

I agree with General Clapper. We do not need to reach into the cyber toolkit every time we are cyber attacked. But I think in our zeal, appropriate enough, to try and protect the nature of our cyber tools and our sources and our capability, we can lead some to underestimate our

ability to retaliate. Eventually we are going to have to build a deterrent regime of some kind. And so we ought to be having a coherent conversation about levels of classification and how we would want to do demonstrations.

Fourth I would say doctrine. This is always kind of the military bugbear in me. But what is the definition of a cyber attack? I think it is time we really grappled with that, and on a spectrum that runs from nuisance defacing of websites to kinetic demonstrations that actually kill people and destroy massive amounts of material and equipment, somewhere on that spectrum lies what we ought to think about as a cyber attack. I would argue what North Korea did to Sony Pictures, an American corporation, which included kinetic damage and a high degree of business and economic damage does, in fact, verge into an attack, not as was categorized at the time as cyber vandalism.

Sixth -- and then I will kind of stop there because you asked specifically about this -- organizing the government. Taking Director Clapper's views about skepticism of both reorganizations and creation of new bureaucracies, I will put it this way. I think there needs to be a voice in the cabinet that focuses on cyber. Now, you could take the Director of National Intelligence and make that the Director of National Intelligence and Cybersecurity, for example. You could have a new department. We have a Department of

Agriculture, a Department of the Interior. These are important organizations, but they reflect where we were as a Nation 150 years ago. The idea of having a dedicated voice in the cabinet talking about cyber has appeal to me.

I will conclude by saying I had a wonderful career in the military. Now I am an educator. I am the Dean of the Fletcher School of Law and Diplomacy at Tufts University. I have come to value education even more.

And I will close with something the Director said at the beginning. 65-70 percent of the cyber intrusions and attacks occur because of bad cyber hygiene, which is bad cyber education. The more we emphasize science, technology, engineering, math, computer science, coding, the more we have an informed population, the better protected we will be. That may be the most important thing we can do of all.

Thank you for listening to a few ideas. I will close by saying, because I have two Air Force Generals with me, in the world of cyber, we are kind of on the beach at Kitty Hawk. We have got some work to do ahead of us. Thank you very much.

[The prepared statement of Mr. Stavridis follows:]

Chairman McCain: General Hayden?

STATEMENT OF GENERAL MICHAEL V. HAYDEN, USAF, RETIRED, PRINCIPAL, THE CHERTOFF GROUP AND FORMER DIRECTOR, CENTRAL INTELLIGENCE AGENCY

Mr. Hayden: Thank you, Mr. Chairman, Senator Reed. Let me, first of all, violently agree with the diagnosis that both of you laid out in your opening comments. I think you have got the symptoms we are trying to treat here exactly right.

I first encountered this cyber thing more than 20 years ago. I was pulled out of Bosnia, a war that was essentially medieval in its conduct and in its causes, and parachuted into San Antonio, Texas at the Air Intelligence Agency, which was actually on the cutting edge of thinking about cyber then. And I still remember the introduction I got from my staff. They never quite said what I am going to tell you now, but if I boiled it down, it was, General, we are glad you are here. Take out a clean sheet of paper and a number 2 pencil and write this down. Land, sea, air, space, cyber. It is a domain. It is a theater. It is a location. It is not bandwidth. It is not a budget line item. It is a place where we are going to go and operate. By the way, I think that is exactly right and it is now American military doctrine.

I think what we are debating for the next 20 years is what of our life experience and lessons in these domains

transfer or do not transfer into this new cyber domain. So, Senator, you mentioned questions of sovereignty or what is an act of war, what is legitimate state espionage, what are the principles of deterrence. And I could go on. But there is really no consensus yet even within the armed forces as to what experience here still applies up here.

And I think one of the reasons we lack consensus is as a Nation, not just as a military, we lack policy because we lack consensus. We lack consensus because we have not had that adult discussion that we need to have, and we have not had the adult discussion because frankly I do not think we have a common view of the reality, a common view of the battlespace. And that is inhibited, as has already been mentioned by both of you and by General Clapper, by the lack of knowledge, information in this space, over-classification. And before I focus exclusively on the government, let me include industry in that as well because they keep the ball on their hip a lot of times too for their own purposes. And so I do think we need to have far more openness as to what goes on, what our capabilities are, what the threats are, and frankly, exactly what happened.

General Clapper just mentioned the Iranian attacks against the banking system in New York, massive denial of service attacks, but something our government will not go out of its way to actually say has happened with the clarity

that Jim had just used.

Part of the over-classification problem -- and General Clapper and I probably share guilt here -- is that our cyber thinking in the armed forces and in the government is rooted in the American intelligence community. If this had been developed at another part of our structures, I think a lot less of this would be on the other side of the door and a lot more would be open. Of course, without consensus on policy and these basic foundational definitions, the organizational structures that should follow that is always in flux, always subject to debate.

I was, to be fair, present at the creation when we decided to put a Title 10 warfighting function at Fort Meade. It was not quite Cyber Command then. It was Joint Functional Component Command Net Warfare, but I am the first Director of NSA who actually had Title 10 warfighting abilities and authorities under Strategic Command.

Even when we did that -- and I still recall briefing the Chairman of the Joint Chiefs of Staff and he turned to me -- it was General Dick Myers, whom I had known for a long time -- and said, Mike, is this going to solve this. And my response was, oh, no, sir, not at all, but we will be back to you in a couple years messing this up at a much higher level than we are currently. And that has been the evolution. As we develop technology, a trained workforce, a

deeper understanding, the structures will change as our understanding changes.

And so let me join consensus here. I think there is a point in time -- and I do not think it is very far away -- where the structures have to adjust to changing capacities and Cyber Command and NSA have to be separated. That is not a panacea. It is not the philosopher's stone. It is not going to turn digital lead into digital gold for us, but I think it is a powerful step forward.

Senator McCain, I was really intrigued by your comment about perhaps the U.S. Coast Guard is a workable model. I actually joined an effort by the American Enterprise Institute about a year and a half ago that actually tried to seek how should we organize as a government not just as the armed forces to deal with the cyber domain. And the Coast Guard model really does offer some interesting examples. It is an educational organization. It is dedicated to public safety. It is a first responder. It conducts search and rescue. It is a law enforcement element of our government and in extremis, we can use it as a combat arm of the American Government. Obviously, it does not transfer perfectly, but I do think there is some really interesting parallels here that we could profit from as we try to move forward and create a whole-of-government response.

Again, one more time, let me join consensus. The Coast

Guard is an intriguing model because it straddles government and private sector. We really do have to do that in terms of cybersecurity. So any model that allows us to put our arms around the private sector where, frankly, I think most of these battles will be won or lost, is one that we should pursue.

I look forward to your questions and learning a great deal from my colleagues here.

[The prepared statement of Mr. Hayden follows:]

[COMMITTEE INSERT]

Chairman McCain: Do you think the private sector is eager to cooperate?

Mr. Hayden: The private sector gets it as victim. This is life experience. I am out of government 8 years now. When I first started talking with them, we were a nuisance talking about cybersecurity. They now know that cybersecurity is not a subtraction from the bottom line, but it is integral to the top line. That part they get.

What they have not yet embraced is that they could enter into a deeper relationship with the government that would not inhibit either their financial or their cybersecurity success. And so the burden of proof might be a bit more on us than on them.

Chairman McCain: I get the impression that a lot of these particularly major Silicon Valley corporations would like to stay as far away as possible from the Federal Government.

Mr. Hayden: Senator, we are probably still feeling the after-effects, the second and third order effects, of the Snowden revelations and so on. And I would have agreed with you more strongly 2 or 2 and a half years ago, but in my recent dialogue with them, I do see a shift. Let me give you an example.

I will be a little oblique here. Vault 7, which was allegedly an awful lot of CIA cyber tools going public. We

have not seen Silicon Valley rending their garments in outrage about this. I think their response to this has been far more mature, far more understanding of the appropriate role of government than we saw 2 or 3 years ago.

Chairman McCain: Thank you.

I take it our witnesses agree that until our adversaries believe the consequences of an attack in cyberspace will outweigh the benefits, behaviors will not change.

Mr. Stavridis: Yes, sir.

Mr. Clapper: Yes, sir.

Mr. Hayden: Yes, sir.

Chairman McCain: Every event is being handled on a case-by-case basis. Is that appropriate or sustainable?

Mr. Clapper: That is true, but I think that is a swing at me from the prior administration. Every case is a little different, at least for the cases we encounter. It would be nice to have a broad policy, though, that you could start with, which we really do not have.

Mr. Hayden: Let me go deeper than Jim. In the Bush administration, we could not do a cyber thing without having a meeting in the situation room.

Chairman McCain: What are the impediments? There is a common refrain here, constant refrain, we do not have a strategy, we do not have a policy, therefore, we have huge

problems. What is the impediments here? What is keeping us from -- the last administration and then the administration before that were all good people. They all understood the threat, but yet, we have not developed a policy or a coherent strategy. Is it a lack of leadership? Is it a lack of focus? Is it a lack of evolving technologies? What is the problem here? I am not sure we can solve it without defining the problem.

Mr. Clapper: I will take a try at that, although I do not think it will be satisfactory to you, Senator McCain, is what I tried to get at in my statement about lack of confidence in our ability to absorb a counter-retaliation. And that is why to me, if you are going have a serious discussion about deterrence, the fundamental underpinning of deterrence has got to be defense and resilience. And unless we are confident that we can withstand a counter-retaliatory action, which may not be as measured and precise as we might employ, having a serious discussion and writing things down in the absence of that is pretty hard.

The other thing I ran into, not to sound like an excuse here, but are legalities. I think Jim mentioned the Sony attack. And of course, putting aside the issue of whether that impacted the national security of not, the First Amendment I guess, so if we consider only using the single domain of cyber to retaliate, then the issue comes up, well,

we have to execute and attack through someone else's infrastructure in order to get ultimately at the target. Is that an act of war against that intermediary or not? And lawyers have a field day with that kind of an issue.

So in the end, in the case of Sony, we ended up not doing anything in the cyber domain but using other tools, sanctions against North Koreans, which for me were ceremonially satisfying but really did not have a lot of impact.

So those are the complexities. It sounds legalistic and bureaucratic, but to me, those are the kinds of things that have inhibited us.

But the main point I would make is that unless we have confidence in our ability to absorb an attack and be resilient, it is always going to inhibit a single domain response, that is in cyber. That is why I mentioned using all the other tools.

Mr. Stavridis: Senator, if I could, Chairman McCain. I think those are salient points.

I would add back to this theme of education. For the Senate Armed Services Committee, the question becomes are those in the military under the purview of this committee receiving enough computer science. Are each of the academies training to this, the ROTC programs? Over time, I think some of these problems will be solved simply by

demographics, as younger people who are digital natives come into positions of authority. But I think that is part of the problem we are trying to solve here.

Mr. Hayden: Senator, I would just add one thought. I totally agree with Jim's analysis about our defense. We self-deter because we do not understand how well we could deal with the second and third steps.

But with regard to what is legal, what fits policy, the problem is we do not have any case law. We do not have any generalized recognition of what constitutes accepted international practice.

One way to create accepted international practice is to practice. We actually have the opportunity to establish case law. We have the opportunity to begin to set out what is accepted international practice. And I would suggest a country like ours with checks and balances and transparency would be doing the world a service by creating an accepted regime in this domain by prudently using some of the capacities we have.

Chairman McCain: Well, I thank the witnesses.

On the issue of the cyber corps, or whatever you want to call it, I do not know if we ought to establish that. But right now I do not see a clear career pattern and a path to success for these very valuable individuals who have these special talents, maybe not to be a fighter pilot or a

tank commander, but to be able to engage in this hand-to-hand combat that we are involved in. Again, I am not sure whether it is a cyber corps, but we better establish a path and incentives for people to engage in countering what we all agree is a major threat to American security.

Senator Reed?

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

Thank you, gentlemen, for your excellent testimony.

And just a quick follow-up, General Hayden. We can make some law by doing things that are accepted either explicitly or implicitly by the intelligence community. We also can sit down and try to essentially do an agreement. We did it with the financial world after World War II with Bretton Woods. And I do not sense any effort anywhere to try to do that. Am I missing something?

Mr. Hayden: There has been an effort. Actually Michele Markoff at the State Department, who takes the Acela up to New York routinely and tries to use the U.N. to transfer the accepted laws of armed conflict here and transfer them up here into the cyber domain -- and she has been somewhat successful.

Beyond that, though, Senator, I think the real issue we have is there is a big chunk of the world -- and some of it comprises our friends -- a big chunk of the world who consider cybersecurity preventing that for which we think we

have the Internet in the first place, which is the free flow of information. Their definition of cybersecurity is control of data entering into their sovereign space where ours is quite different. And so we run headlong into this lack of consensus. Hence, my approach to begin to create a normative regime established in essence by practice by a prudent, law-abiding nation.

Senator Reed: With respect to a normative regime, as I indicated in my opening statement, the task force on cyber deterrence suggested that we develop the ability to hold at risk key aspects of potential opponents or adversaries, including in some cases the individual wealth or the individual status of potential opponents.

Is that something that is in this concept of trying to establishing the rules of the road, General Clapper?

Mr. Clapper: Well, I think what you are getting at -- at least it conjures up in my mind, Senator Reed -- is the notion of using sanctions, economic sanctions, to leverage identified cyber opponents.

Senator Reed: I think you could almost go further than that of using as cyber operations to literally go after the resources and the finances of individuals.

Mr. Clapper: Sure, I think that would be useful to have in the toolkit.

Senator Reed: And again, going back to the point that

General Hayden made, if we have it in the toolkit, we never use it, it is not seen as deterrence. Do we have to use it at some point?

Mr. Clapper: Well, yes. And of course, you kind to come to think about why does the nuclear deterrent work. And it has so far -- knock on wood -- for 70 years. But that really is not a very good comparison when you think about it because they are different, and there are only nine countries that have that. And the fact that we have not, no one has used nuclear weapons 70 years in itself -- and the problem with cyber it is so ubiquitous, it pervades so many aspects, and there are so many things that go into the cyber world that do not merit -- you know, they are annoyances, and they do not merit certainly a nation state response. So those comparisons to me are not very satisfactory.

Senator Reed: Admiral Stavridis, your comment.

Mr. Stavridis: Just to pick it up, as I was saying earlier -- and I think this is where General Hayden and I are on the same page -- using an appropriate, demonstrative, offensive capability can have a wonderfully clarifying effect on the minds of your enemies. And I think it is time to lift the veil a little bit. Finances are one thing, I think absolutely. And I think another is military forces, not the nuclear forces, though, should be off the table, but showing that we have real capability against nation state

actors I think it is time to strongly consider some form of that. Again, as General Hayden says, it builds a regime in international law that I think would be salutary.

Senator Reed: Just a final point. I think your comments clearly reveal that we have significant vulnerabilities, particularly on our civilian sector. We have done a lot more for the military, but we could do much more. But when we come to the civilian sector, it is quite vulnerable -- our critical infrastructure.

And it seems to me there are a couple of paths to pursue. One would be pass laws, regulations, require them to do this or that. And second is to use the insurance market perhaps to get them to include in their operating costs the costs of protection. And one element is insurance -- we have the terrorism reinsurance initiative, which is essentially designed for structures that might be destroyed. But I think we are getting to a point in the world where the structures are less vulnerable in some respects than the electronic infrastructure. But, again -- quickly because my time has expired -- are there any thoughts?

Mr. Clapper: If I could just foot stomp something that Admiral Stavridis said, which is the huge importance of education. At my headquarters, just ODNI, Office of the Director of National Intelligence -- and you know, this is composed of intelligence professionals that understand the

threat. Yet, the only way we could improve their sensitivity to spear phishing, you know, a fairly common thing out there, is to test and then throw up the results on the screen once a week at the staff meeting, embarrass the senior leaders about your folks need to be better educated, and we just keep testing and the grade scores would go up. Well, we do not do that. And to me, it is just fundamentally important that institutionally and individually, there needs to be better recognition and better education about the threat.

Mr. Hayden: Senator Reed, can I just double down on the cyber insurance question?

Senator Reed: With the chairman's permission.

Mr. Hayden: That unleashes a business case for businesses to actually increase their cybersecurity without the negative effects of a compliance mindset coming out of government regulations. So anything the Congress could do to make that more possible, whether it is second insurer or other aspects of the insurance industry, I think would be a real plus.

Senator Reed: Thank you.

Mr. Stavridis: I agree with that, and I want to be on record as such. Thank you.

Senator Reed: Thank you.

Chairman McCain: Senator Wicker?

Senator Wicker: Admiral Stavridis, give us an example scenario of how we would demonstrate openly our offensive cyber capability.

Mr. Stavridis: Following an intrusive attack into our electoral process, bank accounts disappear from leading Russian oligarchs who are connected closely to the regime, sort of level C; government officials, many of whom are moving money offshore in Russia, level B; or go after Vladimir Putin, level A. You want to think very carefully as you go up that ladder of escalation, just like you do with traditional --

Senator Wicker: Go after Vladimir Putin specifically how?

Mr. Stavridis: Two ways. By attacking his accounts and diminishing them or by simply revealing them to his people. You are currently seeing Prime Minister Medvedev under enormous political pressure in Russia, a whole series of demonstrations around the country tied to revelations about his offshore financing, his yachts, his multiple luxury goods. That kind of reveal I think would have a salutary effect.

Senator Wicker: And General Hayden, are you wanting to jump in there?

Mr. Hayden: Yes, just very briefly. Jim wrote about this right after the attacks became public, and one of the

other ideas I think that was contained in his original article is so you have the Russians attacking the foundations of American democracy. So we return the favor. We use cyber tools to attack the foundations of Russian autocracy, which is the ability of the Russian surveillance state to track its own citizens. So pushing in a covert way tools into the Russian cyberspace that make it more difficult, anonymizing tools to make it more difficult for their security services to follow their own citizens demonstrates the cost to Putin of his fooling with our processes.

Senator Wicker: And, General Clapper, what might the counter-response be?

Mr. Clapper: Well, you preempted me, Senator. I am all for doing this, but there needs to be also due consideration for what the potential counter-retaliation might be. And of course, while we think in terms of very specific attacks, Putin's bank account or the oligarchs' around him, they may not react in kind. That is not to say not to do it. It is just that we need to consider what the potential domain or expanse of -- what the space would be that they might retaliate against us. And ergo, my point about resilience.

Senator Wicker: For instance, how might they?

Mr. Clapper: Well, they could go after our critical

infrastructure, for example, unrelated to the fairly narrow attack we might mount using Admiral Stavridis' example. That is not to say that, well, let us go after President Trump's bank account or something. That would be pretty big. It may not be a good example. But anyway, we cannot --

Senator Wicker: Or General Clapper's bank account.

Mr. Clapper: Well, that will be trivial.

All I am trying to say is we cannot count on an equal or symmetrical counter-retaliation if we retaliate. That is not to say we should not think about it and consider it. All I am asking or plugging for is that we also consider about what the total space might be for a response.

Senator Wicker: General Clapper, you felt that the response in the example of North Korea was unsatisfactory. What might we have done other than sanctions, which you viewed as ceremonial, that might actually have helped the situation?

Mr. Clapper: Our leverage, U.S. direct leverage, over North Korea is kind of limited. You know, we are pretty much out of Schlitz on direct binary sanctions. And, of course, what we have tried to do is to influence the Chinese, who do have some leverage over the North Koreans. What we wanted to do, of course, was to counter-attack. And we knew what it was because it was attributed exactly. But

then you run into the complication of you have to go through another country's infrastructure to get to the target. And we were inhibited from doing that primarily from the standpoint of -- again, this gets back to the definition of what is an act of war. And would that have been an act of war against a third country?

Senator Wicker: Quickly. We have talked about state actors and then non-state actors. How expensive is it to be in this business, if you are a non-state actor?

Mr. Clapper: How expensive is it?

Senator Wicker: Yes.

Mr. Clapper: Not very. Not very. If you want to roam around the dark Web and acquire tools and capabilities, it is not all that expensive.

Senator Wicker: So how expensive would it be for our government to gear up significantly in this regard?

Mr. Clapper: To gear up for an attack?

Senator Wicker: Well, to be more of a major player and to get organized and do what has been recommended at this table.

Mr. Clapper: Well, I do not know. I cannot answer the question, how much it would cost. I just would again foot stomp. I am sorry to sound like a broken record, but to me I do not think it is within the realm of possibility to completely foreclose a counter-attack. If we attack, we are

going to be counter-attacked I would guess, and we need to be prepared for that eventuality. I guess what it does say, if we have money to invest, we need to think about defense first before we get off on all of the offensive tools which we are going to be inhibited from using unless we are confident in our resilience.

Senator Wicker: Thank you, gentlemen.

Chairman McCain: Senator Shaheen?

Senator Shaheen: Thank you, Mr. Chairman.

And thank you all very much for being here.

I just want to follow up a little bit on the whole issue of sanctions because, as you said, General Clapper, you felt the sanctions against North Korea were not very satisfying. That is kind of how I felt about the sanctions that we did against Russia after the elections. They were not very satisfying.

On the other hand, there is a much more comprehensive sanctions bill that is sponsored by Senator McCain and has bipartisan cosponsors that would go after the energy sector, for example, and some of the financing in Russia. Do you think that would be a better way to hold Russia accountable for what they did?

Mr. Clapper: Well, it would certainly convey a message to them, no question about it. But again, what will they do in response? I am all for sanctions --

Senator Shaheen: Well, it is not a cyber response.

Mr. Clapper: And the sanctions that we have imposed particularly after Ukraine were effective. They probably lowered the GDP of Russia 2 or 3 percent. But, of course, the major problem Russia has is the price of oil going up and down. That is really what affects them.

But I think we could do and could have done more targeted sanctioning against certain figures in Russia. I do think kicking out 35 intelligence operatives and closing the two dachas was a great first step.

Senator Shaheen: I agree.

Mr. Clapper: But I would have like to have seen more.

Senator Shaheen: But I understood you all to say that if we do not take action in response to what has happened, whether it is Russia or North Korea, that we will continue to see these kinds of intrusions.

Mr. Clapper: Absolutely. And that has been the pattern. You know, there has been an insidious increase. As adversaries, whether a nation state or a non-nation state, they are encouraged to push the envelope, and how much can we get away with? And if there is no reaction, they will keep pushing that envelope.

Mr. Stavridis: I will just add a way to think about this is the old saying if you live in a glass house, you should not throw stones. I do not agree with that in this

case. We do live in a glass house. I think we need to throw a few stones, or we are going to see more and more of this and it will ratchet up over time.

As to the point about being unable to go after somebody because it goes through another nation's server setup, I take the point. I would counter by saying we fly Tomahawk missiles over other countries' airspace pretty consistently when we want to go after a target. So while I understand the legality piece of that, I think tactically that is not an insurmountable barrier.

Mr. Clapper: And we do not do that over China or Russia.

Mr. Hayden: That was one of the issues I was suggesting of what down here applies up here. So I can offer just an hypothesis. Does a server in Malaysia enjoy as much Malaysian sovereignty as the building it which that server is located? And the fact of the matter is I have seen very good legal minds take that on, and the answer is, no, it does not because it exists up here. In addition to its physical location, it also exists up here in this global commons, as if it were in space or at sea.

Senator Shaheen: Well, I think it is no doubt that our legal framework has not caught up with our technological framework.

And I would go to your point, Admiral Stavridis, about

education. I think one of the challenges is that this a topic that is so foreign to so many people that they do not have any idea how to address it. I mean, witness the audience at the hearing today. I think that is an example of that.

And one of the things that struck me reading about the hack into Macron and the French elections was how simple the response of the Macron campaign was to what Russia was doing. They only had 15 people, and what they figured out was if they put out a lot of decoys basically with a lot of information, that it would really blunt that attack. And so I think part of our education effort needs to be to explain to people that this is not as complicated as it seems and in terms of personal security hygiene.

But could government, knowing that the aversion to regulation that we have -- would it not be possible for us to require any system that could be hacked that is sold to the government to have certain security requirements that would make it difficult to hack? Is that an option that we should be thinking about?

Mr. Hayden: Absolutely, ma'am. And what that does because the government is such a big consumer, the water level of security in the country then goes up.

Mr. Clapper: And also to be religious about somehow mandating staying up with patches. Whenever there are

changes, make sure that those are updated and somehow making that mandatory.

Senator Shaheen: Let me just ask a final question, if I could, Mr. Chairman, and that is, what is the current or potential cyber threat to this country that you all are most concerned about?

Mr. Hayden: I will jump in first. There is always a possibility of the apocalyptic attack, turning out all the lights east of the Mississippi. That is not where I focus. I cannot say that is zero. So, ma'am, if I draw a chart here in the ether between us as to how bad could it be, Hayden, and this arm is, yeah, but how likely is it, where I end up with is kind of Sony North America plus what the North Koreans did against Sony North America, perhaps enriched by new technology and more aggressiveness in the 2 years. So that is kind of my circle as most likely, most dangerous right now, which if done in sequence over multiple firms, I mean, that is a foreign government attacking a North American firm to coerce its behavior. Wow.

Mr. Stavridis: I am just going to add to that. Even though I agree completely with the General that the likelihood is low, I think the grid is very vulnerable. And I think that is worth spending more time to my other General's point about resilience because that is really the dark end of the spectrum, as General Hayden says.

Mr. Clapper: I think your question was most likely. I worry about the worst case, which is an attack on our infrastructure. And I think the Russians particularly have reconnoitered it and probably at a time of their choosing, which I do not think right now is likely, but I think if they wanted to, they could do great harm.

Senator Shaheen: Thank you all very much.

Thank you, Mr. Chairman.

Chairman McCain: Senator Fischer?

Senator Fischer: Thank you, Mr. Chairman.

Thank you, gentlemen, for being here today.

As the chairman said at the beginning of this hearing, many of us on this committee have talked for years about the need for a strategy and policy and a definition of terms basically. I think, Admiral, we continue to struggle in defining some key terms when it comes to cybersecurity. And in your statement, you mentioned establishing a solid doctrinal foundation, a common vernacular for cybersecurity policy throughout our government.

General Hayden, you spoke about we have the opportunity before us right now where we can establish some case law internationally, a normative regime.

On an international stage, what are the consequences for our reluctance to move forward in establishing those terms, and how do you view the leadership of the United

States in this process? I would ask you all to comment on that please.

Mr. Hayden: We suffer from a lack of internal consensus, and therefore it is hard for us to begin to build outward from that. If you are asking so if we were to go do that, how would we do that, my instincts are you begin within the Five Eyes community, likeminded English speaking democracies. You develop a consensus there, build out to maybe the G-7 countries who have real skin in the game in terms of cybersecurity, and then maybe out to the G-20. And if you get broad normative consensus, not treaty consensus, in those groupings, then I think you have established international norms.

Keith Alexander, my successor at Fort Meade, had a wonderful to a question to a group once. Is there anyone in this room who knows a redeeming social value for a botnet? Of course, the answer is no. I mean, we can establish normative behavior that if you have a botnet on your network, it is kind of like you have biological weapons. There is no good reason for you to allow that to continue. Again, it requires consensus on our part and building out from that consensus to likeminded nations.

Mr. Stavridis: I agree with all that. I will add to it. Over time when you really want to build that out, there is kind of a rough analogy, Senator, to what we did in the

oceans in the creation of the Law of the Sea. You will recall before the 1980s, some nations had 200-mile territorial seas. Others had 3 nautical miles. Crazy claims were coming into place. The international community came together and created a Convention on the Law of the Sea. There is long back story about U.S. involvement there we will not go into at this hearing. But the point is the international community eventually is going to grapple with this in some form or another.

The botnets are like pirates at sea. Nobody wants them. There are real demand signals emerging for more organization. We do not want to outsource this to the United Nations. We do want to build it from the inside out.

Senator Fischer: So you agree with General Hayden when he said it is up to us, that we have to establish it first.

Mr. Stavridis: Emphatically.

Senator Fischer: And before you speak, General Clapper, in the NDAA we have included some things on cyber mostly to train, equip a force. But do you think this burden lies on us here in Congress, or does it take leadership from an administration willing to step up?

Mr. Stavridis: I take the easy way out. It is both. You have to have a driver at the other end of Pennsylvania Avenue, but you have a role, obviously, in the ultimate disposition, as well as at times driving the other end.

Senator Fischer: And defining it? Thank you.

General Clapper?

Mr. Clapper: I was just going to strongly endorse the Air Force guy, but I think the Law of the Sea is a great metaphor. And I would also point out that took years and years, decades, hundreds of years to evolve. But there is a pretty sophisticated set of laws that seafaring nations generally abide by, and I think that is not a bad basis for thinking about the cyber domain.

So could we prevail upon countries to not attack civilian targets, for example, which would be to everyone's mutual advantage?

I think the United States must take the leadership here if for no other reason than the dominance of the United States in the technology and as much of the world's infrastructure that originates here or passes through this country. And so the obvious international leader here has got to be the United States.

Senator Fischer: Thank you.

Thank you, Mr. Chairman.

Chairman McCain: Senator King?

Senator King: Thank you, Mr. Chair.

First, I want to say this is one of the most informative and interesting and important hearings that I have attended in this or any other committee. I want to

thank all three of you. It has been very provocative.

On Senator Wicker's question about cost, remember he was saying what it will cost. Just a rough calculation, for the cost of one jet aircraft, the Russians can hire 4,000 hackers. I mean, what the Russians did in our elections was warfare on the cheap. I mean, it was very low cost and very disruptive. And I think that is part of the new reality that we are facing here.

I think Senator McCain asked a relevant question. We keep talking about a policy and a doctrine, and it never seems to happen. In my view, the major impediment is the structure which is so cumbersome and confusing and overlapping and dispersed that that produces cumbersome, overlapping, and dispersed policy. Structure is policy in my experience.

And I think this really has to start with the only centralized authority we have in this country and that is the President. It has got to start with the direction from the President that we are going to have a policy. We are going to call together the intelligence community, the defense community, Homeland Security, and we are going to develop a policy and a doctrine.

I think the other piece that is very important that you have talked about is digital literacy. I think it needs to start in the third grade. Every American child at some

point in their youth starts carrying around a computer, and they have got to be educated. In Maine, we have a very extensive -- computers in our schools. Every middle school student in Maine has a laptop -- every seventh and eighth grader in the whole State. And we call it digital literacy, digital citizenship. And people need to understand how to block their doors.

I was really struck, Admiral, by your statement that 65 or 70 percent of the attacks are essentially preventable. And that is really a huge -- our education has not caught up with it. We teach kids how to do things in day-to-day life, but we got to teach them how to distinguish truth from fiction on the Internet. My wife has a sign in our kitchen that says the problem with quotes on the Internet is it is difficult to determine if they are authentic, Abraham Lincoln. And you know, we have got to be teaching those things.

Deterrence. I completely agree. And we are all aging ourselves, but the relevant case to me is Dr. Strangelove. If you have the ultimate deterrent device but do not tell anybody, it is not deterrence. It does not work. Dmitri, why did you not tell us? Well, we were going to wait until May Day or something like that.

And then finally, there is a question in here somewhere. General Hayden, I think we have really got to be

thinking hard about how we integrate with the private sector. Around here we always talk about whole-of-government. This has to be whole-of-society. And the business community is very suspicious of government. They are worried about regulation. They do not want the Federal Government telling them what they got to do in their networks.

Give me some thoughts about how we can bridge that gap because if we do not, it is the private sector, it is the grid, the financial system. That is where the bombs are going to fall, in effect. And that is why there has got to be more communication and cooperation, it seems to me, or it is just not going to work.

Mr. Hayden: Two very quick thoughts, Senator.

One, back to Senator Reed's comment about insurance. That is a far more attractive approach to the business community for the government to assist, support, unleash business to have better security through a return-on-investment model. That is one.

Second, back to my hand puppet here, all of our cultural habits in the executive branch and in the Congress are that the government has primary responsibility, the government is in the lead in terms of providing safety in physical space. And therefore, the private sector is always subordinated to the government. That is our habit of

thought. The government tells the private sector what it is it has to do. That may not actually be a suitable model for this. This is a place where the private sector might actually have a larger chunk of the responsibility for security --

Senator King: In my experience, the private sector overestimates their invulnerability. If you ask any utility in the country, they will tell you we have got it covered. We are okay.

Mr. Hayden: Perhaps because I am consulting with them and they want help, I see a different picture that they do recognize the issue.

And so, for example, we talk about classification. We just got to get better at metering out formally classified information to the private sector. Yes, I get that. But you realize that is embracing the old model where the government is in control of what information is shared. And I think, given enough time, I can think of seven or eight examples where it is not about making the old model, government is on lead, but we will cooperate more with you, work better. But perhaps changing the paradigm that in all but the most extreme cases, we are going to win or lose a cyber engagement based upon the private sector's performance. So now it is about liberating, unleashing, removing liability, and a whole bunch of other things that

would make the private sector more self-reliant and frankly probably a better partner with the government.

Senator King: I think one thing that the government can do -- and General Clapper mentioned this in his agency -- is red teaming the dickens out of this, in other words, trying to break in and showing people where the problems are, whether it is within government or within the private sector.

Mr. Clapper: Two other points just to reinforce what Mike just said is, first of all, the private sector could well be the first line, you know, the DEW line, to use a Cold War -- a distant early warning line could come from the private sector that would know about an attack, particularly the beginning phases, before the government might.

The other thing is the government cannot fully understand what is really important to the private sector segments. And so there has just got to be a better dialogue.

Now, having said that, I have to plug the Department of Homeland Security because I do believe it should be the interface with the private sector, not the spy community directly. We need to support that, but there needs to be that buffer because there is concern, sensitivity, maybe some of it well justified, about the spy crowd doing that. But there needs to be a more robust partnership between what

the government, which cannot necessarily dominate this -- and I completely agree with what Mike said, that the paradigm here may be different.

Senator King: Thank you.

Thank you, Mr. Chairman.

Chairman McCain: Senator Rounds?

Senator Rounds: Thank you, Mr. Chairman.

Gentlemen, first of all, let me begin just by saying thank you very much for your service to our country.

I am just curious. If we had it to do over again and you could start right from 20 years ago and you were going to establish how we affected this domain, would you share with me, if you could begin at that time, what you would look at in terms of how we would establish this today? Where would we be today?

Mr. Hayden: So I had something of this question when I got to NSA. That is 1999. And I thought I was being overly dramatic by going to the private sector to do our IT system. So we actually went to the phones, the computers, the network that for me by 2001 was actually being run by the private sector. And my thought was that is good. That is an appropriate role. It would be inappropriate to more deeply involve the private sector in the mission aspects of what it was we did at NSA.

I may have low balled that. That may have been a bad

judgment. In other words, as we are breaking new trail here -- I began this more than 20 years ago. So in the mid-1990s, we probably should have more aggressively pushed not to extract private sector technology -- we did that all the time -- but to engage the private sector, particularly in the defensive aspect of this, out of the gate, that this is going to be won or lost based on their performance.

Mr. Stavridis: I would add I take General Clapper's point. I think we would probably have centralized this in one entity. DHS did not exist then, but let us hypothesize that it did. I think you would probably start off with a more centralized function in the government. I like General Hayden's points on private/public.

As I mentioned in my initial thoughts, I would certainly consider building some kind of a cyber corps, a cyber service, a cyber first responder force. I would also add look at the very beginning at the international aspects of this. We are flying that airplane and trying to do significant reconstruction on it. If we could get the international community together. I think there are lessons in all of those for today as well, Senator.

Mr. Clapper: Well, let me contradict what I said in my statement about if we could go back 20 years plus and start with a blank piece of paper, I think the notion of a cyber guard service, patterned somewhat after the Coast Guard -- I

am not even sure it needs to be a uniformed or could be a uniformed service. It may be better if it were not. I do not know. But that notion I think does have functional merit, and it would have been a lot easier had we grown that from the get-go when all of this started. But as always, hindsight is 20/20.

Mr. Hayden: Can I just add to that, Senator, very quickly? And this is my talking about myself because I did this.

We can be fairly accused of militarizing the cyber domain. It was our armed forces that went there first. As I said, it is a domain of operations rather than this global commons. What Jim just suggested if we had been smart enough in the 1990s to have begun this with the Coast Guard-ish model, we may actually be in a better place globally than we were by using the Department of Defense model.

Mr. Stavridis: A lot of this is how you think about it. So General Hayden has been using his hand puppet all morning. And I agree with that.

I think another way to think about it is like an iceberg. And the tip of the iceberg is really what the government can do. The mass of the iceberg here is really the private sector. If you hold that image in your mind 20 years ago, you would be in a very different place today.

Mr. Clapper: 85 percent of the critical infrastructure

in the United States is in the private sector.

Senator Rounds: The Defense Science Board made it pretty clear that over the next 10 years, we are going to have to be able to deter those near-peer competitors because regardless of how hard we try, we can make it more expensive for them to get in. But we are not going to be able to necessarily stop them. Our defensive capabilities simply will not meet their offensive capabilities. And there has to be a significant price to be paid for getting in. Agree or disagree?

Mr. Clapper: For me, listening to what you just said, again, I am being a broken record here, but it emphasizes the importance of resilience in my mind.

Mr. Hayden: I would just add do not confine your concept of defense as reducing vulnerabilities or defending at the perimeter. The best minds in this now in the private sector -- it is presumption of breach. They are getting in. Get over it. Fight the fight. It is about discovery, recovery, response, resilience, not about the preventing penetration.

Mr. Stavridis: And if we can shift analogies yet again, think about it medically. If you go into a place with ebola, today we go in with moon suits to try and protect our perimeter. The fight of the 21st century is inside the body. It is antibiotics. It is finding the

immunotherapy. It is knowing that you are going to be infected. How are you going to deal with it medically in the aftermath?

Senator Rounds: Thank you. My time has expired.

Thank you, Mr. Chairman.

Chairman McCain: Senator Peters?

Senator Peters: Thank you, Mr. Chairman.

And thank you, gentlemen, for very insightful testimony as always. I always appreciate your comments.

I will just, before I ask a couple questions, pick up on a comment. Admiral, you mentioned the 65 and 70 percent of attacks with proper hygiene. As you were saying that, it reminded me of a recent trip I had to Microsoft with their cyber folks there and a statistic that was my main takeaway from it was that they said that if you buy a computer at your local store and plug it into the Internet and you do not put any kind of software protections against viruses, that that computer will be infected within 17 minutes, which is pretty frightening and should be a real clarion call to everyone why this hygiene is so important. In 17 minutes. Just doing your normal Internet stuff, in 17 minutes it will be infected. And that is the magnitude of the threat that we face particularly in the civilian side as you mentioned.

I want to continue to follow that line of thought because I think that is my major takeaway from this meeting

as well. And when you were asked, all three of you, the number one threat, each of those were in the civilian sector. They were critical infrastructure. It was the Sony attack. It was the grid. It was infrastructure generally.

And you also talked about the silos and the concerns. I know, General Clapper, you talked about concerns of silos if we have a different command as well.

But I also appreciate your comments about how the Department of Homeland Security needs to be intricately involved in this whole aspect.

So my question is, given the dual nature of how we deal with this threat with the FBI and Homeland Security, Department of Defense, what do we need to do to bring that collaboration together? And is that perhaps part of this new cyber command, however it may be constituted, to involve kind of a real paradigm shift when it comes to different agencies that have these different kinds of responsibilities? And would the FBI be part of it, for example? Or what are your thoughts about what that would look like to incorporate some of our homeland security elements? And to all three of you actually.

Mr. Clapper: Well, let me start. I guess I am the most recent graduate of the government. That is something actually we worked at pretty hard trying to graphically portray what the respective responsibilities are. I mean,

the FBI, for example, hugely important. Of course, it all starts with attribution because then that determines the government response.

So if it is a criminal hacktivist that is in the United States, the first question, where is this coming from. Is it coming from overseas? Is it coming from a nation state? Is it coming from a non-nation state entity overseas, or is it coming domestically? And the way we are currently organized and the way our laws govern us, there is a division of effort here among those players.

And that is why the Department of Homeland Security I think is actually a very prominent player both for interface with the civilian sector and for resilience, you know, being the cyber FEMA, if you will. When we have an attack -- it is inevitable we are going to have them, and if it is of a sufficient magnitude, we have to have a mechanism for resilience, for recovery.

And so I do think -- that is why I alluded to this in my remarks -- that the setup we have today can be made to work provided people have the authorities that are supported by the Congress and the resources to discharge their respective responsibilities.

Mr. Stavridis: I agree with that.

Mr. Hayden: All true.

A couple of additional thoughts. Number one, you got

to man up. The Department of Homeland Security is notorious for having vacancies in senior leadership positions, particularly in the cyber aspects of it. So good talent there for extended periods of time.

Second I think is to end any sense of competition between Homeland Security and NSA, to have Homeland Security and NSA totally agree that NSA can be the powerful back room, but the storefront always has to be the Department.

Senator Peters: One follow-up, if I may, and I am running out of time. And I think, General Hayden, you mentioned about the civilian sector is very engaged in this, and I agree. I am very involved in the area of self-driving vehicles coming from Michigan. This is transformative technology. And certainly they are very aware and are focused on cybersecurity in that area. It is bad enough when someone breaks into your bank account, steals your money. If they take over your automobile, that is an existential threat to you -- and have formed ISACs and other ways to cooperate.

So your assessment of what you are seeing in the civilian sector with ISACs and other types of ideas that they are coming up with. What is your assessment of their effectiveness and how that might be able to be incorporated in this type of reorganization we are thinking about?

Mr. Hayden: No. They are a good news story, but they

are uneven. Across different industries, you get different degrees of commitment, largely based on sense of threat. And so I actually think that the power industry, financial services -- they are ahead of the pack because they know the dangers out there. It is not surprising that you are seeing that kind of cooperation here. But that would be the word "uneven" today.

Mr. Stavridis: I will give you one good one specifically is the banking sector. The eight largest banks in the United States have come together to form something called the FSARC. I will send something in for the record on that.

[The information follows:]

[COMMITTEE INSERT]

Mr. Stavridis: But it is a good news story. And again, it goes to General Hayden's point about a sense of threat. And they ought to feel threatened and they are working together to alleviate that threat.

Mr. Clapper: I would just endorse that. The financial sector in this country has gotten religion about this for obvious reasons. And that is a great model for this.

Senator Peters: Thank you.

Chairman McCain: Senator Nelson?

Senator Nelson: Thank you, Mr. Chairman.

Gentlemen, thank you for your public service.

I get the impression from your testimony that we really have not responded in any way to give the deterrence that we want. So let us take a couple of examples: the intrusion into our election and now the French election and we expect the German election. And so give me a scenario that you might think that we might respond so that anytime that the Russians are fooling around in the future in Ukraine, Syria, other elections, what would be a good deterrence.

Mr. Clapper: Senator Nelson, I spoke briefly to this at my earlier hearing before Senator Graham's Judiciary subcommittee. And I think frankly -- and I mentioned then, as much as I do not like doing hearings, that I thought it was a useful service for the public to have this discussion about the Russian interference, which in my mind far

transcends leaks and unmaskings and all that. That is all internal stuff. But this assault on our democracy by the Russians I think is profound. And the public has got to be educated and it starts with education, just as we were talking about with cyber.

So I will again contradict myself about how the government is organized with respect to messaging or counter-messaging. I would vote for a USIA, a United States Information Agency, on steroids to do the counter-messaging for election interference or counter-message ISIS or any other message that is inimical to our interests and our values because our messaging right now is fragmented across the government. And I have said this before, and the experience we had with this egregious interference in the most important process of our future of our democratic system has got to start with educating our public and doing the counter-messaging against those nefarious messages and the sources of them.

I do think the French went to school on our experience. And in the course of developing our intelligence community assessment, we shared with our friends and allies what we were experiencing. But that to me is a fundamental shortfall in the way we are organized now.

Senator Nelson: Let us hope the Germans do as well.

Mr. Hayden: Senator, I would do all that as part of a

component of a broader response. And here, I would drop what you described not in the information warfare box or in the cyber box. I would drop this in the "we got a problem with the Russians" box. And I would respond across the board.

So in response to this, I would sell arms. I would give arms to the Ukrainians. I would do everything that Jim described in terms of cyber counterpunching. And I think I would have the President fly up to Erie, get in a motorcade, stand on top of Marcellus shale and say this is going to Europe. This gas is going to wean our European friends off their dependence on Russian energy, and we are going to do that in 10 years.

Senator Nelson: I happen to agree. I think we ought to make a bold display of our displeasure. And let us hope that because of our misfortune in our election that, again, it is arming the Germans, as it apparently has armed the French. Part of that was an education campaign, just what you said, General.

All right. So the private sector, though. So, you know, they are really dragging their feet. We have not been able to get them to quickly share threat information with the government, and incentives are not working at the level that we need. So how do we need to change that private sector's thinking?

Mr. Hayden: Very briefly. Number one, keep on doing what we are doing. Keep pressing ahead. Make ourselves a more welcoming and more generous partner in the dialogue, again, back to the paradigm where we are in charge of what is getting shared and they get whatever we decide, again, probably not the right model, far more cooperative.

Mr. Stavridis: I would just add specifically the cyber insurance piece that we have talked about -- that is a very practical piece of this. And also doing a hearing like this -- you probably are -- with Eric Schmidt of Google, Dan Schulman of PayPal, Bill Gates of Microsoft, get those voices. You are probably already doing that.

Mr. Clapper: I do want to mention, Senator Nelson, the pushback that Jeh Johnson, then Secretary of Homeland Security, got from State election officials when he attempted to engage with them particularly on the issue of including our voting apparatus at large as part of our critical infrastructure. So there is a lot of suspicion, whatever it is, pushback at the State level and local level about the Feds getting involved in things, just another manifestation of this reluctance on the part of the private sector to engage.

Mr. Stavridis: Can I just pick up the last point about the States? We have not talked enough about the States and their role in all of this. I am joined today by Dave

Weinstein, who is the head of cyber for the State of New Jersey. They have a hub and spoke relationship with the Federal Government. We need more of that to break down those stovepipes in this area like we try to do in law enforcement.

Senator Nelson: Amen. Thank you.

Chairman McCain: Senator Blumenthal?

Senator Blumenthal: Thank you, Mr. Chairman. And thank you for having this hearing.

This hearing illustrates for me one of the ironies of working here, which is that we are discussing one of the most important topics to our national defense with one of the most erudite, informative panels in my experience on this committee, and the room is empty.

Mr. Stavridis: Hopefully, we are online somewhere.

Senator Blumenthal: I am sure we are online somewhere, but it really illustrates I think the point that each of you has made about education and the focus that needs to be devoted to this topic. I was reminded -- I do not know why exactly -- as one of you was testifying of a book called "Why England Slept," now a famous book because it is written by a former President, John F. Kennedy, about England's sleeping through the buildup in Germany and that buildup left it very far behind when it was directly and immediately threatened. I feel we are living through the same kind of

era right now in cyber, and we will be, I fear, tragically awakened to our complacency at some point.

General Clapper, you said in that Judiciary hearing -- and you were very powerful on this topic of the assault on our democracy -- that there needs to be -- and I am quoting -- I do think as well there needs to be more done in the way of sanctions to the Russians or any other government that attempts to interfere with our election process. End quote.

I have cosponsored and helped to introduce two measures, Countering Russian Hostilities Act and Russia Sanctions Review Act, that seek to codify and impose greater sanctions on the Russians. And I believe, as Senator Graham said at that hearing and both of us have said recently, that the Russians will continue to attack us -- 2018 is not very far away -- as long as they are not made to pay a price or, as the chairman said, as long as the benefits outweigh the price that they pay. That is just the calculus for them, and they are going to continue to do it.

But I also think that people who cooperate with them, aid and abet, collude also should be made to pay a price when they violate our laws. And there is an ongoing investigation conducted by the FBI into not only the Russian interference with our election but also potential cooperation or collusion they receive from Americans, including members of the Trump campaign, Trump associates.

Michael Flynn is subject to that investigation.

Assuming that all of you agree that anybody in this country who cooperates or colludes with that kind of cyber attack, which I regard as an act of war on this country, I am wondering whether I could elicit from you support for appointment of a special prosecutor? I realize it may be somewhat outside the sphere directly of the technical issues that bring you here today, but I do think it is of paramount importance. And you raised this issue by referring to domestic threats in the cyber sphere, General Clapper. You were on CNN this morning, General Hayden, talking about this topic exactly about your previous opposition to such special prosecutors but now perhaps you have a somewhat changed view because of the events of the last 48 hours and the need for what you called, quote, extraordinary structure to uncover the truth and impose accountability.

So with that longwinded buildup -- and I apologize for being so longwinded -- let me ask you, General Clapper and the rest of the panel, maybe beginning with General Hayden.

Mr. Hayden: I will go first because you are quoting me from a couple of hours ago in which I said I instinctively oppose -- these sorts of extraordinary structures go longer, deeper, broader than you want and they become destructive in their own right. But I have been disheartened by the events of the last 48 to 72 hours. I am not yet decided, Senator,

as I said on CNN, but I am very close to having -- I have a far more open mind than I did before lunch 2 days ago, and we will see now whether the ordinary structures can give the nation sufficient confidence that they will not be impeded, they will be enthused, and they will get to the truth and be able to tell us the truth.

Mr. Clapper: I worry about multiple investigations in the Congress, which I think have the effect of dissipating energy. As a frequent witness to these many investigations, I am in the same place that Mike is where I have reached the point where I believe that we need to think about that.

I have previously spoken in hearings that I thought probably the best hope in the Congress was the Senate Intelligence Committee, but in light of the events of the last day or so, I am moving toward that pendulum swinging more towards some kind of independent effort. Whether it is a commission or a special prosecutor, I do not know.

What I do know is we have got to get rid of this cloud over this country. This is in the best interest of the President. It is in the best interest of the Republicans or Democrats. I do not care what the stripe is. But this is a profoundly serious thing for this country. We are in a bad place. And I do not know what the solution is, whether it is some kind of independent body. Maybe that is where we need to go next.

Senator Blumenthal: Admiral?

Mr. Stavridis: I think this is beyond the scope of the executive branch. And the events call for something outside the executive branch, much as an IG in the military sits outside a chain of command and can, therefore, effectively look. What that exact structure is I do not know, and I yield to the Congress to determine it. That is why we have a separation of powers in this Nation.

Senator Blumenthal: I am way over my time, Mr. Chairman. I apologize.

Chairman McCain: Well, it is an important question.

Senator Blumenthal: Thank you.

Chairman McCain: Could I just say to the witnesses this has been very important for this committee? We appreciate the gravity of the challenge, and you have certainly given us a lot of good advice and counsel.

Could I finally say that there are very few benefits of being around a long time that I know of.

We are about to adjourn, Senator Warren.

There are very few benefits, but one of them is the great honor that I have had to know the three witnesses over the years. And I appreciate their wisdom, their counsel, and their outstanding service to our Nation. And I know you had other things to do besides coming here this morning, but I am speaking for the entire committee. I am very grateful.

This hearing is adjourned.

[Whereupon, at 11:12 a.m., the hearing was adjourned.]