Stenographic Transcript
Before the

COMMITTEE ON
ARMED SERVICES

UNITED STATES SENATE

HEARING TO RECEIVE TESTIMONY ON
THE FUTURE OF WARFARE

Tuesday, November 3, 2015

Washington, D.C.

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

HEARING TO RECEIVE TESTIMONY ON THE FUTURE OF WARFARE

Tuesday, November 3, 2015

U.S. Senate

Committee on Armed Services

Washington, D.C.

The committee met, pursuant to notice, at 9:27 a.m. in Room SD-G50, Dirksen Senate Office Building, Hon. John McCain, chairman of the committee, presiding.

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

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

Chairman McCain: Well, good morning. The committee meets this morning to consider the future of warfare. This hearing builds on a series of hearings this committee is conducting to discuss our current geopolitical challenges, examine the ability of our defense enterprise to meet these challenges, and identify what reforms are necessary to ensure that we have the most agile, innovative, and effective military and defense organization possible.

Today we focus on the future, what features will define the battlefields of tomorrow, what technologies and methods of employing them our future warfighters will require, and what we must do to reform our defense institutions to function and adapt closer to the need of innovation than the speed of bureaucracy.

We are fortunate to have a distinguished panel of witnesses this morning who will present their views on how to reimagine and reshape our military for the future. General Keith Alexander, former Commander of U.S. Cyber Command and Director of the National Security Agency, an outstanding leader. Mr. Bryan Clark, Senior Fellow at the Center for Strategic and Budgetary Assessments. Mr. Paul Scharre, a Senior Fellow and Director of the 20YY Warfare Initiative at the Center for a New American Security. And

Dr. Peter Singer, Strategist and Senior Fellow at the New America Foundation.

The witnesses who have testified before this committee continue to warn that the current global threat environment is the most challenging, complex, and uncertain in 70 years. But what is truly disturbing is that as we look to the future, the trends that are making the world more dangerous seem likely to persist and intensify.

Many of our adversaries are investing billions of dollars into reshaping their militaries and developing technologies to counter and thwart America's military advantages. At the same time, the speed of globalization and commercialization means that advanced disruptive technologies are increasingly available to rival militaries, terrorist groups, and other non-state actors. Add to that the harm caused by the Budget Control Act and sequestration, and we are now facing the dual problem of a quantitative and qualitative erosion of our military edge.

Reversing this trend certainly requires greater military capacity. There is still a lot of truth in the old adage that quantity has a quality all its own. That said, simply buying more of what we have now is insufficient. That is not how we will preserve our military technological advantage or win our future wars. Our enemies are not just investing in new defense technologies, they are investing in

strategies to counter America's traditional military strengths asymmetrically through cyber, hybrid warfare, and anti-access and area denial capabilities. Doing more of the same simply plays into our adversaries' hands.

As the National Defense Panel concluded, quote, maintaining the operational and technological edge of our armed forces requires sustained and targeted investment. I want to emphasize "targeted." We are witnessing rapid technological advancement in areas such as cyber and space capabilities, robotics, and unmanned systems, miniaturization, and directed energy, hypersonics, and data analytics. This is not science fiction. It is happening right now and we better understand the implications of these changes for the future of warfare because we know our adversaries are working overtime to do so.

This is a major defense acquisition challenge because these kinds of disruptive technologies are being developed more by non-traditional commercial companies than traditional defense industry. Indeed, the top four U.S. defense contractors combined spend only 27 percent of what Google does annually on research and development, and yet the defense acquisition system all too often serves to repel rather than attract producers of disruptive new technologies. Leading commercial companies are innovating on an 18-month cycle, but the Department of Defense is stuck

on 18-year cycles. This is a recipe for failure and fixing this problem must continue to be a top priority for this committee's acquisition reform efforts.

It is not enough, however, just to acquire new technologies. We must also devise entirely new ways to employ them. It would be a failure of imagination merely to try to conform emerging defense technologies to how we operate and fight today. Ultimately we must recognize the radical potential that these capabilities possess and shape new ways of operating and fighting around these new technologies.

The classic example is the tank prior to World War II. At the time, all the major powers had tanks, but they could only imagine them as mobile artillery or armored cavalry. It as the Germans who first understood that a tank is a tank, and they built entirely new operational concepts around it and realized its true potential.

Similarly, the United States Navy in the 1930's adapted itself despite fervent opposition at times, both internal and external, from a force built around a battleship to one organized around carrier aviation. Key military leaders at that time anticipated the opportunities that aviation presented, developed novel ways to fight with aircraft at sea, and prepared our Nation to wage and win a new type of naval warfare.

We face similar challenges now. Instead of thinking about how cyber or unmanned systems or other new technologies can simply enable us to do things we are already doing now, we must discern the real potential of these capabilities, both how they may be used against us and how they should be used by us. Then we must rethink and reimagine and reshape our military around these disruptive new technologies. That is the only way we will sustain our qualitative military edge.

This will require tough choices. Prioritizing for the future will not always be popular in all quarters of the defense establishment. Advocates for the status quo will likely resist change. But these are the choices we must make to ensure that our military will be ready to deter and, if necessary, fight and win our future wars.

I look forward to the testimony of our witnesses.

Senator Reed?

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

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

Let me join you in thanking our witnesses for their willingness to appear today to provide their thoughts on the future of warfare and how it may shape the organization of and the investments in our military going forward. Each of you has contributed to our national discussion on these issues. And I look forward to your testimony. Thank you, gentlemen.

A central theme of last week's hearing, one that I suspect will continue today, is the steady erosion of U.S. technological superiority and the need for a so-called third offset strategy to recapture a distinct qualitative advantage over our adversaries in operationally critical areas. The presumption that the decades' long technological superiority enjoyed by the United States and our allies will continue into the future may no longer be valid, as near peer competitors have learned from our past success and made advancements of their own, particularly in the areas of precision and long-range strike, anti-access/area denial, space, and cyber. This diffusion of technology has even impacted our advantages over non-state groups like ISIL and al Qaeda who are increasingly able to acquire and employ tools, including drones and satellite communications

equipment which would have been unthinkable only a few years ago.

As Deputy Secretary of Defense Bob Work told students at the National Defense University last year, as any good student of Clausewitz knows, the fundamental nature of war is an interactive clash, a two-sided duel, action followed by reaction. While the United States fought two lengthy wars, the rest of the world did not sit idly. They saw what our advantages were back in 1991's Desert Storm and they studied them and they set about devising ways to compete. He continued, our forces face the very real possibility of arriving in a future combat theater and finding themselves facing an arsenal of advanced disruptive technologies that could turn our previous technological advantage on its head where our armed forces no longer have uncontested theater access or unfettered operational freedom of maneuver.

Underlying these challenges are several technological trends that are reshaping the future of warfare. Global investment, notably by the commercial sector, in research and innovation is far outpacing the research and development budgets of the DOD and the U.S. Government as a whole. To compete, we will have to develop better acquisition hiring policies, harness this trend to incentivize some of those talented scientists and engineers in the U.S. private sector to work with us. And we will have to protect the military

and civilian research programs, laboratories, and agencies that are driving innovation that will shape our future military capabilities. The pace of technological change is accelerating, but DOD processes seem to be slower and more bureaucratic than ever. We need a 21st century defense enterprise to keep up, and I hope this is a key theme in the committee's efforts at defense reform being led by the chairman.

Beyond acquisition reform, this includes the development of new military concepts of operations that, for example, deal with complex robotic systems, new rules of engagement for the expanding cyber battlefield, new regulations to smartly deal with expanded use of things like nanotechnology, artificial intelligence, or biotechnology, and a new attitude both in the Pentagon and in Congress that encourages the informed risk taking and innovation that is characteristic of the people and companies that are shaping the future.

I welcome the witnesses' thoughts and suggestions on these issues, and I look forward to the testimony. Thank you, Mr. Chairman.

Chairman McCain: Thank you.

General Alexander, welcome.

STATEMENT OF GENERAL KEITH B. ALEXANDER, USA, RET., FORMER COMMANDER, U.S. CYBER COMMAND AND FORMER DIRECTOR, NATIONAL SECURITY AGENCY

General Alexander: Thank you, sir. Chairman McCain, Ranking Member Reed, distinguished members of the committee, I would like to talk briefly about what you have addressed in your opening statement, Chairman, about where technology is going and what this means to the future of warfare. I am going to do this rather quickly.

I submitted a statement for the record and would ask that that be put on the record.

Chairman McCain: All witness statements will be made a permanent part of the record.

General Alexander: Thank you, Chairman.

When you look at the rate of change of technology, what you brought up in terms of the cycle of where we are with the DOD acquisition system and where industry is, 18 years, versus 18 months, it is unacceptable especially when we look at cybersecurity. When you think about the rate of change for cybersecurity, it is doubling every 2 years. So that means that the kids that are in college today, what they learn in their freshman year -- half of it is outdated by their junior year. When you think about the volume of information that is being created, the unique volume of information, it is about 7 exabytes. What that means is we

are going to create more unique information this year than the last 5,000 years combined. And when you think about the staggering rate of that change of information and where it is going, and then you look at on the civilian side, the top 10 in-demand jobs now did not exist 10 years ago. So that means we are teaching students for jobs that do not exist, using technology that has not been created to solve problems we do not even know are problems.

But there is tremendous good that is going to come out of this in terms of the future of warfare and health care and saving money for our taxpayers in the energy market and others. When you look at just the revolution that is going to go on in the energy sector and how we can stabilize our Nation and other nations' energy sector and not waste billions of dollars in fuel costs a year, this is a huge opportunity for our Nation.

But with that opportunity comes tremendous vulnerability, and when you think about what the Defense Department is required to do, it rests on that civilian infrastructure. It rests on the energy sector, the communications infrastructure, and all of the other communications that are intertwined. Our Nation, in order to execute warfare, depends on that being there. And it is not secure. Tremendous vulnerabilities.

And I will just hit some highlights of what I think we

are going to face over the next several years. And you only need to look back at what happened in Estonia in 2007, first a distributed denial of service attack; 2008, a distributed denial of service attack. Both of those were by Russian hackers. I learned this from my daughter to put footnotes around when she said a dirty word, but I will use "Russian hackers." These are FSB. They are going after our Nation. In 2007, it was Estonia. In 2008, it was Georgia uniquely timed to Russian troops entering into Georgia. And as you know, Chairman, 2008 in October is when we found malware on the Defense Department's networks. And if you jump to 2012, we saw a series of distributed denial of service attacks against our Nation's financial systems, largely attributed to Iran. It was preceded by a destructive attack against Saudi Aramco that destroyed the data on over 30,000 systems. So from 2012 August when that attack occurred to 2013, 350 attacks against our Nation's financial infrastructure.

And now, when you jump forward to where we are today with what has happened to Target, Home Depot, Sony, and you look at what hit other countries, you are seeing that those nations who disagree with us are looking at ways to come at us using the full spectrum of power, diplomatic, political, economic, military, and within military, the easiest form for at least Russia and Iran, has been cyber. And now when you look at what is going on around the world today, you can

see that what is going on in Syria, if we have a disagreement with Russia, or if the Iran deal goes bad, or if we do not have a meeting of the mind on the Ukraine, or something pops up in North Korea, I expect these countries will come back at us with cyber attacks, and they can say not our guys. It is an asymmetric way of hitting our country and cause tremendous damage. And our Nation is not ready for these types of attacks across the board.

I think the cyber legislation that was brought forward takes us a great step down the road, but I think there is more that needs to be done. Within the Defense Department, only the Defense Department can defend this Nation in cyber. Homeland Security can set standards, but when our Nation is under attack, the U.S. Cyber Command, NSA, FBI -- those are the ones who are going to be the first responders.

So let us look at what happened to Sony and use that as a case example to end my opening statement, Chairman.

When Sony was hit -- everybody can say, well, that is not critical infrastructure. I have got it. But when Sony was attacked, we would not allow as a Government Sony to attack back against North Korea. The reason is if Sony were to attack back, it could start a bigger war on the Korean peninsula. That is the responsibility of governments. But if Sony is not allowed to attack back, then who does that for Sony? That is where our Government steps in. That is

where our Defense Department is, and that is what we are needed for. But we cannot see Sony's networks, and I am not advocating for the Government to be in all the networks.

What I would advocate for is like a radar system. When a company or a sector is being hit, that they can tell the Government at large I am being attacked.

Now, two things have to occur in order to do that. Those companies need to up their game in cybersecurity and understand what is going on, and they need to, much like a radar system, be able to tell the Government something is going on. Then the Government can determine what to do. And all of this has to occur at network speed. It is not a place where you can have someone in the loop making a decision. Chairman, it is analogous to doing nuclear exchange where we are racing down the road building Powerpoints to brief the White House on the next step when the missiles come in 30 minutes and the briefings come in 30 hours. In cyberspace to go halfway around the world takes 67 milliseconds. That is your decision space. It does not provide any opportunity for us to miscalculate in this area.

And when you think about what those who wish us harm want to do, if I were a bad guy -- I am a good guy, Chairman, I believe. If I were a bad guy, I would look at this as a military campaign and say how do I want to attack our financial sector, our energy sector and our Government.

And I believe those who want to do us harm can do that much like what happened in 2012 but this time with more destructive tools against our energy sector and against our financial sector. And if that happens the cost to our Nation would be measured in the trillions.

So where do we need to go? I think that is one of the things, Chairman, that we ought to discuss, where we go in this area, how we set up and organize within the Government and set the rules of engagement and get things right, train our troops across the board, and partner with industry. We have got to do both. We need industry to tells us what is going on, but the Government has got to be there to protect industry. I am not an advocate of us pushing money to industry for them to go fix their problem. I am advocate for industry upping their game and having the capability to tell the Government that something is going on.

These are areas that -- you know, I like to really talk about what is going on in this domain. And when you look at it and the Internet, our Nation is the one who created the Internet. We were the first to do this. We ought to be the first to secure it.

Thank you, Chairman.

[The prepared statement of General Alexander follows:]

Chairman McCain: Thank you very much, General.

Mr. Clark?

STATEMENT OF BRYAN CLARK, SENIOR FELLOW, CENTER FOR STRATEGIC AND BUDGETARY ASSESSMENTS

Mr. Clark: Good morning, Chairman. Chairman McCain, Ranking Member Reed, members of the committee, thank you for asking us to come here to testify today on this very important topic.

I wanted to highlight some elements from my written statement to get at the strategy we should be using to approach technology development and the Department of Defense to get at some of the trends that General Alexander and that yourself brought up earlier.

We have got a very dynamic security environment today, as we talked about in other sessions recently, and a very dynamic technology environment, as General Alexander highlighted. And what that is doing is it is transitioning our several decades of military dominance that we have enjoyed since the Cold War into one of competition. So we are now going to have to compete to be able to maintain our warfighting edge against our likely adversaries.

To be able to maintain our technological edge, we need to have an effective strategy that goes after the kinds of enduring advantages that we need to be able to have to deterring the future. The last time we were faced with a situation like this, where we had a long-term competition against a single or a series of adversaries, was during the

Cold War. During that period, we used several series of offset strategies that have been described by Secretary Work and others to be able to demonstrate to the Soviets that we would be able to hold them at risk, attack their targets at home, and attack their forces out in the field. These involved nuclear weapons initially with the new look of President Eisenhower's strategy in the 1950's, and it was followed later on with the strategies the Defense Department mounted with precision strike, stealth, and related capabilities, always keeping the Soviets on edge that they did not know if the U.S. was going to be able to effectively attack Soviet targets at will. And that kept them probably from attacking our allies in Central Europe.

So these efforts were successful in large part, though, because we were able to identify the next phase in important mission areas such as strike and undersea warfare, develop capabilities that were going to be effective in that next phase of those warfare areas and establish an enduring advantage. So I will talk about a couple of examples.

So in one, in undersea warfare, at the beginning of the Cold War with the advent of the nuclear submarine, the U.S. realized that passive sonar and submarine quieting were going to be key features of undersea warfare going into the Cold War and developed those capabilities. And as a result, we were able to maintain a dominant position in undersea

warfare versus the Soviets for almost the entire Cold War, and that redounded to a benefit in terms of our strategic deterrence because we could protect our own ballistic missile submarines while threatening those of the Soviet Union, as well as giving us the ability to attack their attack submarines out at sea.

Another area would be stealth. So we saw later in the Cold War that Soviet radar systems were getting better and better. Those were being proliferated to their allies in the Warsaw Pact and elsewhere. And so we started to develop stealth technologies and low probability of detection sensor systems that would need to be able to be effective against the kinds of sensors that the Soviets were developing. Those capabilities entered the force near the end of the Cold War, and we are all familiar with stealth being used in the Gulf War and then later gave us an advantage that still is benefiting the United States today in terms of the ability to strike targets at will almost anyplace on the globe. So several decades of benefit came from anticipating the next phase of warfare, developing the capabilities for it, and then moving into that next phase with an advantage that endures.

So once again now we find ourselves in a situation where we are geographically disadvantaged because our allies are far away and we have to project power in order to

support them, and we are numerically disadvantaged because a lot of our potential adversaries like China have much bigger forces than our own.

So we need to, again, look at the approach we took in the Cold War of anticipating the next phase in some important warfare areas and important missions and then developing the capabilities to be effective in them. That should be the heart of our technology strategy, the offset strategies that we have been talking about. The third offset that Secretary Work talks about should be looking at the next phase of mission areas that we think are important to deterring the adversaries we are facing today.

So some of those shifts -- I talk about them in detail in my written statement, but just to highlight the major shifts.

First of all, undersea warfare is likely to see a shift from listening for submarines with passive sonar and just quieting your submarines to one in which we use active sonar and non-acoustic methods to find submarines. That will mean our quiet submarines will not have the same benefit in terms of their survivability as they do today. We need to come up with new ways to counter detection using active systems, just as we do above the water to use jammers to counter radars. We will have to do the same thing under water probably.

In strike, we are going to see the continuation of the trend we saw towards stealth and low probability sensors that started during the Cold War but sort of went on hiatus with the Soviet Union's fall. So stealth and low probability detection sensors are going to be the de rigueur features of strike warfare going into the future.

In the EM spectrum, we have been operating today with very high power systems, very detectable systems, and we are not going to be able to do that in the future. We will have to move to systems that are increasingly passive and low probability of detection. There are key technologies we need to develop in those areas.

And then last in air warfare, these sensor advancements are going to result in a situation where fast, small, maneuverable aircraft are going to no longer be as beneficial as large aircraft that can carry big sensors and large weapons payloads in air-to-air warfare.

So those are some key areas that we need to be able to take into our existing advantage and build upon in order to be successful against the adversaries we are likely to face in the future.

General Alexander brought up cyber and space. So cyberspace is obviously an area of competition today. Space is a big area of competition. But it looks like, given the policy choices that the United States has made and is likely

to make in the future and our own dependence on both of those areas, it may not be that those are areas where we gain a significant military advantage. We may be faced with a situation where we just have to defend our current capabilities as opposed to being able to use those areas to asymmetrically go after our enemies. We may be forced into a defensive mode there.

So to be able to advance these technologies, we need to look at how we develop technology in the Defense Department. We have talked about and you talked about, Senator, the fact that we have an 18-month cycle in technology but an 18-year cycle in the Defense Department. There are some key ways that we need to drive the Defense Department to be able to develop technologies more quickly.

The first is operational concepts. Today we develop technologies absent a real idea of how we are going to use them, and we develop ways of fighting that do not take advantage of new technologies. We need to marry those two ideas up and get new operational concepts that leverage new technologies to be able to build requirements that drive the acquisition system towards new systems.

We also need to look at how we focus our technology investment. Today our technology investment is spread all over a large portfolio of areas instead of focused on those areas that are going to give us the greatest benefits

strategically down the road. So we are watering all the flowers in hopes some of them will turn into trees, but in fact we need to focus on the ones that are most likely to turn into trees.

And the last one is how do we develop requirements. Acquisition reform has been a big topic, I know, a big focus area of yours, and in the Department there is working going on as well. One key area that has not been addressed yet is the need to refine how to we develop requirements. When we develop the requirements for a new platform, we start from scratch every time we come up with a new airplane or ship or missile and define the requirements for it up front before we even start building the thing. Instead, we need to look at ways to build the requirements as we are prototyping technologies to get an idea of what requirements are going to be feasible. So how fast can it go for a reasonable cost? What is achievable in terms of schedule, and what is achievable in terms of the performance parameters of the particular weapon system? Those can be defined in large part by prototyping existing technologies and then building the requirements as you do that. That would be how a business might go about it, but in the Defense Department, we build requirements in isolation from any expectation as to how feasible it will be to deliver those requirements. So refining the requirements process will be a key feature

of speeding up that introduction of new technologies.

So we have an opportunity here with our current technological capabilities, many of which are maturing in these mission areas that are really important, but we need to make some changes in order to leverage them to gain this enduring advantage that will take us into the future.

And I look forward to your questions. Thank you.

[The prepared statement of Mr. Clark follows:]

Chairman McCain: Thank you.

Mr. Scharre?

STATEMENT OF PAUL SCHARRE, SENIOR FELLOW AND DIRECTOR OF THE 20YY WARFARE INITIATIVE, THE CENTER FOR A NEW AMERICAN SECURITY

Mr. Scharre: Thank you, Chairman McCain, Ranking Member Reed, distinguished Senators. It is an honor to be here today.

We are living in the midst today of an information revolution that is sweeping in its scope and scale. There is about $3.8 trillion spent every year on information technology, and that is more than double all military spending, R&D procurement personnel by every country on earth combined.

Now, that is maturing a number of underlying technologies and sensors, computer processing, data networking that will have significant impacts on how militaries fight. It is already having those impacts today.

And so we are seeing changes in warfare much like how the industrial revolution led to changes in World War I and World War II in tanks and aircraft and submarines. And the U.S. has already been able to be a first mover in the information revolution and gain many of the fruits of this technology with things like GPS and stealth and things others have mentioned today.

Now, the challenge that we have is this technology is proliferating to others. We got an early move, but we do

not get a monopoly. As Chairman McCain mentioned, many of those investments are happening outside of the defense sector.

So we saw in the Gulf War what some of these technologies can do in terms of inflicting significant damage and lethality on the enemy. But now we are going to have to face that same technology in warfare.

And there is precedent for these kinds of changes. In the late 19th century, the British developed an early model machine gun, a Maxim gun, that they used for conquests all across Africa. But in World War I, they faced an enemy that also had machine guns with incredible devastating effects. In the Battle of the Somme, the British lost 20,000 men in a single day.

We are not prepared for those changes that are coming as this technology proliferates to others and then continues to evolve and mature.

Thousands of anti-tank guided missiles now litter the Middle East and North Africa in the hands of non-state groups. Countries like China and Russia are developing increasingly capable electronic warfare and long-range precision strike weapons and anti-space capabilities, all of which threaten our traditional modes of power projection.

Now that they have guided weapons, they can target our forces with great precision as well, saturating and

overwhelming our defenses. Now, today missile defenses are very costly and the cost-exchange ratio favors the offense.

Now, this vulnerability of our major power projection assets, our carriers, our ships, tanks, our bases, coincides with the very unfortunate long-term trend in U.S. defense spending in decreasing numbers of capital assets. This precedes the current budget problem and will continue beyond it unless there are some major changes.

For several decades, the per-unit cost of our ships and aircraft has steadily risen, shrinking the number of assets that we can afford. Now, to date our response is to build more capable assets. We have extremely capable, qualitatively capable, ships and aircraft and submarines and aircraft carriers. But, of course, this drives costs up even further, reducing our quantities even more.

Now, this has made sense in a world where others do not have weapons that can target us with great precision. We have been willing to make this trade, and we have done so in many cases very deliberately trading quantity for quality.

But this is no longer going to work in a world where others can target us as well with great precision, can concentrate their fire power on our shrinking number of major combat assets. We are putting more and more eggs into a smaller number of vulnerable baskets.

Now, the Department of Defense broadly refers to these

challenges as anti-access/area denial. The problem is reasonably well understood. The problem is in launching a new offset strategy to counter it. A better ship or better aircraft alone is not going to solve the problem because on the path we have been on with the acquisition system and our requirements system that we have, we will build something that is even more expensive that will be good but even more expensive, and we will have even fewer of them.

So to operate in this area, we need a more fundamental shift in our military thinking. We need to be able to disperse our forces, disaggregate our capabilities into larger numbers of lower cost systems, operate and deceive the enemy through deception measures and decoys, and we need to be able to swarm and overwhelm enemy defenses with large numbers of low cost assets.

Now, so early thinking along these lines is underway in many parts of the Department. The Army's new operating concept talks about dispersed operations inside anti-access areas. The Marine Corps is also experimenting with distributed operations inside the littorals. The Naval Postgraduate School is researching aerial swarm combat with a 50-on-50 dog fight between swarm drones that they are working to develop. And DARPA's System of Systems Integration Technology and Experimentation program -- it is one of those long DOD acronyms called SoSITE, S-o-S-I-T-E --

aims to disaggregate aircraft capabilities entirely into a swarm of low cost expendable, cooperative assets.

So collectively these hint at the next paradigm shift in warfare, from fighting as a network of a very small number of expensive, exclusive assets as we do today to fighting as a swarm of a large number of cooperative distributed assets.

The main obstacles that stand in our way are not fundamentally technological. We could build the technology and within a reasonable defense budget if we are willing to make trades. They are not financial. The main obstacle is conceptual. It is a willingness to experiment with new ways of warfighting, and it is urgent that we begin this process of experimentation now.

Thank you very much.

[The prepared statement of Mr. Scharre follows:]

Chairman McCain: Dr. Singer?

STATEMENT OF DR. PETER W. SINGER, STRATEGIST AND SENIOR FELLOW, NEW AMERICA

Dr. Singer: Chairman McCain, Ranking Member Reed, distinguished members of the committee, thank you for inviting me to join you here today. It is a deep honor.

I am a defense analyst who has written nonfiction books on various emerging topics of importance to the series from private military contractors to drones and robotics to cybersecurity to my new book "Ghost Fleet: A Novel of the Next World War," which combines nonfiction style research with a fictionalized scenario of a 21st century great power conflict to explore the future of war.

This choice of scenario is deliberate as while terrorism and Middle East insurgencies are not going away, we face a return to the most serious kind of national security concern that shaped the geopolitics of the last century, great power competition, which could spill into actual conflict, either by accident or choice. In turn, the scale of such a challenge demonstrates the stakes at hand which hopefully we will not have to wait for to drive change.

In my written submission, I cover five key areas that distinguish the future of war, most especially in a great power context and needed actions we need to take from recognizing the challenges of new domains of conflict in

space and cyberspace, to dealing with our pattern of buying what I call the Pontiac Azteks of war, defense programs that are over-promised, over-engineered, and end up overpriced.

But in my remarks today, I would like to focus on one important issue, the new technology race at hand.

Since 1945, U.S. defense planning has focused on having a qualitative edge to overmatch our adversaries, planning to be a generation ahead in technology and capability. This assumption has become baked into everything from our overall defense strategy all the way down to small unit tactics.

Yet U.S. forces cannot count on that overmatch in the future. Mass campaigns of state-linked intellectual property theft has meant we are paying much of the research and development costs for our adversaries. These challengers are also growing their own cutting-edge technology. China, for example, just overtook the EU in national R&D spending and is on pace to match the U.S. in 5 years, with new projects ranging from the world's fastest supercomputers to three different long-range drone strike programs. And finally, off-the-shelf technologies can be bought to rival even the most advanced tools in the U.S. arsenal.

This is crucial as not just are many of our most long-trusted, dominant platforms from warships to warplanes vulnerable to new classes of weapons now in more conflict

actors' hands but an array of potentially game-changing weapons lie just ahead in six key areas.

And new generation of unmanned systems, both more diverse in size, shape, and form, but also more autonomous and more capable, meaning they can take on more roles from ISR to strike, flying off of anything from aircraft carriers to soldiers' hands.

Weapons that use not just the kinetics of a fist or the chemistry of gunpowder, but energy itself, ranging from electromagnetic railguns able to a fire projectile 100 miles to new directed energy systems that potentially reverse the cost equations of offense and defense.

Artificial intelligence, ubiquitous sensors, big data, and battle management systems that will redefine the observe, orient, and decide and act, the OODA loop.

Hypersonics, high speed rockets and missiles, 3-D printing technologies that threaten to do to the current defense marketplace what the iPod did to the music industry.

And human performance modification technologies that will reshape what is possible and maybe even what is proper in war.

The challenge, though, is the comparison that could be drawn between what is now or soon to be possible versus what are we actually buying today or planning to buy tomorrow. Our weapons modernization programs are too often not that

modern. For example, if you start at the point of their conception, most of our top 10 programs of record are all old enough to vote for you, with several of them actually older than me.

We too often commit to mass buys before a system is truly tested, locking in on single major programs that are too big to fail and actually are not all that new. And this dynamic shapes not just what we buy but extends their development time and ultimately our expectations of how much of it we will buy decades into the future, limiting our present and future flexibility. To abuse a metaphor, the growing per-unit cost of the cart is driving where we steer the horse.

At the heart of this is that while "disruption" is the new buzz word in defense thinking today, part of the Pentagon's new outreach to Silicon Valley, we struggle with the dual meaning of the concept. We claim to aspire for the new, but to be disrupted, the outdated must be discarded.

The roadblocks to disruption play at multiple levels, from specific weapons programs to organizational structures, to personnel systems and operating concepts. For instance, there is a long record of the Government funding exciting new projects that then wither away in that space between lab and program of record because they cannot supplant whatever old gear or program, factory, or internal tribe that is in

the way. Indeed, there is even a term for it, the "valley of death." The same goes for all the new and important ideas and proposals you have heard in these hearings over the last several weeks. To be adopted, though, something will have to be supplanted.

As you program for the future, ultimately what you support in the new game-changers of not just programs but also thinking, structures, and organizations what you eliminate in the old and what you protect and nurture across that valley will matter more than any single additional plane or tank squeezed into a budget line item or OCO funding. It may even be the difference between the win or loss of a major war tomorrow.

I would like to close by offering two quotes that can serve hopefully as guideposts, one looking back and one forward.

The first is from the last interwar period where Churchill may have said it best. Quote: "Want of foresight, unwillingness to act when action would be simple and effective, lack of clear thinking, confusion of counsel until the emergency comes, until self-preservation strikes its jarring gong, these are the features which constitute the endless repetition of history."

The second is from a professor at China's National Defense University, arguing in a regime newspaper how his

own nation should contemplate the future of war. Quote: "We must bear a third world war in mind when developing military forces." End quote.

We need to be mindful of both the lessons of the past but acknowledge the trends in motion and the real risks that loom in the future. That way we can take the needed steps to maintain deterrence and avoid miscalculation and, in so doing, keep the next world war where it belongs, in the realm of fiction.

Thank you.

[The prepared statement of Dr. Singer follows:]

Chairman McCain: Thank you very much, Doctor.

General Alexander, you mentioned that the legislation that was recently passed on cyber was a good step forward. What more?

General Alexander: Chairman, I think the key thing that has to be clear in that legislation, that when there is a military response required from actions that that has to go immediately to the Defense Department. What I am concerned about is we set up a process that it is delayed at the Department of Homeland Security, inspected, and then sent. And so how long does that inspection take? And for metadata, we could do that automatically.

So what I would encourage is the development of a set of standards -- think of these as protocols -- where both houses in Congress could agree that these type of information hold no personally identifiable information and is necessary for the protection of the Nation, and it could go directly to all the parties. So I am not saying cut DHS out. I am saying ensure that DOD gets it in real time. It would be analogous to a radar, and instead of DOD getting the radar feed on where the missile is, that goes to DHS and then they tell you where the missile is.

Chairman McCain: You said it is important to partner with industry. I get the impression that industry is not particularly interested in partnering with us.

General Alexander: I think there are two parts to that. You know, it has been an exciting year and a half out. What I have found is industry is very much into cybersecurity. They are very concerned about what they share with the Government because of liability. But at the end of the day, they recognize that the Government is the only one that could defend them from a nation state-like attack.

Chairman McCain: Dr. Singer, is the F-35 the last manned fighter aircraft in your view?

Dr. Singer: I do not know if it is the last because certainly other people may continue to construct them. We may as well. The question is, to make a historic parallel, its comparison, if we are thinking about the interwar years, the Spitfire or, to use a Navy example, the Wildcat systems that the investment prove worthwhile, or does it parallel the Gloster Gladiator, the last best biplane? I would offer to the committee to explore that parallel history of a program that we set the requirements. The requirements were set early, and then the world changed around it. And so all the things that seemed fantastic and useful about the Gladiator -- it was a metal biplane. It carried two machine guns. It could go faster than previous biplanes. And it was outdated before it even left the development cycle. But they continued to push forward with it. And its nickname

among pilots who flew it in World War II was not the Gladiator but it was nicknamed the "flying coffin."

Chairman McCain: Some other aircraft have inherited that moniker as well.

Dr. Singer: So I think the challenge is going to be -- we will buy the F-35. I think we are going to have to wrestle with, obviously, the issues that you have pointed out, the per-unit costs, how that will affect in the long term our plans for how many we want to buy. I have a hard time believing that in the year 2025 or 2030 we are still going to be buying the same numbers that we expect to buy now. The world will have changed. The capabilities will have changed. Also its integration with unmanned systems and what role will it play or will it be able to play in terms of partnering with unmanned systems or managing them. So there is a sea of change.

My worry is that it is a program that many of the concepts for it were set, to put it bluntly, the year that I was leaving college.

Chairman McCain: Mr. Scharre, we all agree that the Pentagon is not structured nor is the command system structured now to meet the new challenges that you witnesses have aptly described. Take a stab at how should we restructure the Pentagon to meet these new challenges.

Mr. Scharre: Thank you, Mr. Chairman.

I think one important disconnect that has come to light in the last 15 years is the disconnect between what the Pentagon is doing in terms of long-term acquisition and very near-term needs in the combatant commands. We saw this in Iraq and Afghanistan, the creation of all of these ad hoc processes like MRAP task force, an ISR task force, and JIEDDO, things that were basically silver bullets the Secretary had to personally fire at a problem to get it fixed. So institutionalizing that is important not just for counterinsurgency or guerilla wars, perhaps even more importantly for major wars where the level of violence is likely to be higher and the timelines are shorter and the need to rapidly innovate in a battlefield is really essential, as well as to anticipate these problems.

The Department has made some steps in that direction with the creation of things like a joint emergent operational needs sort of pathway to create requirements. But I think there is a lot more to be done in terms of giving the COCOM's a voice, in terms of near-term capability development, and then creating a pathway. And the services have some of these individually -- the Air Force does -- to do rapid capability development.

Chairman McCain: Mr. Clark?

Mr. Clark: Yes, sir. So I would say that we need to look at having one process that is how we develop the

requirements and acquire large manned acquisition programs, so ships, aircraft, where we might want to have a more deliberate process by which we develop the requirements because of the need for them to last several decades and potentially protect large numbers of people onboard. And then have a separate process like Mr. Scharre is talking about where we acquire smaller programs, so everything below that which is 99 percent of the programs that we develop in DOD where we can develop the requirements in concert with a technology demonstration and prototype program. A lot of the technologies that new acquisition programs leverage are already mature and sitting, waiting at the valley of death to make the trip across. So they are waiting for some boat to come and pick them up and carry them there. Well, we could take advantage of and bridge that valley if we instead said everything that is not a large manned platform, for example, weapons sensors, unmanned vehicles, et cetera, is able to take advantage of an acquisition process where we develop requirements at the same time as we develop the specifications and the plan for the system. So it would merge requirements and acquisition to a much greater degree.

Chairman McCain: So we would not need a 1,000-page document for a new handgun.

Mr. Clark: Exactly. New handgun, new unmanned system, all of those technologies are ones we are going to harvest

from industry or DOD labs that have already been developed. So why not just create a process that develops the specifications that we actually want in the final program very quickly based on what has already been achieved technically and we know what the cost is going to be.

Chairman McCain: Thank you.

Senator Reed?

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

And thank you, gentlemen, for your very, very insightful testimony.

It strikes me that we are talking about, as many of you mentioned, this disconnect between the reality that we all recognize today, even the leaders in the Defense Department and my colleagues here, and operational practice, institutional outlooks, the equipment, the training, everything. And the question is how in very real time, quick time we sync those things up.

And one thought is by having exercises where we actually game this out in a comprehensive way. I am recalling -- someone mentioned the interwar years where -- and the chairman mentioned the development of the carrier, et cetera. That was done when people were sitting at the War College in Newport thinking very carefully about the threats, the new technology, and providing a basis. So where are we in the process of sort of forcing the system by

having comprehensive exercises that will force us to answer specific questions like how do we organize or reorganize. What equipment do we really need, et cetera?

And, General Alexander, you can start and then I ask all the witnesses.

General Alexander: Senator, I think the first thing that we have to look at is to expand our outlook on what cyber can do to our country. I think in the military, we focused on military-on-military engagements. But practically speaking, an adversary is going to go after our civilian infrastructure first. You know, on war, when people talk about total war, take the will of the people out to fight. We are seeing that in some of the things going on today. Take down the power grid and the financial sector, and everybody is going to forget about these problems. And we are essentially isolated. So I think we have to step back and look at this in a more comprehensive manner. What does it mean for the Defense Department to really protect the Nation in this area.

I think there is a great start with the way the teams have been set up and what they can do, but there is a long way to go. And I do think we have to have this war game.

You know, during my tenure at Cyber Command, some of the questions came up. Do we go from sub-unified to unified to separate service where folks like Petraeus and Stavridis

said go to a separate service. I was not there, but I do think we have to step into this area. And Secretary Gates had some great insights on so how are we going to do this because it is a new way of thinking about warfare where our Nation now is at risk. In the past, we could easily separate out the military to overseas and what went on in the country as others. In this area, you cannot do that because the first thing they are going to go after is our civilian infrastructure.

And so I think the war game has got to start with that and how we respond to that. And it is going to escalate at orders of magnitude faster than any other form of warfare that we have seen.

Senator Reed: Thank you.

Please, Mr. Clark.

Mr. Clark: Senator, I would say looking at the interwar years is a great example because what we did back then is the warfighters would get together at Sims Hall up at the Naval War College and play out the war game on the floor there with play ships and models and everything and then go out and do a series of battle experiments at sea to practice the best of breed concepts that came out of that process.

So right now, the Department of Defense is reinvigorating its war-gaming efforts in an effort to try to

put the intellectual capital into the development of new warfighting concepts. And then those warfighting concepts that emerge from those, the best of breed, if you will, for how they are going to fight in the future -- then they need to be taken out, as you are saying, and experimented with in exercises using real systems in a real operating environment.

I would say one other thing that DOD does not do well, which they need to start doing a better job of, is incorporating technologists into these discussions. So we run a war game. We get a bunch of operators together and we give them a problem and they know their systems that they have today from the ship or aircraft they just left, and they go play it out and figure out the best way to fight. But they are not taking advantage of what technology might offer them in the next 5 or 10 years, which is really the timeframe we are aiming for. So we need to bring into those war games, into the subsequent experiments the technology experts that know where technology is going but do not necessarily know how it is going to be used. And by putting those two groups of people together, you are more likely to get an operational concept that comes out it that is able to leverage new technologies and do something different than what we did before.

And the examples of the past where we had stealth or

where we developed passive sonar are perfect examples of where our technology people came in and said, well, this is possible. And operators said, well, I think I know how I would use that, and they came up with a way to apply it. Then we could take that out in the field and practice it. That is something DOD needs to do a better job of.

Senator Reed: Mr. Scharre, my time is diminishing. So your comments, please.

Mr. Scharre: Yes. Thanks, Mr. Senator.

I guess I could not agree more that this process of experimentation is really critical. And I would just add that it has to be segregated from training in terms of qualifying a unit. When we send in Army units something like NTC, that is about ensuring the unit's readiness and training. There may be room for actually taking some units -- we have done them in the past -- and setting them aside as experimental units to try new concepts, and that is something that the Department should be looking at.

Senator Reed: Thank you.

And Dr. Singer, finally.

Dr. Singer: Very rapidly. I think the challenge in the existing system is the exercises either are about validating existing concepts -- you hear the phrase often "getting back to basics." What if the basics have changed in the interim -- or they are about allies, making allies

feel better them about themselves, partnership capacity building and confidence building. That is different than the interwar years of the Louisiana maneuvers and the fleet problem exercises.

Secondly, those were very valuable in the interwar years not just in showing what to buy and how to use it but the "who," what kind of personnel thrive in these new styles of war. So it is linking the exercises to your personnel system.

Third, rapidly, a quick issue is the budget is not a preventative of it. They went through the Great Depression and figured out aircraft carriers, amphibious landing. It is often culture of implementation.

And then finally, beware in this of the lessons and the people saying they are adopt but only in an uneven manner. And I think that, to circle back to the cybersecurity aspect, is a challenge here where we are taking a lot of new capabilities and putting some of them into old boxes. So we have built up Cyber Command, but we still have a system where the Pentagon's own weapons tester found, in their words, significant vulnerabilities in every single major weapons system.

Senator Reed: Thank you.

I assume, if someone disagrees, that General Alexander's comment is that this is much broader than the

Department of Defense and we tend to look ourselves in sort of stovepipes of defense planning, et cetera. But this has to be a usually comprehensive exercise involving the Federal Reserve, the Department of Defense, the major utilities, everyone engaged. And I assume everyone agrees with that.

Thank you, Mr. Chairman.

Chairman McCain: Senator Inhofe?

Senator Inhofe: Thank you, Mr. Chairman.

First of all, General Alexander, I appreciate the time we had. I learned a lot in the time that we spent together when you were in your position. And it was very meaningful.

I recall when I was first elected -- I came from the House to the Senate -- I replaced David Boren. David Boren was the chairman of the Intelligence Committee. He told me at that time one of the problems that we were never able to deal with was the fact that we have all of this technology and all these things that we are finding out, and yet we seem to be competing with ourselves. I mean, you have the FBI, the CIA, the NSA -- we did not have Homeland Security then.

But I am kind of seeing the same thing. Well, we made some headway there. In fact, up in Tuzla during the Bosnia thing, was the first time all of the entities I mentioned were in one room together. At least they were talking.

Now, you mentioned in your statement commercial and

private entities cannot afford to defend themselves alone against nation state attacks nor nation state-like attacks in cyberspace and that the U.S. Government is the only one that can and should fire back.

Now, it just seems to me that we had that -- I would ask you what agency -- how this should be restructured because we have each one of these like the NSA. They have a cyber division and the CIA and all that. How would you envision -- and I know you have given some thought to this -- restructuring this thing to be more effective?

General Alexander: Well, I am going to take from what I talked with Secretary Gates about because I think he had the greatest insights. And when you look at the departments that are responsible for protecting the country in this space, you have Homeland Security. You have the Department of Justice, and you have the Department of Defense. And practically speaking, all the technical talent really lies at NSA in deep technical expertise in the network, and hence the reason we put Cyber Command there so you married those two pieces up.

The FBI has some great talent for domestic capabilities, but they do not have any of the deep technical talent that came out of World War II for encryption, decryption, and the things that really helped the network operate. So when you talk about network operations, that is

probably the best expertise.

So I think as you look at it, the question then becomes what do you do that brings those three departments together. And he looked at a third hat. And I would ask you to reach out to him and get his thoughts on it. I know he has testified once, but he had some great insights and I think directly from him on that, what is probably the best approach. And we actually started down that road and fell apart at one point. But I think that is where our country needs to get to because that allows you to look at what you are going to do to defend the Nation and what you are going to do to recover when bad things happen. And both of those have to be synchronized as we go forward.

Specifically it goes back to what Senator Reed brought out. If our Nation is attacked and they take down the power grid and they do massive damage, where is your first priority for the future of the Nation is something that has to be, well, how am I going to defend this country, first and foremost has to be put on the table. So those kind of decisions have to be made. And I think that is what I would do.

I am not sure -- I have not been able to think of a way of collapsing all the intel agencies together unless you just smashed them all together under the DNI and then made some agencies. But you are actually back to where you are

today. So I do not know a better way right off the top of my head to do that, Senator.

Senator Inhofe: I was going to bring up the effort that you made in that position like going out to the University of Tulsa, and they developed a great program there. As Dr. Singer mentioned, we have to watch what the Chinese and others are doing, the emphasis they are putting on, they are teaching their kids. I look down the road and think they are passing us up everywhere.

Let me just real quickly get back to the fact that a statement that was made by Bob Gates talking about how we have never once gotten it right. I can remember the last year I served on the House Armed Services Committee was 1994. I recall when we had experts testifying, and one of them said that in 10 years we will no longer need ground troops. Well, that is kind of an example of what is out there in a reality that we have not been getting it right.

But one thing I think that Bob Gates got right was when he was on the panel. Incidentally, we have had great panels the last 3 weeks and up to and including this panel of experts. We had the people in think tanks. We also had the five professors from different universities. We had them all responding to the fact that Bob Gates stated that in 1961 we spent -- defending America consumed 51 percent of our budget. Today it is 15 percent of our budget.

In all the problems that you are addressing that you have been talking about -- and I would ask all of you this question -- are we not giving the right emphasis to defending America? Right now with sequestration coming on, they are insisting on having an equal amount of money affecting the social programs as defending America. So do you think that we need to -- you can just say yes or no, going down the table -- reprioritize making defending America the number one priority again? Dr. Singer?

Dr. Singer: Sequestration is incredibly unstrategic, but it is akin to shooting yourself in the foot not shooting yourself in the head. So how we deal with it will determine success or failure.

Senator Inhofe: I think that is yes.

Mr. Scharre?

Mr. Scharre: Thank you, Senator.

I acknowledge there are some very difficult domestic political compromises here, but I think it is very clear that we certainly are not spending enough on defense today in order to defend the country adequately.

Senator Inhofe: Thank you.

Mr. Clark?

Mr. Clark: Yes.

Senator Inhofe: Thank you, Mr. Chairman.

Chairman McCain: Senator Manchin?

Senator Manchin: Thank you, Mr. Chairman.

And thank all of you for being here today.

General Alexander, if I could ask, which country or which group has the most to gain from attacking -- the cyber attack to America? Russia, China, ISIL? Who do you rate as the number one?

General Alexander: So each of them have different objectives. But Russia -- when we disagreed on the Crimea, we saw increased attacks against companies like Target and Home Depot from their hackers.

Senator Manchin: How would that benefit them as a country?

General Alexander: Well, they allow their hackers kind of freedom. They can say, okay, you guys can go do this. We are not watching. Go have a good time. They steal. They make money. We get hurt. Russia kind of sends an indirect message.

The same thing in Iran. When you look at the disruptive attacks on Wall Street, what they are doing is they are sending a message. You have sanctioned us in the finance and the energy sector. We will fire back. Saudi Aramco, your energy sector.

In China, it is different. China is all about building their economy. All they are doing is stealing everything they can to grow their economy. It is intellectual

property. It is our future. I think it is the greatest transfer of wealth in history. And interestingly, we could stop that. I believe that. I really do.

I think, Senator, if I could, what Senator Reed and Senator Inhofe brought up, if you put those two together and said why do we not have a major exercise with industry in there, industry is willing to pay their portion for cyber defense. I am convinced of that. And if they did their part right in defending what they need to do in setting up the ability to tell the Nation when they are under attack, you could stop attacks from Iran, Russia, and China, and we should do that.

Senator Manchin: Let me ask you about the NSA. We are talking about all this outside interest in attacking the United States for many, many reasons you just stated. What have they done to stop the Edward Snowdens of the NSA from inside attacks?

General Alexander: So we set up a program in 2013 to look at all the things that --

Senator Manchin: Was it a surprise to you? I am so sorry to interrupt you. A surprise to you have this happen. I know you were there.

General Alexander: I was surprised at a person who we had entrusted to move data from one server to another really was not trustworthy.

Senator Manchin: You had him at a high level. I mean, you knew you had him at a very sensitive, high level, and you did not vetting him well enough?

General Alexander: No. His level was exaggerated by himself. He was actually a very low level system administrator with an important job of moving information from the continental United States to servers in Hawaii. And in doing that, he took data from those servers.

We came up with 42 different series of things that could be done. We shared those actually with the rest of the Government, with industry -- the ones that we could -- on how to stop insider attacks.

It is interesting. When I talk to most of the financial institutions, more than 50 percent of their concerns come from insider attacks. So these are things that are going on. You have got to do both, and it is all in the behavioral analytics and modeling that would go on to stop that.

So I think we did a good step, but you note a very important point. We were caught flat-footed on Snowden.

Senator Manchin: Do you think those steps have been taken to shore that up so that it does not happen again within the NSA? You are not sure if other private organizations have taken your all's advice or lead?

General Alexander: Well, for sure in the NSA because

we ran tests. We actually gamed, and then we ran backward data and found that we detected them every time.

Senator Manchin: And how damaging was the information that he has shared or basically stolen and taken with him and distributed around the world?

General Alexander: I think it was hugely damaging. You can see what the DNI recently said about support to our troops in Afghanistan, the fact that some of that information has gotten out, and our ability to now detect adversaries in Afghanistan has been impacted.

The same thing on terrorist attacks. It has set us back. I personally believe that what he is doing with Russia is hurting our country.

Senator Manchin: Do you believe that Snowden should be treated as a traitor?

General Alexander: I do.

Senator Manchin: And tried as such.

General Alexander: Yes, I do.

Senator Manchin: Thank you.

Chairman McCain: Senator Sessions?

Senator Sessions: Thank you, Senator McCain, for your leadership and for the series of hearings we have been having.

I would just join with you in your comments about our breaches and Snowden and those issues, General Alexander. I

think it is very important. And I do not sense from my study of it that we are having any significant threat to individual Americans' liberty. Apparently the President knows everybody that owns a gun in the last campaign and ran ads targeting everybody for every little thing that they favored, they knew about and targeted their campaign message. So we do not have anything like that with regard to our defense analysis.

Well, several years ago, my subcommittee, the Strategic, talked about the threats we might have to our missile and space systems, and we asked that we have reports and analysis of that. Senator Levin, who chaired the committee at the time, and Senator McCain and others agreed that this was not only a problem for our missile systems but for our entire defense systems. I think Dr. Singer just said that earlier.

So we have got legislation, General Alexander, that focuses on that that calls for an analysis of our vulnerabilities and puts now $200 million toward identifying those and creating a response and a plan to protect our vulnerabilities. So I will ask you and Mr. Clark about that, others if you would like to share thoughts about it.

So, first of all, are you familiar with the legislation? Do you think it is a step in the right direction? Do we need to go further? And are we vulnerable

and can we take actions that would improve that to limit our vulnerability?

General Alexander: I am not 100 percent steeped in it but I am aware of it, and let me give you my thoughts, if I could.

I think on the vulnerabilities and where we are going to detect and repair those vulnerabilities, that we have got to continue to upgrade how we do that. And let me give you an example. When I had Cyber Command, the issue that we faced was 15,000 enclaves. How do you see all those enclaves? And the answer is as the commander responsible for defending our networks, I could not. And so when I so how do I know these guys are fixing the vulnerabilities and doing everything we told them to do, well, they report up and so it cascades up. And so simple fix is done at manual speed. It takes months when it should be automated. The humans should be out of the loop.

So I think it is a step in the right direction. I would look at and encourage you to look at how we could now automate parts of this because I think it is crucial to blocking those attacks. So I think what you are doing is right. I think there are some steps now that we could take to go beyond that, and I would be happy to talk with some of your people on that.

Senator Sessions: Thank you very much.

Mr. Clark? By the way, Mr. Clark, I see you had the distinction of serving on the nuclear submarine Alabama. It is kind of special to me. Tell Senator McCain what you say when you finish off on your announcements on the Alabama?

Mr. Clark: Roll tide.

[Laughter.]

Chairman McCain: It is deeply moving.

Mr. Clark: It is, is it not?

[Laughter.]

Mr. Clark: So I would say I agree with the General, obviously, that we need to move towards using automation to a much greater degree to protect our systems from cyber attack. And then also this idea that we need to modernize our networks that deal with missile defense and for strategic deterrence in particular to reduce the number of separate systems involved and reduce the amount of surface area, if you will. So every separate enclave that he described has its own vulnerability to attack like a bunch of little forts that are out there and you have to defend every fort individually. And so instead, we need to start bringing more of those into the same enclave so we only have to defend one perimeter as opposed to hundreds of perimeters.

And today in some of these areas where we have had legacy systems cobbled together over time, we have got a

bunch of different systems that are now interconnected as opposed to having one system that is able to protect itself automatically. Then that goes back to the automation idea.

I would say a couple other things with regard to our vulnerability in space, though. We also have to deal with the fact that in space, the advent of the new technologies like micro-satellites and servicing robots, to use that again with quotes, but the idea that there are countries that are developing satellites that are small, satellites designed to repair or service or put new batteries into other satellites could also be used to attack a satellite without generating the kind of debris that we would normally assume would deter somebody from attacking a satellite in space. So new technologies that would allow attacks in space are something we have got to consider as well in terms of how do we protect our satellite infrastructure that we depend on for strategic deterrence and for missile defense.

Senator Sessions: Thank you.

Mr. Scharre or Dr. Singer, would you like to add to that?

Mr. Scharre: Thank you, sir. I would just add on the space side that an important component of enhancing our resiliency in space is off-space backups and networks for redundancy and in part to protect our assets but also to reduce the incentives for attacking them in space. The

Department of Defense has had a program to build an aerial layer, the joint aerial layer network, to do communications and position navigation and timing for a number of years that is consistently underfunded and in large part because it is the kind of thing that does not sort of strike a core constituency within the services. So that is something also to add to thinking about our strategic resiliency.

Senator Sessions: Dr. Singer?

Dr. Singer: Thank you, Senator.

I would add a note of caution, maybe a little bit of disagreement on the panel, and then some suggestions.

The note of caution is we should not lean too much on the Cold War parallels of deterrence and mutuality of response, thinking that showing our ability to hit back will deliver 100 percent security in either space and also the idea of the quick timeline. Yes, cyber moves at digital speed, but for example, attacks take not days but months, sometimes years to put together. On average, it is a time period of 205 days between when an attack starts and when the victim finds out about it. In turn, your best response often in cyber attack is not to try and hit back within that 30-minute window with nuclear weapons of the parallel, but in fact, it may be to pause, study it, steer them into areas that they cannot cause harm. So the parallels sometimes are not exact.

The deterrence model that I hope we look for -- and we have heard it from the panel here in both space and cyberspace -- is more on deterrence by denial, which is building up resilience, whether it is in space by moving from a billion-dollar, single points of failure that can be easily taken out to networks of smaller, cheaper, micro-satellites. The same thing in cyberspace, building up resilience in both the military and on the civilian sector.

And within that, I hope we are willing to look at alternative approaches and stop trying to take new capabilities and problems and put them into old boxes. So, for example, I would contrast our defense approach and the way it has not done a great job of pulling in civilian talent. Estonia was mentioned as a model of a victim, one of the first victims of state-level cyber attack, but they have also built up a level of national resilience that we do not have. I would suggest the model of the Estonian Cyber Defense League as an alternative to our approach right now that might be a very positive one.

Thank you.

Senator Sessions: Thank you, Mr. Chairman.

Chairman McCain: One of the problems with the Estonian model is the privacy issue that causes many of the industries here and companies to be resistant to that model.

Senator Shaheen?

Senator Shaheen: Thank you, Mr. Chairman.

And thank you all for testifying this morning.

If I could ask each of you to give a very brief response to do you think the biggest threat as we look at cyber attacks and other challenges to our power grid and to the United States come from the great powers, the great power competition that you referred to, Mr. Clark, or do they come from terrorist groups and non-nation states? General Alexander?

General Alexander: I think the greatest concern comes from nation states. The most frequent attacks come from hackers, terrorists, and others.

Senator Shaheen: Mr. Clark?

Mr. Clark: I agree. I think the greatest threat is going to be from nation states.

Senator Shaheen: Does anybody disagree?

Mr. Scharre: Yes. I guess I would disagree. I mean, I think in terms of large scale, certainly nation states can bring more power to bear, but I think that this issue of frequency and likelihood is absolutely critical. It is something we need to factor into thinking about threats. I think it is clear that non-state actors can wreak quite a big of destruction on the United States. And deterrence is less effective.

Senator Shaheen: General Alexander, I think I

understood you to say that we could stop attacks from Iran, Russia, and China, and you prefaced that by talking about the importance of the private sector and their willingness to invest in their own cybersecurity. If we can do that, what has been the impediment to doing that, and how should the operation be organized?

General Alexander: So I think there are several impediments. First, having the right cyber technology, a holistic and comprehensive approach that allows a commercial entity or company to understand when they are being attacked or exploited, the ability to share that information, both from cyber legislation and from a technical perspective, the ability for the Government to receive and then to respond. And I do think it is here where the wargaming and other things would go on. So what is your response going to be if these events occur? So you have thought that through ahead of time and you know how and what and the commands know what they are going to do.

Senator Shaheen: Well, again, if we can do that, should it be organized under the Cyber Command within DOD or should it be organized someplace else? And why have we not done that already?

General Alexander: Well, this goes back to the organizational structure that was asked previously. We have parts of this in DHS that is really responsible for the

resiliency, correctly. We have the DOD defend the Nation. And then you have the Department of Justice with the responsibility for criminal activities.

What Secretary Gates said is you have got those three, but they are all talking about the same domain and you can go very quickly from, as Mr. Scharre brought up, a non-nation state actor acting like a nation state actor.

So I think you have to have war games and we have to go through that. We have not organized ourselves right, nor did we bring Government and industry together and we do not have the legislation to allow that to occur.

Senator Shaheen: And are you suggesting that we should organize it within the Department of Defense?

General Alexander: I think the Department of Defense has to have a key if not the lead role because when push comes to shove and somebody has to respond for the good of the Nation, it is the Defense Department. And if our Nation is under attack, they are the ones that are going to be held accountable.

Senator Shaheen: Thank you.

Mr. Scharre, you recently wrote about the dangers of radical transparency and how our adversaries would be able to exploit what our military does because they will be able to get that information because of our transparency. Can you explain or suggest what we might do to respond to that?

Mr. Scharre: Sure. So I think there are a couple of components of that. One is the digitization of Government data. Certainly we have seen this with incidents like Snowden and Bradley Manning and the ability to take large amounts of data. Now, there are obviously a number of efforts underway inside the Government.

But I think there is also an element of transparency in terms of our military operations being conducted. We have seen this transformed domestic policing in the United States. Now this era of ubiquitous smart phones where every action can be recorded. And I worry that our forces on the ground are not adequately trained and prepared for that. We have seen one-off incidents in these wars where there is an incident like Koran burning or someone urinating on corpses and their strategic effects. But a world where every action by one of our soldiers and marines on the ground is recorded and tweeted around in real time is something that I do not think we are prepared for. I say this in large part from personal experience fighting as an NCO on the ground in Iraq and Afghanistan where occasionally we will have interactions with the population where things are rough. These are difficult conflicts. But having it go viral is a very different kind of environment.

Senator Shaheen: My time is up. But, Mr. Chairman, if I could ask just one more question.

Secretary Gates, when he was here, referenced the fact that the U.S. Information Agency is defunct now and that our strategic efforts to communicate really pale in comparison to some of our adversaries. Certainly that is true with Russia. It is true with ISIS I think. And so how do any of you suggest that we better respond to that, and should those efforts to get out, given the challenges of transparency that you mentioned, but our need to do a better job in these areas -- how do we do that and who should head that effort? Should it be Defense? Should it be the State Department? Mr. Scharre, since you are answering.

Mr. Scharre: Yes. I think it is worth exploring the idea of a new agency. It is possible. That is a good solution. It is possible that does not help. But certainly we do need to adapt our communications to this digital and social media age.

Mr. Clark: I would add that I think one area that we have not fully exploited since the Cold War is taking advantage of the demonstration of new technologies, whether they are successful or not, and communicating that to potential adversaries to create uncertainty in their mind as to whether they are going to be successful. So we develop a new railgun. We develop a new laser. We develop an electronic warfare system that we think is going to offer a lot of promise. Or we go build a few of them and go

demonstrate them and then communicate that so that it is more widely understood. So I think we could take a radical transparency and turn around and use it for our own purposes by creating uncertainty in the minds of potential enemies.

Senator Shaheen: I certainly agree with that.

Dr. Singer?

Dr. Singer: Part of why they have been so successful at is they are using a technology that is inherently networked and coming at it with a network-style approach. So I would guard against us coming at it with a kind of 1940's centralized approach. That is part of why we are not doing well.

Second is they know specifically what they want to do. We have not yet figured out whether we want to counter-narrative or take them off the network or, in turn, take advantage of this very same radical transparency and intelligence gather on them. So on one hand, ISIL is getting its message out. On the other hand, we are gathering more information about them than any adversary before because of this. So we need to figure that out for ourselves.

And then third, why they have been able to do it in some manners better than us is that they have cohesion between their communication strategy and their battlefield operations. So, for example, before they launched the

operation against Mosul, they had preset hash tags ready to go. We do not have that kind of cohesion between our strategic communications and our battlefield operations.

Senator Shaheen: Thank you all.

Thank you, Mr. Chairman.

Chairman McCain: Senator Fischer?

Senator Fischer: Thank you, Mr. Chairman.

Dr. Singer, earlier you said the per-unit cost of the cart is driving where we steer the horse. I would like to open it up to the entire panel and ask what can we do about cutting. Where can we do less? A lot of times we talk about where we can do more. I would like your opinions on where we can do less with research, with buying, training. What will we not need in the future? Dr. Singer?

Dr. Singer: I think you have heard from the panel many great ideas, and the question is whether we will be able to implement them in shifts in everything from our personnel system and professional military education, all the way to the example of distinguishing between the type of systems and the requirements that we build for them when we approach it, the problem of legacy systems.

Another thing that I would put specifically on the table is our tendency to plan and assume for the best and then we act surprised when things do not work out that way. And that was what I was referencing in terms of the Pontiac

Aztek of war problem where we have systems -- and again, all of you are thinking about certain systems in terms of we develop a warship that our Navy's own tester says will not be survivable in combat, and then we act surprised and say, gosh, we got to fix that, or tanker aircraft that are planned not to be in anything above a medium threat environment. And then, of course, the enemy gets a vote, and we go, gosh, we should have figured out about that.

And what I am getting as that we too often, in an attempt to -- again, we get caught within this dynamic of the per-unit costs. It is shaping everything from what we develop to, oh, my goodness, we cannot change the amount we were planning to buy for what it will do to the future per-unit cost of it. And as part of this, we should also be able -- and I would associate myself with the other remarks -- revisualize how certain weapons systems can take on new and important roles the way the B-52 bomber, for example, went from strategic nuclear deterrence operations to close air support. We may be able to rethink that approach in everything from what is an aircraft carrier -- will submarines be able to take on that role -- to the long-range strike bomber. Is it just for strike, or will it be able to take on ISR or even air-to-air combat roles in the future? These are possibilities if we allow them to happen and not be locked in by past decisions.

Senator Fischer: Mr. Scharre?

Mr. Scharre: Thank you, Senator.

I think there is an issue of quantity. There certainly are places to trim the quantities of assets, not just to have fewer numbers of more capable things but then to trade that for larger numbers of lower-cost systems. And so moving to this issue of thinking about, as Dr. Singer mentioned, sort of the major combat assets as -- think of them as sort of a quarterback behind a fight, a bomber that is not just carrying assets to the fight, but the pilots are controlling a swarm of maybe lower-cost unmanned vehicles and a submarine as the hub of a network of autonomous undersea vehicles or undersea payloads that then expand the capabilities we actually have in the fight.

Mr. Clark: What this kind of points to is separating the platform, if you will, from the payload. So what we have done in the past is we have developed the ship or aircraft with all of its systems built into it, and we would then periodically modernize that by tearing it all apart and then rebuilding it all with new technology every 10 or 20 years or so. We need to move towards not buying the next generation of these aircraft and ships and other platforms in a way that integrates all those systems, but instead buy much cheaper and less equipped things and then equip them with payloads that can then adapt much more quickly over

time because the innovation cycle for something like a missile or a radar system or a passive radar sensor is much quicker than that of the overall platform. So we can afford to go to cheaper platforms.

So in terms of what we have today, I would not say that we want to throw stuff on the scrap heap that we currently have in the fleet, but we want to look at ways we can reequip it with the next generation of payloads. Instead of replacing them with another highly integrated airplane or ship, let us keep them, take out their old stuff, and just use then interchangeable payloads in the future to start reducing the cost of these platforms in the future. So to get to the F-35 example, so maybe the F-35 is the last aircraft we buy that is really a purpose-built strike fighter. To Dr. Singer's point, maybe you do end up with airplanes in the future that are just larger and have bigger sensors and they do all the missions and the payload changes to accommodate that.

General Alexander: Senator, I think one of the things that we should look at is -- the commercial industry spends billions if not trillions of dollars a year in cybersecurity alone. And when you think about all that money that is being spent, it is being spent to solve their problem. But they, if they work together, create a sector solution and that sector solution could be very important for defending

our country. If we had Government and industry work together in a way that was meaningful so that what they applied those resources for helped give them more reflective surface in cyber -- it would tell the Government when the Government has to act -- you could focus Government resources where it is really needed.

So I think the idea of having a war game and then looking at how you get the financial sector, the energy sector, the health care sector, and the Government together and maybe a few others, put those in a room and look at what they are doing, what you would find out is, you know, one big bank along is a spending almost $750 million a year in cybersecurity. What if it was done in a way that helped protect the whole sector, and if they worked together, that surface would be far better than anything the Government could do. We need them to do that so that the Government can focus on what you want, especially the Defense Department, to do.

Senator Fischer: Mr. Scharre, you were talking about swarms and a change in warfighting. If I could, Mr. Chairman, we hear about platforms. We hear about payloads. What about personnel? Are we going to be looking at the same infantry in 20, 30, 40 years? The infantry can take and hold ground. Can technology replace that?

Mr. Scharre: Well, I think technology can certainly

aid in taking ground. Yes. When it comes to holding it and then building up a security infrastructure that can pass on to someone else, that is something that is going to require interpersonal interaction.

Could we use robotic systems in war to help ground maneuver warfare? I think absolutely. And I think there is a lot of opportunities. The Army probably is not yet seizing to look at something like a modern day robotics, the Louisiana maneuvers, to experiment with maneuver warfare. But when it comes to sitting down with tribal elders, a person has got to do that.

Senator Fischer: Thank you.

Thank you, Mr. Chair.

Chairman McCain: Senator Kaine?

Senator Kaine: Thank you, Mr. Chairman.

And thank you to the witnesses.

General Alexander, you talked about and we read about all the time the number of cyber attacks on the Nation or on governmental agencies that are occurring with greater frequency. I think you use 350 cyber attacks. I am not sure what unit of time that was. Give us a good example of a counter cyber attack that the United States has undertaken. So when we have been attacked, give me a good example of something we have done in response.

General Alexander: Senator, I cannot give you that in

this forum, but I think that is something that would be good to discuss for the committee in a classified session.

Senator Kaine: I just want to make this point. I thought that was going to be your answer.

There is not a deterrence doctrine if people do not know what the response will be. The President last week said he was going send 50 special forces to Syria. I know to the number how many bombing raids we have run in the war against ISIL that is now in its nearly 16th month. We know the number of personnel that are deployed.

When the American public and policymakers read over and over again in the press about cyber attacks on the Nation, they are very public. But when we cannot discuss even with the committee in a public setting or with the American public what we are doing in response, it kind of leads to a little bit of a feeling of like we are impotent against these attacks. And I know that we are not. But if we can talk about troop deployments in the war on ISIL and bombing sorties that are run but we cannot talk in open session about what we do in response to cyber attacks that are every bit in the public news as any of the bombing campaigns are, I think it really leads to a sense of helplessness by the public and the committees themselves. I hope we will have a follow-up and talk about this.

General Alexander: Could I offer, Senator?

Senator Kaine: Please.

General Alexander: Let us go hypothetical instead of actual, and we could talk about hypothetically what the Defense Department could do and others.

Senator Kaine: I would rather actually move to another topic. Hypotheticals are great. Why can we know actual in so many realms of what we do in defense, but we are not willing to talk actual about cyber? Because we certainly hear about the actual attacks on us. So I think that raises a question I would like to explore more.

A very interesting hearing, all your written testimony and oral testimony too. And the title was provocative, "the Future of Warfare." A lot of the discussion has been about technical technology issues.

I think one of the interesting areas about the future of warfare is the question of unilateral being with partners. We were attacked on 9/11 by al Qaeda and we immediately assembled a coalition that amounted to about 60 nations to try to respond to that. The first thought after the attack on Pearl Harbor was not we ought to go out and assemble a coalition, although there were other nations, obviously the allied nations that were involved in World War II.

Is there something unique about the future -- certainly the current and the future of warfare that renders this

whole idea of coalitions kind of more of a common feature? The F-35 is a platform that was built with the participation of nine partner nations, not just different service branches but partner nations. Talk about coalitions and alliances in the future of warfare. I would just be curious to any of your thoughts about that.

General Alexander: If I could, in the cyber realm, we would be much better off with partners in this area. Think about the undersea cables. They come from the United Kingdom to us, 12 of the 17 or 18. So the United Kingdom and Europe -- if they had a similar approach to cybersecurity and they agreed to defend their end, we defend our end, we have now moved our defense out to Europe for our country. I think that is a very good thing and we could do things like that in this space. So I do believe there is much need for collaboration, but it also brings in all the issues now you have with civil liberties and privacy because every nation sees it different, even in Europe. Every one of those see it differently. So I think we have got to set the standard, and that is one of the things that we could do as a country.

Mr. Clark: I would say the benefit that we get from coalitions, though, is primarily non-material. I would argue that they do not bring a lot of necessarily military capabilities to bear that are easily applied in a unified

command context. It actually makes it a little bit harder if you are trying to do it with multiple nations' forces. But what they do bring, as General Alexander was saying, is access to areas that we would otherwise not be able to base from or operate from or be able to monitor.

And it also provides, if you will, the political top cover so that if we can demonstrate that that is the way that we are used to operating, it may drive our competitors or our adversaries into a calculation where they realize that, well, I am not just going to be upsetting the United States if I take this action, but I will also be upsetting a number of my other neighbors, which could create other problems down the road politically for them. So there may be a political benefit in the long term to us managing things through a coalition.

Chairman McCain: Senator Rounds?

Senator Rounds: Thank you, Mr. Chairman.

General Alexander, do we have a stated doctrine with regard to what is a cyber attack or do we have a defined limit where we identify something as an act of war if our defense, our energy, or our financial resources are attacked?

General Alexander: The only thing that I know that comes close to that is the President's statement of 2009 about how we would respond using any form of power, cyber,

military, diplomatic, to respond to a cyber. There are no rules of the road or red lines in cyber. I think war games can help tighten some of that up and should.

Senator Rounds: Would anyone disagree with that analysis?

Mr. Clark: I would add one thing, that one of the challenges you have in cyber is that if we try to use a cyber capability to respond to a cyber attack, we may end up making clear to the adversary the access that we have into his networks. So one problem we have is we do not want to burn the source. And so if we are attacked in cyberspace, we might need to go to some other means to respond because we do not want to give up the fact that we have got access to his networks and are able then to monitor his activities in the future. And as General Alexander said, we might be able to take advantage of the attack to actually gain new access that we do not want to make clear to the enemy.

Senator Rounds: Yes. Mr. Singer?

Dr. Singer: I would just add the key is not the means. It is not that it is cyber. It is the end effect which will determine it. So whether it is through cyber or a missile as to whether it causes loss of life, physical damage, even if someone set a -- a foreign adversary set a fire that killed hundreds of Americans, we would not say, gosh, you used matches not cyber or a missile. So cyber can be a

little bit of a misdirection. It is more about the end effect and how we judge that.

Senator Rounds: Do we need a different doctrine? Do we need an established doctrine to determine whether or not a cyber act is an act of war?

Mr. Clark: I would say we need to have a real clear definition of what we think constitutes an attack that would be meriting of a response because we do that in the physical realm to a much greater degree. Obviously, this gets built up as a body of action over time. So it is precedent that does it to some extent.

General Alexander: If I could, to answer that question, I think when you look at our NATO responsibilities, I think we do have to have this laid out. What we cannot do is walk into a war because we did not understand that this would be an act of war so that if someone were to attack one of our NATO allies and cause destruction and lives, what constitutes an act of war is not really clearly stated. There has been a lot of stuff in the Tallinn Papers that have been written, but it does not get to the point of this is clear. And so I think we need to have those discussions in a classified and unclassified realm so everybody understands. And I do agree with it is the intent of the individuals. If their intent is to do harm, I think you now need to look at where you take --

Senator Rounds: Would you share with me what you consider to be an appropriate response should there be an act of war in the cyber realm?

General Alexander: I think first ideally you could prevent it, but if you could not prevent it, I think you now have two things that are going on, the resilience in your networks, bringing those back up, and then a whole series of actions from political, economic, diplomatic, military. And in cyber, there are a lot of things you could do to stop that nation from communicating outside that nation with other tools. And I think it is those types of capabilities and wargaming and things that ought to be looked at analogous to the way we did armored warfare 70 years ago.

Senator Rounds: Sometimes we talk about this in a way in which we have a tendency to literally scare ourselves because we are talking about how serious these could be. Do we have the capability and the resources right now to actually respond should we have that type of a cyber attack that would amount to -- if we define it properly as an act of war, are we in a position today as a country to respond to an act of war?

General Alexander: We have 40 offensive teams that were created at U.S. Cyber Command. Those teams have some great capabilities. It does not cover the whole world, but it gives you a great starting point. And I think our first

thought in 2010 was let us set up with the initial force structure that we needed it, set it up in terms of offense and defense in teams that could actually do offensive actions to defend the country.

Senator Rounds: Anyone have anything to add to that? Yes, sir. Dr. Singer?

Dr. Singer: I would just add two things. The first is the idea of assuming that our response would have to be limited just to cyber means. If someone carries out an act of war against us using cyber means, we are not and should not be limited in our response to use other means. And that is why we are seeing that kind of deterrence hold.

The second, though, is to -- as General Alexander said, we have built up great cyber offense capability. There are many things that Mr. Snowden did, but one of the other things he did is revealed that we have very potent cyber offense capability. I would add, though, to those who believe that building up more will deliver deterrence, the question why has that not delivered deterrence yet. There is no question that we have great cyber offense capability and yet the attacks have continued to come. That is why I echo back to we need to do more about building up deterrence through denial which is making ourselves more resilient both in military and civilian means so we can shrug off those attacks, which therefore makes the attacks less productive,

less likely on us.

Senator Rounds: Thank you, Mr. Chairman.

Chairman McCain: Senator King?

Senator King: Thank you, Mr. Chairman.

Dr. Singer, I must compliment you. To found a technology advisory firm called NeoLuddite is an act of genius.

I also enjoyed your Churchill quote. One of my favorite Churchill quotes was he was once asked how he thought history would treat his role in World War II. His response was, very well because I intend to write it.

On this issue of deterrence -- and I think Senator Rounds really hit the point, and I think we should follow up on this. It is the question of what is an act of war and when will we respond because if an act of war is not defined, your opponent has to know that you are going to consider it an act of war and that there will be a response. And, Mr. Singer, I think your point is well taken, that it does not necessarily have to be a cyber response. But I do think there does need to be some response. Deterrence by denial, it seems to me -- ultimately you have got to have some offensive capability. You have got to be able to punch back or you are simply always on the defensive. You are nodding your head. I assume you agree with that concept.

Dr. Singer: I very much agree. I will compliment you

in turn. Thank you for your kind words.

I have an article coming out next week on this question of deterrence and the three approaches are what the committees wrestled with. It is one to set very clear norms so both sides or all the sides understand what is and is not an act of war so that there is no miscalculation.

The second is to understand that you can respond, but you can respond in many other means, many other areas and it is not just through military. It may be through trade. It may be through espionage, whatever. There was a far more complex game going on in the Cold War where your only response was you hit me with a nuke. I threaten to hit you back.

And then the third is this point about deterrence by denial, something that was not possible in the Cold War. The idea of civilian involvement was kind of -- you know, the bomb shelters and the like were not very useful. Deterrence by denial, though, now would be an incredible useful concept, and importantly, resilience works not just against state-level attacks, but it is also effective against all the other attacks out there, whether it is non-state actors like terrorists or just criminal groups.

Senator King: On that point, General, good to see you again. And I think a point you made that I had not really thought about was the idea of a joint private sector

cybersecurity effort perhaps facilitated by the Government but not with Government involvement so we do not have the privacy issues. But it strikes me as inefficient in the extreme to have Bank of America spending billions on cybersecurity and Anthem and Target and Walmart when, in reality, they are all chasing the same problem. And it may be that a consortium -- as I recall, there was a semiconductor consortium some years ago -- to deal with this in a joint way might save the private sector a lot of money. The Government could just act as a facilitator.

Dr. Clark, I think an important point that has been made today -- and it was made in one of the hearings the other day -- was instead of building weapons systems that have absolutely everything that are going to last 40 years and therefore, by definition, be obsolete, we ought to building modular systems, if you will, that can be modernized on the fly rather than starting all over again. Is that essentially what your testimony was?

Mr. Clark: Yes, definitely. That gives you the ability to take advantage of the technology refresh cycle that exists for those smaller systems. We talked about Moore's Law and how that results in a doubling of computer programming power every 12 to 18 months. And the computer is really the heart of almost every one of our payloads, whether it is a sensor or a missile or even a smart bomb

today, or unmanned vehicle. So we should take advantage of the fact that that technology refresh cycle is going to be so fast and develop those payloads on a much faster timeline.

Senator King: And trying to develop a weapon system that has everything for everybody at one time that will be fixed in time is just the wrong way to go.

Mr. Clark: Which gets back to the requirements problem. If I define my requirements in isolation from what the technology might be able to give me in a near-term time frame, I end up aspiring to something I will never be able to achieve.

Senator King: And the requirements proliferate because everybody wants their -- it is the problem of a camel is a horse designed by a committee.

Mr. Clark: Right, instead of defining requirements in conjunction with what your technology is already delivering.

Senator King: Dr. Singer, if your article has not gone to press, I would urge a quote from Robert Frost, good fences make good neighbors. When people know what the rules are, that is when you can avoid conflict.

A final question just for the record. General Alexander, very chilling in your early testimony that we will not have time for human decision-making in responding to some of these kinds of attacks. In other words, the 30

minutes or an hour for the missiles is now in a matter of seconds. The question is how do we war-game and prepare a response that can be done instantaneously without the intervention of human discretion. I think that is an issue -- my time has expired, but I think that is an issue that deserves some serious thought and discussion.

Thank you, gentlemen, very much. This has been very illuminating.

Chairman McCain: Dr. Singer, I would suggest words of Chairman Mao. It is always darkest before it is totally black.

[Laughter.]

Chairman McCain: Senator Ernst?

Senator Ernst: Thank you, Mr. Chair.

Gentlemen, thank you for your support to our Nation in so many varying ways. I think the discussion today has been very beneficial I think for all of us and our constituencies.

General Alexander, I would like to start with you, sir. We have spent a lot of time talking about the cyber threats that exist out there and the devastating effects to our networks, should they be attacked or when they are attacked, and really the ability to recruit and retain some talent to deal with the cutting-edge threats that exist out there.

What I would like to know is a little bit more. How

can we utilize our Reserve and our National Guard forces to bring in some of the best and the brightest? We have a lot of folks that certainly serve in very similar capacities in their civilian employment. Is there a way that we can use them to leverage our forces?

General Alexander: Actually, Senator, that is a great question. We were doing that when I was on. I know that continues. So each of the National Guard units are setting up cyber teams that would also help. And as you note, some of these have some of the best technical experts in civilian industry that partner with us. So you go out to the State of Washington with Microsoft employees or all around the world -- all around the U.S. I think there are some great partnerships there, and it also gives you an opportunity to bring those on to active duty when you need them and then taking them off.

Finally, if we work it right, it also helps provide security for the State and local government.

Senator Ernst: I think that is wonderful. I know that in my transportation company, we had some computer whizzes working in the civilian industry. They were truck drivers when we were mobilized. But a lot of talent that exists out there.

And, Mr. Scharre, Paul, I know that we have spent some time talking about future personnel generations in our

Department of Defense. And I would like to visit a little bit with you about, again, the National Guard and the Reserves and where you see their role in the future, whether it is Army, Navy, Air Force, Marines, and how they can support future conflicts.

Mr. Scharre: Thanks, Senator.

I think this issue of civilian expertise is a unique capability that the National Guard and Reserve brings to the table. And your example of computer experts driving trucks -- and I saw active duty reservists -- many similar things in Iraq -- were even doing civil affairs functions. We still had people misaligned. We are not as aligned as well as maybe they could be with some of these skills that actually are resident in a Guard and Reserve force. And so a process inside the Department to actually identify -- have service members self-identify those skills and allow them to be tracked inside the Department so that if the Nation needs to be able to draw upon that, we could know who are these experts would be extremely valuable and I think a way to really increase even further the skills and capabilities that the National Guard and Reserve bring to the table.

Senator Ernst: I think that is a great idea. I know that we do identify many of our civilian skill sets through the Guard and Reserves, but I do not know that the DOD truly pays attention to that. And I think we have a lot of, as I

said, talent and abilities that could be better utilized on or with an active duty force.

Do you think that the DOD will continue to rely heavily upon our Guard and Reserves as we move into future conflicts in outlying years as heavily as they have maybe in the past 14 years?

Mr. Scharre: I think there is no question they will continue to play a valuable role. Certainly we have asked a lot of Guard and Reserve members, and they have given a lot in the last 14 years. And so I think they will continue to be a valuable contributor in the future.

Senator Ernst: Thank you.

I will move on to a different topic and, Mr. Clark, maybe you can assist with this. Today I did lead a number of my colleagues in a letter regarding our concern for Russia's activities near some of our underwater cables. And it is very concerning because these are fiber optic cables and they carry everything from sensitive information, communications, many of these things that are vital to our economic stability. And I know that it is a very sensitive topic, but I think it is pretty vital that we start talking about our interests in underwater fiber optic cables.

So are you concerned at all about the security that we have that either exists or does not exist out there? And if you could expound on that, please.

Mr. Clark: I am very concerned about it. Those cables carry trillions of dollars in financial transactions every year. About 90 percent of the world's economy runs on undersea cables as a result of that.

And the Russians for a long time have had an undersea reconnaissance program where they go and look at things under the water, and they have taken an interest recently in undersea cables. We can tell by the areas where they are operating that they are looking for something down there in the vicinity of undersea cables.

Out in the open ocean, these undersea cables are fairly hard to find because you kind of have to search a large area. But in the areas where they have their landings on the shore, either the United States, over in Europe, or in the Middle East, they are relatively easy to locate and then trace back into the water.

I think one concern we would have is in conflict. Those cables could be easily broken. They are broken fairly regularly today as a result of trawlers or anchors that take them up. And today the responsibility for responding or replacing or repairing those cables lies with industry. And so they have on call the cable laying ships that go out and fix them. But you are talking about time frames of weeks to months to repair a cable that has been damaged as a result of either hostile or accidental action.

So one concern I would have is we need to improve the ability to rapidly respond to these kinds of attacks to be able to restore the activity on those cables. And then two, we need to have better monitoring capabilities in the vicinity of these landings where it is a target-rich environment for an undersea vehicle or a ship that is going to deploy a remotely operated vehicle to go attack them.

But there are technologies out there that could provide the ability to monitor these areas pretty well, but counter-UAV technology will be a key part of it and being able to find something small like Dr. Singer and Mr. Scharre have talked about is going to be really hard. So we need to come up with better capabilities to detect these very small underwater vehicles that could be used against undersea cables. But it is a huge potential vulnerability that could be exploited both in peacetime or in war.

Senator Ernst: Yes, I agree. Thank you very much. I appreciate that. I think that that is something that we need to turn our direction to also.

So thank you, Mr. Chair.

Chairman McCain: Senator Hirono?

Senator Hirono: Thank you, Mr. Chairman and to all of you who are testifying.

The Defense Department has used a technology, basically quality over quantity, to stay ahead of the other countries.

So one of the other hearings we had said that we are falling behind in our ability to rely on our technical superiority. So do you share that view, and if so, what are some very fundamental steps we should be taking in order to increase our capacity, technological capacity? Any of you can answer.

Mr. Scharre: I will start.

I think one of the main factors is time. How do we shorten the time by which we develop major programs? Mr. Clark talked about modularity, thinking about payloads over platforms. I would also encourage us to think about software over payloads. You can upgrade software very rapidly. But there are even some more sort of fundamental shifts that people are thinking about. You know, this DARPA program that I mentioned earlier SoSITE, is thinking about basically taking a major platform and breaking it apart entirely into a larger number of basically just the payloads that are all interacting together, and that is something worth experimenting with and exploring.

Senator Hirono: So are you saying that we should spend more money on R&D or is it also the way we are structuring how the money is spent?

Mr. Scharre: I think the way in which you spend the money is absolutely critical.

Senator Hirono: And how would you change how we are

spending our money?

Mr. Scharre: The R&D spending in the Department is very decentralized and fragmented. And so just a more centralized process that focuses, as Mr. Clark mentioned, on the key areas, and this effort is underway with the LRDP, long-range something something defense acronym -- you know, I think are beneficial in that regard.

Dr. Singer: Senator, I would just add. I think it is both the way, but we also clearly do not spend enough on R&D. And we have seen the percentages go down both on the Government side but also as a Nation, as was mentioned, in the defense industry side as well. And the issue of quantity/quality is not just in terms of the weapon system but just simply if you run out of missiles, say, for example, in a fight, you will have to exit. So you may survive but you have deferred to the enemy in that time.

Senator Hirono: Did you want to --

Mr. Clark: I would just add one more thing is that we have a pretty good investment inside DOD in R&D. It is not well focused, as we talked about.

In addition to that, industry used to do a lot of internal research and development with their own money to go explore new military capabilities that might be beneficial in the future. They have reduced that investment significantly with the reduction over the last several years

in the amount of procurement because it is normally a percentage of procurement. And also there are some things that the Department is doing that has been disincentivizing industry from pursuing its own internal research and development that has in the past given us things like stealth and things like new radar technology. So I think one thing we ought to look at is how do we encourage industry to be independently looking at problems that they could address with their new technologies.

Senator Hirono: And perhaps one of the ways that we incentivize the private sector is, of course, to have the potential of technology transfer in whatever research that they are doing and developing.

For Mr. Scharre and Mr. Clark, what impacts do you anticipate our reliance on fossil fuels will have on our planning and the effectiveness of our future warfighters? And what is your assessment of the Department's progress in terms of reducing its reliance on fossil fuel sources?

Mr. Scharre: I think there are a couple key reasons to do so. One is, of course, strategic risk and vulnerability. Another one is cost. But an important one is alternative energy solutions can help increase the endurance for many various sort of long-endurance capabilities, particularly robotics, that we could put out on the battlefield. So things like better batteries, fuel cells, solar power can

allow us to put persistent surveillance sensors out there to help detect the enemy for a very long period of time, months or years at a time. And so there are some significant operational advantages as well.

Mr. Clark: It is about not so much fossil fuels as just reducing our energy dependence in general because what you see is we have to project forces over a very long distance because all of our friends and allies are an ocean away from us. So we are generally transferring those forces over a long distance, and even when they get there, they are having to operate at the very edge of our logistics chain. So reducing the amount of energy they need in general would be important. And taking advantage of technologies that do not require fuel at all would be important. So the idea of going to new battery technologies that are able to last for a very long period time and then eventually be recharged by the sun or by returning to some docking station would be a very good way for us to reduce the tether that we have to maintain because right now we have to have refueling aircraft and ships out at the edge with the ships that they are refueling and then refuel a ship, for example, every few days while it is operating, and then aircraft, obviously, have to operate for a much shorter period of time before they need to be refueled. So moving to energy technologies that do not require fuel to be delivered to the platform on

a regular basis I think would be very important.

Senator Hirono: Thank you.

Chairman McCain: Senator Sullivan?

Senator Sullivan: Thank you, Mr. Chair.

Sorry Senator Hirono and I had to step out for a few minutes. We were actually celebrating the 240th birthday of the United States Marine Corps. So we had to welcome the chair and ranking member as members of the Navy and the Army.

Chairman McCain: A dark day.

[Laughter.]

Senator Sullivan: Gentlemen, thanks very much for your testimony.

General Alexander, I was actually struck by your testimony in one area that -- well, in a couple areas I thought it was very insightful. But one of the things that we have been hearing about in terms of cyber is this idea that -- this notion that we are constantly being attacked, we are constantly -- and you mentioned it. And some of the dollars and statistics you have in your testimony on cyber crime and what that costs is really eye-popping.

But there has been this notion of us being on defense, defense, defense. One thing that I liked about your testimony is that you talked about a little in terms of offense where we have invented a lot of this technology. We

are the leader in it still. So there are all kinds of opportunities for offense.

Could you just provide some examples of that? I mean, the chairman's opening statement about turning technologies into offensive advantages I think was very illuminating from a historical perspective. But what are some opportunities in terms of offense that we have with regard to cyber?

General Alexander: Well, there are a number of offensive capabilities. I think first and foremost you have to be able to see what the adversary is doing, hence the need for the commercial sector to be part of the solution so what is hitting them can be seen by everyone. So if you think about how two computers actually talk -- you know, I want to talk to you. You come back and say on this channel. We go to the ACK and NAK kind of thing. That takes time, milliseconds. And if you think about some computer trying to get in while that is happening, if the Government can see it, the Government can stop it or at least delay it or stop the router or do things with it. So what you have is opportunities to change what is happening in cyberspace with offensive tools that would defend the country.

And the issue comes down to so what would you authorize, for example, Cyber Command to do in order to defend it. You might say, well, I am going to let you do everything you can to block all the way to where it is

originating from, but I do not want you to destroy systems yet. Destroying systems is going to go a step further. But technically speaking -- and you have seen this -- you could destroy a computer in cyberspace by getting on it and doing certain things to it. So the technical ability is there. It is public record. Now all you need is access, and how you get into that access is where you take the capabilities of an NSA with a Cyber Command and FBI at times and put those together. So you have tremendous opportunities.

And I think when we look back at our capability, you look at we are the most integrated networked society in the world. And we look back, and we say look at all these opportunities in the offense, and then you look at ours on the defense. You would say, man, we are broke. If we throw rocks, we have all these glass windows. First step, fix those.

Senator Sullivan: Let me ask just kind of a related question on -- I know there has been a lot of discussion in this testimony on deterrence or raising the costs of cyber attacks. And it seems to me -- and I would welcome any of your opinions -- that if you are from an authoritarian regime like Russia or Iran or China, they in some ways have an advantage because they can just deny and lie. No, we had nothing to do with that, even though they did or they do.

But you mentioned like one example to me that the

Iranians were attacking our financial system. Would it make sense for us to say publicly that if you do that again, we will crash your entire financial sector? Is that the kind of thing that we should be looking at in terms of raising the cost? Because it seems to me if you are an authoritarian regime, you can lie about who is doing it, that the costs of actually all these attacks is almost minimal because we do not react. Should we maybe look at being a little more public in upping the ante and saying if you do this, North Korea, Iran, China, we will respond? In some of these countries, I am sure we could crash their whole economy. What would be a problem with that kind of deterrence that makes it a little more transparent but raises the cost dramatically? Then, of course, if we announce that, we would have to act. I am curious. Any of the panelists, what would you think of something a little more transparent from our perspective, and do we have a disadvantage when we are dealing with authoritarian regimes that routinely lie about this issue?

Mr. Clark: I would say one thing we have to think about is the fact that the deterrent action might need to be fairly proportional with the action it is intended to deter because it will not have credibility otherwise. If we say that because the Iranians are attacking some of our banking sector, that we would go and crash their financial system,

that might be disproportional, and therefore they do not find that to be a credible threat because they will say, well, they will never do that.

Senator Sullivan: But what if we did it?

Mr. Clark: Well, if we did it, it may deter further action, but it may be seen by the international community as being highly disproportionate. So we might need to come up with a more proportional reaction to things like that so that the adversary will say, well, he actually could do that. I mean, this is something that the United States could do in response.

And that gets to where maybe the response needs to be not in cyberspace but in another domain, for example, electronic warfare, jamming, small attacks on oil infrastructure. Those could all be undertaken with a relatively small amount of collateral effects while also demonstrating the resolve of the United States and being able to do something that they would find to be credible and that we could repeat but that does not cause such a huge damaging reaction that people are not going to believe we will ever use it.

Dr. Singer: Senator, the challenge in this is there is not the mutual, in terms of the old mutual shared destruction. So, for example, we are far more vulnerable to cyber attack than North Korea, but that is actually a good

thing because we are integrated with the global economy. We have freedom. We have all these other things. We would not want to be in that position that they are in. So recognizing the lack of mutuality, echoing the points about maybe looking at other deterrence angles.

But I would add one more important thing. When we are talking about offense, when we are talking about steering Cyber Command to taking on these roles and the civilian lead, it is moving it and us away from its role in clear warfare itself, and the determinant of success or failure in future wars with cyber will not be thinking about it individually but will be how it is integrated with other warfighting capacity. So the more we focus on the power grid, the less it is integrating that cyber capability in terms of war, using it to take down an air defense so it is cohesive with your warplanes going over as, for example, Israel was able to pull off in Operation Orchard. So what I am getting at is be careful of steering Cyber Command more and more towards civilian roles. It may lead us to success in non-war but set us up for a fall in real war.

General Alexander: I just want to add some clarity to that to make sure that, at least from my perspective, you understand because where you can get commercial industry to help is to do their part. That is the war game and the effort. But Cyber Command and our Defense Department cannot

work without the energy sector. If that is shut down, we got a problem. Our Defense Department needs to defend the nation in this area. I am not proposing that they go in and prop up any energy company or any of these. Help them build the right cybersecurity so that we know they can defend themselves and call for help when they need it, and then push that out beyond the boundary.

But I think our Defense Department has to think more comprehensively of this whole thing. I agree. Going after all targets and stuff is part of it. But my concern is the easy thing, if I were a bad guy, I would just go after our infrastructure. I would take it out before you could respond. And that is what the Chinese approach to warfare is. So I think we have to put all that on the table, war-game it, and then ensure we have it correct.

Senator Sullivan: Thank you.

Thank you, Mr. Chairman.

Chairman McCain: Senator Ayotte?

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

I wanted to follow up, General Alexander, on something that you had in your prepared statement, and you wrote that Russia's intervention in Ukraine and in Syria -- the Syrian conflict are just the start of a potential series of actions that seek to reshape the international environment. So I

wanted to get your assessment based on all your experience of what comes next with Moscow and what should we be doing to respond.

General Alexander: Well, my greatest concern is eastern Ukraine. I think everything that is going on is for Putin to get more closure on eastern Ukraine where the weapons platforms that he really cares about are created. I think he wants control of that. And I think by pushing what he has done, he is going to continue to go for that. There is nothing that I have seen that would indicate he is going to stop from doing that, and I think he will lie. He will do everything he can and then help make that happen.

Syria is a great way to push -- you know, think of it as a faint. He can accomplish some real objectives there between Iran, Syria, and Russia, and he is doing that by helping to shape what he thinks are the best proxies for Russia, Syria and Iran, in the region. So he wins twice there. It takes our focus off eastern Ukraine -- people are still dying there -- and focuses everybody on Syria. I would not be surprised if over the next 6 months we see some more action in eastern Ukraine at the same time.

With respect to Syria, what I am really concerned about is the tension it creates up. We get to a point where we have to fire back against Russia or Iran for their actions in Syria. If we do that, I think we are going to see their

response in cyber. I really do because there is no way Iran can come after us. They can launch terrorist attacks. We have been fairly good at stopping those, but they can hit us with cyber. And it goes back to what is a credible deterrence. What happens if they change their approach from disruptive attacks against the financial sector to destructive against the financial and the energy.

Senator Ayotte: So I guess I would -- anyone who wants to comment on this. But as I hear you discuss this, I think if we let him continue to do this without any response, as far as I can see, does this not almost become a fait accompli, which we could see ourselves headed in this direction which is going to require -- you know, put us in a more dangerous situation? If you were advising right now the President, what would you tell him to do to respond to Putin?

Mr. Clark: I would say refocus back on Ukraine. So Syria is obviously a very dynamic and difficult situation, but Ukraine is a situation where we have a friend of the United States, not an ally, but a partner that is under threat and attack by Russia and providing the Ukrainians the capability to better defend themselves in the electromagnetic spectrum, as well as in cyber, would be really important to giving them the capability to defend themselves and disrupt the Russian attempts to gain more

territory. And that would force Putin to now refocus his effort back onto that and make a determination as to whether he is going to be resolved and continue in Ukraine or if he is going to eventually recede. But right now, because we have not been focused on it, he is able to continue to accrete influence without any counter.

General Alexander: If I could. I agree. I think our vital interests in Eastern Europe and in the Middle East are at risk. I think we have already had some outcomes of the Iranian deal. I think having some deal with Iran to stop nuclear weapons is important, but we lost some of our allies in doing this. And losing those allies is something we cannot afford to have happen. So I think we have to step back and say what is our strategy for both. We are going to have to deal with both at the same time. In the Middle East, we need our allies to know we are going to stand beside them. It is the same thing in eastern Ukraine because everybody is looking at it. They say you have made all these declarations about NATO about you are going to be there for us. So what happens? Are you going to be there?

And at times, unintentionally our actions may look like we are not. And what I am concerned about when you talk to Saudis, the Israelis, and others, they think hold it. Are you here with us or are you with Iran? What is your objective? I think we have to clarify that. Our Nation

needs to let our allies know we are there for them. I think that is the first and most important thing we should do, and we should discuss with them how we are going to stop issues in the Ukraine with NATO and what we are going to do in the Middle East to shore up our allies there.

Senator Ayotte: Does anyone want to add to that?

Dr. Singer: I would just add that the last several decades of U.S. foreign policy strategy, defense strategy has been focused on the challenge set of networks of individuals, criminals, insurgents, terrorists and the problem set of failed states. And moving forward, we are going to have to recognize that whether it is Russia or also China, we have a return to great state competition, and what that means is that when we look at certain areas, we need to look at it through a lens of not just the failed state but proxy warfare as well. And I think we are seeing certain echoes of that and we are going to be able to learn the lessons from the past of what does and does not work in proxy warfare and reframe our approaches along those lines. And on top of this is focusing on how do you keep a lid -- how do you win a competition, but also keep a lid on it from escalating.

Senator Ayotte: Thank you all. Appreciate it.

Chairman McCain: General, just to follow up on your comment to Senator Ayotte, you say we would have to take

some actions to reassure our allies or other nations in the region in the Middle East. What actions would those be?

General Alexander: I think we need to reach out to Saudi Arabia, United Arab Emirates, Kuwait, Jordan, and Egypt and sit down with them and say we are here. I think some of things that we ought to talk about is --

Chairman McCain: We say that all the time, by the way.

General Alexander: You know, when you look at it, when you look at Egypt, perhaps some of the best comments I have heard on a strategy for Egypt was, well, how do you get them stability. How do you get them security? You got to have energy to growing jobs. You got to give these guys jobs. 24 percent unemployment is really bad for us. It is bad for the world. How do we help get the Middle East in place? They have enough money to do it. We have the expertise to help them get there. I think we have got to look at the security, the stability, the energy sector, and the jobs, the economic development for the Middle East to get them to a place where they can be looking forward to their future versus fighting all these issues that we are seeing with radical Islam. So I think a comprehensive program like that, led by our country and others in the Middle East, is a step forward and let them know that we are going to be there not just for a couple hours but for the next several decades.

Chairman McCain: Right now, the Egyptian regime is becoming more and more repressive. 45,000 people in prison, no semblance of any real progress on a number of areas which are in contradiction to our fundamental principles.

General Alexander: This is a tough area. I have been to Egypt several times, and there is no good solution without economic growth. So I guess the question, Chairman, is how do we help them get out of this because in my dealings with our counterparts, they understand and want to do it. How do you get there? And there is so much tension in that region. If we do not help them get to economic growth, what they are going to have is continued failed states, and with those failed states, now we got -- it is just another one. And so it seems to me at some point we have got to come up with a strategy that counters that. And I personally believe that that is some way of developing their economies.

Chairman McCain: Dr. Singer, I have your book on my desk admittedly in a pile of books on my desk. I will move it to the top of the pile. The next time I encounter you, I will be able to give you a vigorous critique of the thesis that you espouse in that book. Congratulations on its success.

Mr. Scharre, thank you for your articulate answers to the questions.

And Mr. Clark and General Alexander, a special thanks to you for your past service but also it will be the intention -- and we do work on a bipartisan basis, as you know, with this committee -- to start looking at the follow-on to the cyber legislation that we just passed through the Senate. And we will be calling on all of you as we move forward with that effort. I think you would agree that additional legislation is necessary. Would you agree with that, General?

General Alexander: I do, Chairman.

Chairman McCain: Thank you.

Jack?

Senator Reed: Mr. Chairman, this was an extraordinarily insightful panel. I am not surprised. You chose wisely, a West Point graduate whose fleet commander shaped his life. You have a submarine officer. You have an Army Ranger, and you have a graduate of Harvard University. So good job, Mr. Chairman.

Chairman McCain: The hearing is adjourned.

[Whereupon, at 11:46 a.m., the hearing was adjourned.]