THE BROOKINGS INSTITUTION

DEFENDING THE NATION AT NETWORK SPEED

A DISCUSSION ON CYBERSECURITY WITH GENERAL MARTIN E. DEMPSEY, U.S. ARMY

Washington, D.C.

Thursday, June 27, 2013

Introduction and Moderator:

PETER SINGER
Senior Fellow and Director, Center for 21st
Century Security and Intelligence
The Brookings Institution

Featured Speaker:

GENERAL MARTIN E. DEMPSEY, USA
Chairman
Joint Chiefs of Staff

* * * * *

P R O C E E D I N G S

MR. SINGER: Hello, I'm Peter Singer, Director of the Center for 21st Century Security Intelligence in Brookings, I'm delighted to welcome you all to this event. I'd like to begin it with a story. The first time I ever saw a computer, I was 7 years old, my father took me to a science museum in North Carolina to see a Commodore computer, if you remember those. And then I took a class to learn how to program one of the most important inventions in the history of mankind, to design a smiley face, which then printed out on one of those spool printers that you tore the perforated paper from the side of it.

Three decades later, the centrality of computers to our lives is almost impossible to comprehend. Indeed, we're so surrounded by computers that we don't even think of them as computers anymore; we're woken by computerized clocks, we take showers in water that's regulated by a computer, we drink coffee made in a computer, eat oatmeal that's been heated up in a computer, drive to work in a car that has hundreds of computers in it while we sneakily check the news on a phone that is really a computer. And then at work, we spend much of our day pushing buttons on a computer, an experience which was once so futuristic that it was the job that George Jetson had. Remember, he was a Digital Index Operator, which was this crazy concept back in the 1960s, that you would work behind a computer.

But what's truly important is that these machines are not just omnipresent, they're now connected. Computers once stood alone, literally linked to nothing else than the electrical socket and maybe that printer. Just a generation ago, the concept of cyber space was a word that the writer William Gibson made up for a science fiction novel that he was writing, mashing together the word cybernetics and space to describe his concept of "A graphic representation of data abstracted from the banks of every computer in the human system. Lines of light ranged in the nonspace of the mind, clusters and constellations of data."

This nonspace of the mind is real, and it's connected at network speed. The first electronic mail, email, was sent in 1971, today over 40 trillion email are sent every year. The first website was made in 1991, today there are over 30 trillion individual web pages. Moreover, the internet is no longer just about sending mail or compiling information, it's integral from everything to the operation of our electrical plants to the tracking of purchases of Barbie dolls, to our topic of today; the core functions of the U.S. military and its role in national security.

This realm of communication and connection has allowed globally networked military operations, which, in turn, has led to immense military reliance on this, with well over 98 percent of U.S. government communications going over privately owned networks. And, in turn, it's meant that it's a growing space for both contestation and even conflict. And so, much as how science fiction technologies of a century ago, like the submarine or the flying machine, allowed us to access new domains, and then led to fundamental questions in everything from international law to military doctrine, so has the emergence of cyberspace posed deep questions in everything from policy to law to ethics and doctrine.

And, of course, just like the rise of new forces back then, like the undersea warfare community, or the Army Air Corps turned into the Air Force, this new technology has led to the formation of new military forces around the globe, like the U.S. Cyber Command, or the Chinese Information Security Base, new military units whose very role is to fight and win wars in cyberspace. And, different from back then, they're also being joined by a host of non state actors. It's an exciting time, it's a fundamentally important time, which is why a new focus on the questions of cyber security and how they connect to our other interest areas of defense policy, of arms control via intelligence community is what led us to form the Center here at Brookings, the Center for 21st Century Security Intelligence. We hope to explore how these issues cross with each other, but also learn lessons from the connections between these fields.

Now, as part of the launch for this new Center, we've been conducted our own research on these questions, but also hosting an inaugural series of discussions with some of the top leaders in the field, and thus, it could not be more appropriate than to host our speaker today for this discussion on the challenges of defending the nation in a time when both the threats and the opportunities move at network speed.

General Martin Dempsey is a 1974 graduate of the U.S. Military Academy, he also holds Master's degrees from West Point and Duke, his career in the nation's service has taken him around the world during both war and peacetime, from places that ranged from Germany to Iraq, from platoon leader to Chief of Staff of the Army. In 2011, he became the 18th Chairman of the Joint Chiefs of Staff, where he currently serves as the nation's highest ranking military officer, and principal military adviser to the President and Secretary of Defense and the National Security Council.

General, we're especially honored and delighted for you to join us today.

MR. DEMPSEY: Thank you. (Applause) Thank you, Peter, it is, I'm very pleased to be here, the attendance, I think, is indicative of the importance of the topic that we'll have the chance to discuss today. Since we're comparing first impressions, I'll tell you that my first impression of communications was a black rotary dial phone in Bayonne, New Jersey, on 3rd street, I can remember my first phone number, Federal 96712. And, actually, my sister still has it, she was down at Woodbridge, and it looks now like something out of a museum, doesn't it?

When I asked my staff about the fellows, and I've been here before, and I'm delighted to be invited back, but when I asked about the fellows here, it reminded me that you have experts on many things; drones, private security contractors, one of the people who discovered Stuxnet, the editor of the most controversial national security blog, and our former commander in Afghanistan, of course, General, retired, John Allen. I felt as though, listening to that particular universe of thought that I probably should wear body armor as I came here in preparation for the question and answer period.

I will say, before we get too far along, Peter, that I know, inevitably, I'm sure you'll ask me something about drones. I'll just ask you to remember that you write about them, but I actually have them. (Laughter) Seriously.

MR. SINGER: (off mic)

MR. DEMPSEY: yeah, we won't go there. Seriously, me and my team that accompanied me here today are delighted to have a chance to engage with those scholars who are taking time to look to our future. Especially as the defense community begins to focus inward on the implications of changing resources and this thing called sequestration. It's important that we force ourselves to continue to look outward at the changing world around us.

One person who always looked outward was a man by the name of Douglas Englebart, after serving as a radar technician in World War II, Englebart became an engineer at Stanford. Those days were heady times in computer science, 46 years ago this week, he submitted a patent application, and the patent application was titled, The XY Position Indicator ForA Display System. He later nicknamed it a mouse. Englebart's research was funded by DARPA's predecessor, his lab at Stanford was one of the original nodes of the internet. And the mouse he invented with taxpayer funds was later licensed to Apple for a meager $40,000.

The revolution in computer technology that Englebart helped has transformed our world; more than a billion mice are in used today, 3 billion people have access to the web. By this time next year, Peter mentioned all the different ways that we find computer technology around us. By this time next year, I'm quite certain that my toaster will be connected to the internet and probably Tweeting. I can actually anticipate the hashtag even now; burned toast at quarter six. But the spread of digital technology has not been without consequence, it has also introduced new dangers to our security and our safety.

Since becoming Chairman two years ago, nearly, I have been focused on what this revolution means for our military. I visited Silicon Valley, sat with security teams of major tech companies, and spent time with an internet service provider, I sought out tech experts and even met with a venture capitalist. One thing is clear; cyber has escalated from an issue of moderate concern to one of the most serious threats to our national security. We now live in a world of weaponized bits and bytes wherein an entire country can be disrupted by a click of Englebart's mouse.

There are new missions we must take on as a military, and steps we must take as a nation to defend ourselves from this threat, so let me talk briefly about the cyber threat. Cyber incidents have steadily increased over the past year, U.S. banks have been hit with sophisticated denial of service attacks. Last August, in the first largescale destructive cyber attack, the Shamoon virus wiped clean the hard drives of 30,000 computers at the Saudi Arabian State Oil Company, Saudi Aramco. Over 20 nations now have military units dedicated to employing cyber in war, and toxic malware continues to proliferate among militaries, but also among hackers, alike.

This is the new normal in cyber space. Disruptive and destructive cyber attacks are becoming a part of conflict between states, within states, and among non state actors. Even if a state adversary doesn't engage in cyber conflict, global hacktivists might, and they do so on its behalf. The borderless nature of cyber space means anyone, anywhere in the world can use cyber to affect someone else. Strengthening our cyber defenses on military systems is critically important, but it's not enough in order to defend the nation.

In cyber conflict, civilian infrastructure and businesses are often targeted first. Since I became Chairman, intrusions into our critical infrastructure have increased 17 fold. The computer controlled systems that operate our chemical, electrical, water and transport sectors have all been probed, several intruders have successfully gained system access. The gap between cyber defenses employed across critical infrastructure and offensive tools we now know exist presents a significant vulnerability for our nation. Secretary of Defense, Chuck Hagel, has called cyber an insidious and dangerous threat, and many of you remember that former Secretary of Defense, Leon Panetta, noted that we're at a pre 9/11 moment in which attackers are plotting, but our nation remains inadequately prepared.

Today, I add my voice, again, to the chorus of concern, so let me talk about defending against that threat. In response to the threat, the Department is growing our capacity to protect our networks, but we're also taking on a new mission when asked, and with interagency partners that is defending the nation from cyber attacks. To do this, we're integrating the cyber mission across the force, and we're adding personnel to the United States Cyber Command, over the next four years, 4,000 cyber operators will join the ranks, we're also investing $23 billion in cyber security.

And we're doing all this not to address run of the million cyber intrusions, but to stop potential attacks of significant consequence, those that could threaten life, limb, and the country's core critical infrastructure. At Cyber Command, three kinds of teams will operate around the clock, national mission teams will counter adversary cyber attacks on our country. A second and larger set of teams will support our combatant commanders as they execute our military missions around the globe. And the largest set of teams will operate and defend the networks that support our military operations worldwide.

These three teams constitute the cyber force that will defend our networks, defend military forces, and be prepared, if asked, to defend the nation. Our most immediate priority is keeping the .mil domain secure, but in the event of a domestic cyber crisis, our cyber forces will work in support of the Department of Homeland Security and the FBI, who lead our nation's response in the .gov and the .com domains. To ensure this force is able to operate at network speed rather than what is often called swivel chair speed, we now have a play book for cyber. The President signed a directive that codifies how each part of the government will respond in the event of a series cyber attack.

Under this directive, the Department of Defense has developed emergency procedures to guide our response to imminent significant cyber threats. We're updating our rules of engagement, the first update for cyber in 7 years, by the way, and we're improving command and control of our cyber forces. We have more work to do, but these important steps significantly strengthen our ability to defend the nation at network speed.

So let me talk a bit about cyber as that was the threat of cyber and our response, let me talk for a moment, though, as well, about cyber as an asymmetric advantage. While cyber may be our nation's greatest vulnerability, it also presents our military with a tremendous asymmetric advantage; the military that maintains the most agile and resilient networks will be the most effective in future war. This is the kind of force we're building for the future, a force that I've described as Joint Force 2020. Each Service is doing its part: Cyber is strengthening the Air Force's ability to achieve global reach; the Army is preparing to fight on a battlefield that is as much defined by cyber space as it is enabled by it; the Navy is putting its entire work force through a cyber emergent program; and the Marine Corps is smartly integrating cyber across the Corps.

Collectively, the Services are making the investments necessary to ensure that the joint force can operate in cyber space as it operates in the land, sea, air and space domains. This includes recruiting the right people for our cyber work force, establishing common standards across the joint force, and achieving a higher degree of coordination in how we invest and how we manage our critical cyber resources.

The next step is making our networks joint. Today, the Department of Defense operates 15,000 networks. We're consolidating this sprawling mass of IT into a common set of enterprise services, all based in the Cloud. New joint information environment, as we call it, will deepen collaboration across the services and missionaries, it will also be more secure, helping ensure that the integrity of our battle systems prevail in the face of disruption. As part of this new joint information environment, we're building a secure 4G wireless network that will get iPads, iPhones and Android devices online in 2014.

In fact, I have here today with me a secure mobile phone and data processor that allows me to operate in the SIPR environment, both phone and data, no matter where I am. Now, it's not where it needs to be yet, but it's an incredible first step, and has the potential to revolutionize command and control. This phone, by the way, I think, would make even Batman and/or James Bond a bit jealous, and I did have to keep an eye on Peter as you stood up here glancing at it enviously. (Laughter)

With tools like this, the Smartphone generation joining our military will help us pioneer a new era of mobile command and control. This revolution will empower our greatest resource, that is, the ingenuity of our people, and the philosophy of mission command that we all embrace. To help unleash the potential for user-driven innovation, a federated app store will allow any DoD user to write and share phone and tablet applications. By using off-the-shelf technology, we're bringing the full force of the technology revolution into the classified environment.

So what's an important next step? Let me talk about cyber legislation and diplomacy. Although we've made significant progress embracing cyber within the military, our nation's effort to protect our critical civilian infrastructure is lagging, too few companies have invested adequately in cyber security. I worry that adversaries will seek to exploit that chink in our nation's armor, to them, our economy and our infrastructure are the softer targets than our military. One of the most important ways we can strengthen cyber security across the private sector is simply by sharing information.

Right now, threat information runs primarily in one direction; from the government into the operators of critical infrastructure. Very little information flows back to the government. That has to change, we can't stop an attack unless we can see it. I'm confident that indicators of a pending attack could be shared in a way that preserves the privacy, the anonymity and the civil liberties of network users. I understand that the country is debating the proper person, purpose, limits of intelligence collection for national security, but let me be clear that these are two entirely different issues.

One is collecting the intelligence necessary to locate foreign terrorists and their potential domestic coconspirators; the other is sharing information about malware to protect our critical infrastructure from a different kind of attack. We can't allow these separate debates to become conflated. The reality is that, every day, adversaries are injecting malware into our networks, the worse of this malware is equivalent to cyber bullets and bombs. We must share what it looks like so that we can stop it before it detonates. Ultimately, it will take legislation to significantly strengthen our ability to withstand cyber attacks while safeguarding civil liberties.

Information sharing is just one way to be safer, improving cyber standards is another. Still a third is to work with other nations to set norms of responsible behavior in cyber space. One of our most important dialogues on that topic on cyber is with China. During my visit there last month, I reinforced the need for us to address cyber in the working group that Secretary Kerry proposed. We're poised to begin that process, and hopefully to make some progress in meetings that begin next month. Avoiding miscalculation in cyber space is another important goal. Our agreement to open a cyber security link with Russia is a step in the right direction, a step that we should eventually take with others.

In conclusion, as you see, we have our work cut out for us as a military, as a government, and as a nation, and as an international community. The rise of cyber is the most striking development in the post 9/11 security environment. Not only are military systems being targeted by tools that can cause physical destruction, but adversaries can increasingly hold our nation's critical infrastructure at risk. As a result, our military must be ready to defend the nation, and to do so at network speed. We're doing everything we can inside the military to be ready to operate in cyber space. I call on our elected officials and the private sector to match that urgency. Together, we must place this nation on sure footing against a cyber threat.

I thank you for giving me the opportunity to address you today, and I look forward to your questions. (Applause)

MR. SINGER: So many different areas to discuss, we won't touch on drones, we'll just focus on cyber. You described very well the immense growth of both threats, but also, in turn, our organizational response to them, and personnel, and budget, new organizations. One fundamental question I wanted to pose is, given the amount of changes going on, is this a realm where scale matters, and how do we determine that?

Another way of putting it is, if we increase our budget by 300 percent, do we get 300 percent more of the capability, or do we get 3,000 percent more the capability, or actually do we just get 30 percent more the capability? This, of course, a fundamental question in these war austere budget times. How do we look at this question of scale?

MR. DEMPSEY: Yes, good question. Can you all hear me?

MR. SINGER: Oh, I will ask it again, and we'll try these ones. You've got one right behind you.

MR. DEMPSEY: I do. Redundant communications. The original one is on now.

MR. SINGER: Did you all hear the question?

MR. DEMPSEY: Did you hear the answer, it was really good. (Laughter) That's a great question. So, and we haven't had to confront it to this point, because, from where we started, there was no doubt we needed to do much more. But let me give you, if I could, an analogy that might be helpful to you in understanding our approach, the military's approach to cyber. Post 9/11, we realized that our nation's air space was vulnerable to terrorist attack, and so we have this process called Operation Noble Eagle that I think many people are familiar with, and it's whole government, we have a play book, and we have forces allocated to the mission.

And it's a public/private partnership, and here's how it works; the airlines harden the cockpit doors, the Transportation, the TSA manages the flow of passengers on to the aircraft, as well as putting air marshals in place on selected aircraft. The FAA tracks the aircraft through its flight, and if it deems that there's a problem, they contact us, and we go into a national threat conference very quickly, and essentially, we pass authorities from agency to agency to agency, and if it became necessary to interdict the aircraft, that's where we come in in defending the nation.

When we started that process, to your point about resources, we over resourced it initially, we had F16 squadrons on alert all over the country in a way that was fundamentally unsustainable. And now we're able to, with the experience of 10 years behind us, we're able to manage the level of resources consistent with the threat in a way that's sustainable. And I suggest to you that that's where we will eventually find ourselves in cyber, where we have a whole of government approach, a play book to define the roles and responsibilities we have that, by the way and then the resources will ebb and flow based on the way we see the threat evolving.

MR. SINGER: As a follow up to that, how do go about force sizing in the here and now? So, as an example, why 13 cyber com teams to defend the nation, why not 12, why not 14, why not 50? How do we go about thinking about that, especially given your role also to steward the broader budget where the more we do, then it means we probably have to give up something else in terms of an actual physical, be it a ship, a plane, personnel moving, not working on that. How do you think about force sizing?

MR. DEMPSEY: Not unlike we think about it in the traditional domains of air, land and sea. Meaning we have a pretty clear picture of the threat, and the threat is, in some cases, nation states, and some cases non state actors, and some cases just this issue of broader hacktivists across the globe. And based on the threat that we understand today, we have sized these response teams, those at the national level, those at the regional level against that particular threat. As the threat evolves, then we'll evolve, but I think that where we are today is where we need to be, based on the threat we know today, but this will take constant review and revision as time goes on.

MR. SINGER: I wanted to shift the conversation to organization. I know you've spoken on Capitol Hill about the question of the next evolution of cyber command, you were asked there about should it be unifying command, combatant command.

MR. DEMPSEY: Right.

MR. SINGER: Recently, Deputy Secretary, Ash Carter, talked about how we could visualize it one day becoming its own service. But the way that it's been talked about by senior officials is, we're not there yet, was some of the phrasings, or we need to focus on the threat now, was, for example, how Secretary Carter talked about it. The issue that comes out of that is, as you noted, the threat's not going away, it's only going to continue to grow.

So rather than putting you on the spot by asking you whether you think we should or should not have this shift, the question is more what would be the kind of indicators that would get us to that point of thinking about it? That is, what would, what changes for us to have that kind of discussion?

MR. DEMPSEY: I think we're there now, and we're having that conversation. As you know, at this point, Cyber Com is a sub unified command that resides under STRATCOM, Strategic Command, but the commander of Cyber Com is dual hatted as the Director of the National Security Agency. I'm actually content the way we're organized right now. You asked me what would change, I think it would be if I perceived that, for some reason, the span of control of Strategic Command became unmanageable, if cyber became such a dominant factor in military operations that it warranted elevating it to a unified command, which, by the way, I anticipate that will happen at some point.

But, at this point, STRATCOM, with its global reach responsibilities, as well as its space responsibilities, is also able to manage the workload that comes with being the next senior headquarters to Cyber Com. Unless I saw that change, I would probably be content to keep it the way we have it, but I think that will happen at some point.

MR. SINGER: Is it something that, you talked about the difference between network speed and swivel chair speed.

MR. DEMPSEY: Yeah.

MR. SINGER: Could that change take place at that amount of speed, and compare that to the organizational change speed.

MR. DEMPSEY: Yeah, that's a great point. I do think that, if we get the kind of information sharing that we need, and, as you know, the legislation this year is focused exclusively on information sharing, which I think is actually the proper path. If we get the kind of information sharing we need, that could be a catalyst for change in the organization, because the span and scope of responsibility would change.

MR. SINGER: One last question, and maybe it's a large theoretic question, it's a question in the field of everything from law, but also it's a fundamental question for your own role. As we talked about the terms in this space are both new, but they're very fuzzy, so, to you, when would a cyber war start, and how would you know?

MR. DEMPSEY: You know, I just finished reading World War Z, so I'm kind of attuned to figuring out when something becomes, reaches that level. I actually did just finish reading World War Z, by the way.

MR. SINGER: Somewhere, Brat Pitt is sad that you didn't see the movie.

MR. DEMPSEY: I haven't seen the movie yet. If there's a book, I'd go to the book and then I, with a certain amount of hubris, would go to the movie and criticize it. (Laughter) You know, that is a conversation that we have had, but only fleetingly. That is to say, what changes from cyber theft, when does cyber theft become a hostile act, or when does cyber theft added to distributed denial of services become a hostile act, or is a hostile act simply defined as something that literally is destructive in nature?

And, frankly, that's not a conversation that will be driven by me, I think that the decision to declare something a hostile act and an act of war is certainly one that resides in the responsibility of our elected leaders, with my advice. But to your point about a cyber war, I do think that there are capabilities out there that are so destructive in nature and potential that they would, it would be very difficult not to see them as acts of war. We haven't experienced one, but I know the capability is out there.

MR. SINGER: So, for you, in many ways, it's another way of saying the impact?

MR. DEMPSEY: I think so. Which is not unlike how we would describe war in the other domains. The one thing I do want to point out is that cyber is not a mystery domain, although sometimes it can feel abstract. I mean, it is a physical domain in the sense that it's, it is operated by men and women over routers and servers, and so there is a physical nature to it. As you know, it's difficult to track because it can move at network speed and servers can be taken and used for destructive purposes or for intrusion, even unwitting to the people who own them, so it is difficult to track in that regard.

But it's not abstract, and I think, to the extent that we can always think about it in the sense of the way we've always organized our thinking about the other domains, it might illuminate the challenge a little better.

MR. SINGER: Great. Let's open it up to the audience, here. If you could raise your hand and wait for the mic to come to you, and stand and identify yourself, and finally, all questions end with a question mark. So, right here in the front.

MR. DEMPSEY: I thought I was the English Professor.

MR. WALLACE: Hi. Ian WALLACE from Brookings 21CSI, Cyber Security. Thank you very much for your comments. To look at the international context, and for reasons that you've explained, it is very clear that DoD has a real incentive to build military cyber capability, both offensive and defensive, as the force operates around the world, and to encourage allies to do the same.

But, at the same time, you leave yourself open to the accusation that your militarizing cyber space, which makes life difficult for U.S. companies and other companies. I wonder if you could talk to how DoD is managing that apparent presentational challenge.

MR. DEMPSEY: Yeah. Well, you know, if I were sending a Twitter message back to you, I'd say we have a Navy, but we're not being accused of militarizing the ocean. And that's why I say that, I think the more that we can think about cyber, demystify cyber and think about it in terms that have stood the test of time. We have a Navy to protect the global commons and share the free movement of goods and services in the maritime domain, and that's what we aspire to in cyber and well, by the way.

Now, to your point about the international aspect to this, I have periodic strategic dialogues with, especially our closest allies. So, just yesterday, we had a conversation with our Canadian counterparts over at National Defense University for about three quarters of a day. And one of the topics was cyber, and there was some question about why we should have a common view of the threat in cyber and potentially share some common movement forward.

And it goes back to what I said to Peter about what could happen in cyber inside the United States. You're all familiar with the term botnets. Inside the United States, we could have one sector of our society, the financial sector, an external actor with malware could gain control of it and attack another sector of the United States economy. We could have our own financial system attacking critical infrastructure. That's not outrageous to suggest that that same thing could happen across borders. In fact, it's probably likely that that's the way an attack would evolve, so that it would be deniable and difficult to trace.

So we have to have, and we're not there, and, by the way, we weren't pushing on each other, we were having a very professional conversation about the evolving threat and how it is worthy of further discussion to kind of steel plate ourselves against this threat in the future.

MR. SINGER: Great. Let's get right in the back, there.

MR. ANGEVINE: How are you doing, sir? I'm John Angevine, Colonel, U.S. Army, retired.

MR. DEMPSEY: Then my advice is be kind.

MR. ANGEVINE: Yes, sir, absolutely. Over the past 12 years, the Joint Forces enjoyed high fidelity situational awareness like in Iraq and Afghanistan, and as the U.S. government and the military makes the strategic shift to the African/Indo Asia/Pacific region, we'll be challenged to preserve that high fidelity situational awareness, particularly as we have less boots on the ground and broader geographic regions to take a look at.

Considering that vast regions in the ISR maybe diffused a bit, what are your thoughts on how cyber capabilities can enhance disaggregated operations using a mission command philosophy that you mentioned earlier? Thank you.

MR. DEMPSEY: Well, and I do first of all, to your point about the stress on resources. I mean, clearly, the pressure under which our resources, the pressure on our resources will increase. And, as you well know, we're trying to figure out how to absorb the reductions under the Budget Control Act about $487 billion over 10, and sequester adds another 500 or so on top of that. But, you know, strategy is always the art of balance and science, by the way, balancing ends, ways and means.

I also think of strategy in terms of context and choice. So context in terms of the conversation we're having here today, cyber is, if I haven't convinced you of anything, I hope I've convinced you that cyber is becoming a more important national security issue than it has ever been, and that will likely increase over time. Therefore, that's the context. Our choice must account for that context. So, as we go forward and balancing how we employ the resources of the Department, I suspect, and you would suspect that we will have to reduce our reliance upon what we might describe as traditional and conventional means and advantage cyber in these budget discussions.

I think we can do it, frankly, I think we can figure this out. We'd certainly like a little time and certainty in order to do it, but we don't have any choice, we have to figure that out.

MR. SINGER: Okay, up here.

MR. CLARK: Colin Clark, Breaking Defense. Good morning, sir. You mentioned that elected leaders are going to have to make the distinction about what constitutes an act of war. Are you talking about Congress having to actually issue a declaration of war, or are you talking about revamping the distinctions between Title 10 and Title 50, or all three?

MR. DEMPSEY: Well, I didn't, I'm not making any assertions about Title 10 and Title 50. What I am suggesting is that it is our elected leaders, and notably the Congress of the United States, that generally decides whether the nation is under a condition of war, it's called the War Powers Act. And here's why that's important; there is an assumption out there, I think, and I would like to disabuse you of it, that a cyber attack that had destructive effects would be met by a cyber response with destructive attacks. That's not necessarily the case.

I mean, again, this is why I'm so adamant that we think of cyber as a domain not unique to all others, it has many common features of other domains, that is land, sea, air and space. And I think that what the President of the United States would insist upon, actually, is that he had the options and the freedom of movement to decide what kind of response we would employ. And that's why I say I don't want to have necessarily a narrow conversation about what constitutes war and cyber, because the response could actually be in one of the traditional, one of the other traditional domains.

MR. SINGER: To toss a little bit of history into that, Colin, the last time the U.S. Congress actually formally declared war was in spring of 1942 against Bulgaria, one of the Axis powers that we forgot to include in the Pearl Harbor Declaration.

MR. DEMPSEY: That's why I hate sitting with historians.

MR. SINGER: Fun little factoids like that. Let's get, right here in the front.

MR. JAO: Hi. I'm Jimmy Jao from St. Alban's School of Public Service. From my understanding, current encryption techniques in cyber security infrastructure have advanced to the point where brute force techniques from outside the system have been rendered ineffective, and thus, many attacks actually rely on human error from within the system. And so, how does the government, how do they plan on addressing this threat from within a system?

MR. DEMPSEY: Well, I wouldn't say that it's as stark as, I wouldn't say encryption has made the blunt brute force and ignorance approach completely, we're not completely vulnerable to that. We may be in the .mil domain, we're certainly not that way in some of our .com and .gov and other critical infrastructure domains. But you speak of our approach to, let's call it cyber hygiene, and that's always a big part of this, it's training and it's education, which is not as difficult for your generation as it comes into the military as it is for mine. There's not many of me left, by the way, I'm at the other end of the chronological demographic.

But, you know, it's kind of our mid grade folks who are having the most challenge understanding the importance of cyber hygiene, but there's other things we can do, too, that I do want to highlight. You heard me speak of a joint information enterprise, the fact that we have 5,000 networks we're trying to manage. We really need to get to take advantage of thin client and Cloud technology dramatically reduced the number of systems administrators that we have managing our program, which will make it both more effective, more efficient and safer.

So I don't know if that answered your question, but that's the answer I wanted to give you, so I hope you like it.

MR. SINGER: I'm going to do a follow up to that, because it's my responsibility on the moderator here to tie it to some events.

MR. DEMPSEY: Okay.

MR. SINGER: There's, you absolutely correctly, I mean, I applaud the notion of cyber hygiene, I think it's the right framing for this, contrary to the kind of cold war framing that we often use.

MR. DEMPSEY: Yeah.

MR. SINGER: But the notion of the challenge from the inside is not, some of the incidents have been from bad cyber hygiene, someone picking up a memory stick in a parking lot and putting it in. But some of the larger incidents

MR. DEMPSEY: True.

MR. SINGER: have been insiders deliberately sharing, and you talked about whether it's Manning, whether it's the recent case with Snowden, does this move to the cloud on one hand, as you lay out, maybe by having less people who are systems administrators, you reduce that threat of that kind of individual. On the other hand, how do you avoid the over provision of access as you move, as you allow more and more people, as you bundle things together?

MR. DEMPSEY: Yeah. Well, you touch on, of course, the issue du jour in terms of, it's not only what happened, how could it happen. And, of course, we're taking a very close look at that, as you would expect the National Security Agency to take a closer look. There are things we can do to reduce our vulnerability, but I think it's important, you described it as an insider attack, it is akin, almost, to how do you prevent insider attacks in Afghanistan?

Well, the answer is, you can't prevent, you can mitigate the risk. And what I would like you to take away from the conversation about this incident with Snowden, you can't stop someone from breaking the law 100 percent of the time, you just can't stop that from happening. You can certainly increase the scrutiny in terms of their background investigations, you can reduce the number of them, you can put different degrees of oversight in place, but at some point, if somebody is going to break the law and commit an act of treason, I don't know what he'll individually be charged with, or espionage, there are going to be people that do that.

The key for us, of course, I think systems administrators is the right place to begin to clean this up, though, because they have such ubiquitous access, and that's how he ended up doing what he did. But, yeah, we've got to take a much harder look at this, as we become more reliant upon cyber activities.

MR. SINGER: Great. Let's give an opportunity in the back, there.

MR. FISHEL: Hi, sir. Justin Fishel with Fox News. You mentioned updating the rules of engagement for cyber. What are the rules of engagement right now, and how are you going to update them, and is there anyone actually obeying them? For example, do you know if the Chinese have their own rules of engagement?

And then, just briefly, on Syria, there's a report today in the Wall Street Journal that weapons are now on the move from secret warehouses in Jordan. Do you have any comment on weapons to Syria? Thanks.

MR. DEMPSEY: On the issue of rules of engagement, we do have this play book I described, is a play book that describes roles and responsibilities, whether it's Homeland Security, FBI, Department of Defense, and how those rules and responsibilities are shared, and the authorities are shared. And, by the way, the authorities are shared, and this actually makes us stronger because we have multiple lines of oversight, whether they be executive oversight, judicial or legislative oversight, because we're sharing authorities.

The standing rules of engagement are currently in draft, they have not yet been approached, we've run several excursions and exercises. But, fundamentally, I'll just give you a vignette, if you'd like, if part of our critical infrastructure were under attack from a botnet, let's say, located external to the United States, our first line of defense would be, first of all, to know about it. And we would either know about it because we saw it coming, or because we had this information sharing agreement when we could be told that a particular part of the critical infrastructure was under attack.

Our first instinct would be to pull up the drawbridge and prevent the attack, that is to say either block or defend. If that was unsuccessful, then the play book might call for us to, in the act of active defense, if you will, proportionally, to go out and disabilities the botnet, the particular botnet that was attacking us, active defense. And then, if it became something more widespread and we needed to do something beyond that, it would require interagency consultation and authorities at a higher level in order to do it.

But the thing you need to take away, I'm not going to tell you more than that, because these are classified standing rules of engagement, and they're also pre decisional, but that's what we need. We need this play book of rules and responsibilities, and we have it; we need this standing rules of engagement, and we are close; and then we need the ability to understand what's going on, which will be greatly enabled by this information sharing process. And, no, I won't comment on Syria. You thought I forgot, didn't you?

MR. SINGER: Right here in the front.

QUESTIONER: Thank you, General, for doing this. (Inaudible) Phoenix TV. Two quick questions; first, is it true the U.S. hacked into computers in China? Secondly, the Chinese Foreign Ministry already asked the U.S. to give an explanation on the Edward Snowden's allegation. Do you think the leaks actually deprived the U.S.'s moral high ground when you are blaming China for its attack on the U.S.? Thank you.

MR. DEMPSEY: The activities that nations conduct in the intelligence arena have some pretty clear standards. I mean, for example, to move away from cyber, we run strategic reconnaissance flights outside of Chinese territorial waters, for example, in order to gain some insights to your intention not yours, but to Chinese intentions as they develop their military. And all countries on the face of the planet conduct intelligence activities. China's particular niche in cyber has been theft and intellectual property, and I've had some conversations about that with them, and the conversations generally, you know, we tend to agree to disagree.

Their view is that there are no rules of the road in cyber, there's nothing, there's no laws that they're breaking, there's no standards of behavior, and so we have asked them to meet with us, and the first meeting will be next week, in order to establish some rules of the road so that we don't have these friction points in our relationship. But intelligence activities are a separate matter, and I won't comment on them except to say all nations on the face of the planet always conduct intelligence operations in all domains, and we're no different, they're no different.

It's not, that's not what we're talking about, we're talking about other activities in cyber that I think bear additional scrutiny.

MR. SINGER: General, you're on Twitter, I'm on Twitter, I'm betting many of the people in this room are on Twitter, and so, very appropriate to the topic, what I'd like to do in the next five minutes is take questions, actually, from the world of Twitter.

MR. DEMPSEY: This is the lightning round.

MR. SINGER: This is the lightning round. And so, please give your answers, they don't necessarily have to be 140 characters, but feel free to blast through them very quickly.

MR. DEMPSEY: All right.

MR. SINGER: One question is, and this is from Casey Erdham. How will DoD management key software and security updates, like issues with the F35 UAS and slow acquisitions process? Another way of putting it is, this all moves at network speed, but we buy at glacial speed. How do we deal with that?

MR. DEMPSEY: No, fair program, fair question, great question. As I said, we've got to go to thin client Cloud, joint information enterprise, and we've got to get your defense industrial base into it, and we've got to put some teeth into what we call clear defense contracts.

MR. SINGER: Great. This is from V. Eric McCann. What can private sector do to help the government with learning more about and defending against cyber attacks?

MR. DEMPSEY: Information sharing. Right now, information sharing is actually disincentivized, and we need to incentivize it.

MR. SINGER: Let me ask a follow up to this, a link to a prior topic you mentioned. Private security, we've got it maybe growing equivalent in the cyber realm and the hack back companies that are, right now, I was talking with someone, if you want a couple million dollars in venture capital, say you're exploring offensive cyber, what is your view of this growing potential industry of companies that do hack back?

MR. DEMPSEY: I'm very concerned about that. In fact, I have raised it as all the more reason for us to come together as a whole of government, because we don't want private cyber organizations conducting operations that could be perceived as hostile acts. And if they're perceived as hostile acts, it could lead us into conflict.

MR. SINGER: All right. This is from DRC Mackey. What would the U.S. military's role be if there was a Saudi Aramco like attack on a U.S. company?

MR. DEMPSEY: Well, as I said, we've got a play book that would allow us to share the authorities that are extent in department of Homeland Security, notably FBI, and we would come together, and at the point where it exceeded their capabilities, then we would be asked to block or potentially, if blocking was ineffective, potentially some active defense measure.

MR. SINGER: This is from Jazz42. Where does the authority for cyber fires need to exist, can tactical commands employ or only request strategic, what is tactical cyber?

MR. DEMPSEY: Well, tactical cyber is exclusively intelligence gathering and defensive in nature. There is no decentralized cyber attack authority. To the point, where should cyber fires authority reside? Like the operation Noble Eagle analogy I gave you, those should reside at the highest levels of government.

MR. SINGER: Finally, this is from Jazz Easterly. Why is cyber often analogized to nukes? Discreet, nuanced, nonlethal effects available with precision, why constrain it by bad paradigms?

MR. DEMPSEY: Well, by the way, there are some imprecise and potentially unhelpful paradigms, but I think it's back to the point I made early on, which is, we have to demystify cyber, make it less abstract, make it more understandable. But, make no mistake about it, if the electrical grid on the eastern seaboard were I mean, look, my wife gets mad if she loses network coverage for 15 minutes. I mean, really, we're and, by the way, this is traveling around the world. So, and it's not just an inconvenience, if we lost critical infrastructure on the east coast for a period of time, people's lives would be lost.

And that's indiscriminate, and that's why I think sometimes the nuclear analogy comes into play. Not in terms of its scale, but maybe in terms of its indiscriminate effect.

MR. SINGER: It's a great point to end on, if you'll allow me to ask one final question, which is; as you've talked about, there's a huge need to demystify, and in many ways, the role that you and other senior government leaders are playing is part of this, trying to demystify it to the public, but particularly also warn the public of the challenges that are out there, and call for the need to undertake various actions. But how do you balance that with the risk of unintentionally aiding the impact?

There is, in deterrence theory, there's deterrence by denial, that I'm less likely to attack you if the attack's not going to work. In the computer security world, there's the magic word of resilience, the idea, not only to fail gracefully, but also to bounce back quickly. And yet, you used this example of the ultimate nightmare scenario of the power grid going down, I will bet my month's salary that the power grid will go down in Maryland this summer. But if I add cyber to it, we'll have the comparison to 9/11, and that, I'll bet we'll see a lot of responses in Congress.

And so, another way of putting it is, how do we balance between warning of the threat, but also filling the old British poster of keep calm and carry on?

MR. DEMPSEY: Right. Well, based on where I think we were in the keep calm and carry on for about the last, I don't know, five years or so. And we were carrying on, but we were late to need and inadequate to the task. So, if you sense a renewed emphasis and effort, it's because, as I said, since I became the Chairman not even two years ago, the number of intrusions into our critical infrastructure have increased 17 fold. So keep calm and carry on, I think, is not appropriate to the threat.

And I think we have to, even at risk of, in some ways, by demystifying it, maybe reducing its deterrent value, I think we have to have that conversation with America about the potential impacts.

MR. SINGER: Well, General, thank you very much. This has been an incredibly rich discussion, this has certainly been, by far, the best discussion I've been involved in with a leader on cyber security, so very much appreciated, and I can see people in the audience nodding their head. So please join me in a round of applause. (Applause)

MR. DEMPSEY: Thank you.

MR. SINGER: If I can ask you to stay in your seats so he can actually get to moving at non network speed, which is getting into D.C. traffic.

* * * * *

CERTIFICATE OF NOTARY PUBLIC

I, Carleton J. Anderson, III do hereby certify that the forgoing electronic file when originally transmitted was reduced to text at my direction; that said transcript is a true record of the proceedings therein referenced; that I am neither counsel for, related to, nor employed by any of the parties to the action in which these proceedings were taken; and, furthermore, that I am neither a relative or employee of any attorney or counsel employed by the parties hereto, nor financially or otherwise interested in the outcome of this action.

Carleton J. Anderson, III

(Signature and Seal on File)

Notary Public in and for the Commonwealth of Virginia

Commission No. 351998

Expires: November 30, 2016