THE BROOKINGS INSTITUTION

DEFENSE CHALLENGES AND FUTURE OPPORTUNITIES

THE 21ST CENTURY DEFENSE INITIATIVE'S SECOND ANNUAL MILITARY AND FEDERAL FELLOW RESEARCH SYMPOSIUM

Washington, D.C.
Wednesday, March 16, 2011

PANEL 2: DEPARTMENT OF DEFENSE EFFORTS TO HARNESS CYBERSPACE

PARTICIPANTS:

Moderator:

ALLAN FRIEDMAN
Fellow and Research Director, Center for Technology Innovation
The Brookings Institution

Panelists:

LIEUTENANT COLONEL JERRY CARTER (USMC)
National Security Fellow, Harvard University
"Can the Department of Defense Achieve Cyberspace Superiority"

COLONEL DAVID HATHAWAY (USAF)
Federal Executive Fellow, The Brookings Institution
"The Digital Kasserine Pass: Command and Control of DOD Cyberforces"

BRUCE MacKAY
Defense Intelligence Agency Chair
U.S. Marine Corps University

P R O C E E D I N G S

MR. FRIEDMAN: So the advantage of getting the panel before lunch started on time is one can then proceed to lunch, especially given our distinguished guest of General Robinson. But first, it is my pleasure to introduce this panel.

One of the more interesting things about technology policy is to understand how concepts that we're all familiar with and use on a regular basis have to shift and adapt as the technology changes. And, of course one of the most important areas where we're facing this challenge now is in the area of cybersecurity and information technology.

And we have a great panel today, with two excellent papers that approach really challenging problems of how we're going to take the models that we currently use and adapt them to the cybersecurity domain. And we have an excellent respondent with Dr. MacKay here.

So what we'll do is I'll just introduce the panel, and then we'll have the two papers, and Dr. MacKay will respond, and then we'll open it up to some questions.

So, first speaker, and I've been privileged to get to know here in his time as a federal executive fellow at Brookings is Colonel David Hathaway. Colonel Hathaway has served in the U.S. Air Force for 23 years. He as commissioned as a distinguished graduate in the Air Force Reserve Officer Training Corps. He's commanded F-16 fighter squadron, and most recently served as the vice wing commander of an F-16 wing. A graduate and former instructor of the Air Force Weapons School, and is a graduate of the School of Advanced Air and Space Power Studies. He was also the architect of space and air power strategy for the operations Enduring Freedom and Iraqi Freedom as the chief strategy for U.S. CENTA. Sorry for the abbreviation butchering there.

Colonel Hathaway has a bachelor of science from Wisconsin, and his master in aviation science from Embry Riddle, and a master of military operational art and science, and a master of air power art and science from the Air University.

The second speaker -- who I also have the privilege to know -- is a national

security fellow at the Harvard Kennedy School. Lieutenant Colonel Jerry Carter is a Marine Air-Ground Task Force intelligence officer, who recently served as the commanding officer in the Second Radio Battalion, Second Marine Expeditionary Force at Camp Lejeune. In 2008 he deployed to Iraq during Operation Iraqi Freedom as the task force radio battalion commander in support of the Multinational Force West.

Lieutenant Colonel Carter has a bachelor of arts in banking and finance from Morehouse, and is a graduate of both the U.S. Marine Corps' Command and Control systems course, and the Joint Forces Staff College.

As our respondent, we have Bruce MacKay, who is the Defense Intelligence Agency chair for the Marine Corps University. He retired from the U.S. Army as a career intelligence collector, with operational assignments in Europe and Asia, and has served since 1998 in the Defense Intelligence Agency in a variety of capacities -- most recently with DIA as senior staff officer in the Defense Counterintelligence and Human Intelligence Center, responsible for assessing the effectiveness and viability of defense HUMINT worldwide.

He is also -- and we shouldn't hold this against him -- a lawyer. And in addition to a very distinguished private-sector career, spent some time on loan to the Special Court for Sierra Leone as a legal advisor in the war crimes tribunal they set up there.

He has a bachelor's from the University of Maryland, and a J.D. from Brigham Young University.

So now I'd like to invite David Hathaway to present a summary of some of the research he's been working on here.

COLONEL HATHAWAY: Great. Thank you very much for the introduction.

First of all, let me say that some of my comments will directly address the handout that was provided on the way in. It's a little bit easier to look at pictures of command-and-control diagrams than for me to stand up here and try to describe them to you.

But in North Africa, during 1941 and '43, the Allies struggled to gain momentum

against the German forces there. It culminated in an Allied retreat in the area called Kasserine Pass in Tunisia. Things were looking pretty bleak for the Allies. The U.S. had not learned the lessons of centralized control of air power that the British and French had already learned. Aircraft were designated to primarily support specific ground units, and always operated in a subordinate role to those ground commanders.

This inefficient use of air power essentially relegated it to the role of flying artillery. No efforts were made to take out German airfields, logistics or command-and-control. They were not seen as the immediate threat. This strategy left U.S. air and ground forces vulnerable to the persistent and devastating effects of German aircraft.

After the Allied retreat through Kasserine Pass, revisions to a more centralized command-and-control structure allowed the U.S. Army Air Corps to capitalize on the flexibility of air power, and interdict German logistics, target airfields, and eventually establish air superiority. This enabled the Allied ground forces to push the weakened German forces off the African continent.

What does this have to do with cyber in 2011? Well, today we're seeing a similar debate within DOD on the optimal way to command and control cyber forces. Just like the U.S. Army leaders failed to recognize the flexibility of air power in the early 1940s, today the DOD leaders fail to recognize the unique characteristics of cyberspace -- characteristics that warrant a unique command-and-control structure.

Let me start by saying that though Cyber Command was stood up and became fully mission-capable last November, the command-and-control debate is still not settled.

Before I get into my discussion of the command-and-control options, and my proposal, let me discuss some of the factors that influence the debate.

Cyberspace has some unique characteristics that impact the choice of a command-and-control structure. First is the speed at which cyber-operations occur. They occur much faster, exponentially faster than in any of the physical domains. In the time it takes you to blink, cyber-effects can transit the entire globe. It takes .17 seconds for cyber-effects to move around the globe.

The second is the lack of geographic relevance. You don't need to be in the same geographic location, as you do with physical forces, to produce an effect.

The reverse is also true. So just because you may be in a geographic region -- the European Command, the Pacific Command, African Command -- just because you're located in that region doesn't mean that attacks against your networks, and your command and control are all going to come from within that region. Through cyberspace, they could easily come from anywhere else in the world.

And lastly is the viral nature of operations in cyberspace. As an illustration, we can take a look at the Stuxnet worm that attacked the Iranian enrichment facilities last June. While many characterized that Stuxnet worm as a precision weapon designed to attack that specific system -- and it was an air-gap system, by the way, so not connected to the internet -- that worm has been found in over 60,000 computers in almost a dozen countries. While antidotes have been found to basically negate the effects of that worm, the importance of the fact that it spread that virally, and that it was such a precise weapon, is just an example of the viral nature of anything that goes on in cyberspace.

Besides these characteristics, there are some constraints that impact DOD's command-and-control in cyberspace. First of all is personnel. It is a relatively small pool of cyber-experts within DOD. So trying to divide those up and place them all around the world dilutes the pool, and dilutes efficiencies.

Secondly, for the most part, personnel is a zero-sum game. If you want to create more cyber wars, you've got to take it from somewhere else. We're not going to expect to see an increase in N-strength within DOD, personnel N-strength, in order to make up a cyber force. While DOD may come up with some creative ways to bring on some civilians and Reserve Guard capability, there's still a cost there that will affect the choice of a command-and-control structure.

Next is the network architecture within DOD itself. A lot -- many people go, "Oh, it's '.mil'. It's one network." That is the farthest from the truth. We have about 15,000 networks within DOD, serving, at any point in time, about 7 million computers

and telecommunications devices. Each service owns their own piece of the network. Pacific Command doesn't "own" their network. It's provided by the Services. And each service has structured it in a way to best optimized to support the war fighters.

These different command perspectives -- I'm sorry, taking those things into account, and then applying the different command perspectives leads to differing command-and-control structures. Cyber Command, for example, their mission is to operate and defend the global information grid to conduct full-spectrum operations, then, as required. It sees these cyber threats as a global threat that easily traverses sovereign boundaries.

This global nature, tied to the speed at which cyber effects can occur, drives a more centralized control structure to create efficiency and capitalize on the inherent flexibility of cyberspace.

The other perspective I looked at was that of the geographic commands -- EUCOM, the Pacific, European, AFRICOM, for example. They are given their responsibility and authority over that reach for operations in that region through the Unified Command Plan signed by the President of the United States. They get assigned an attached force -- physical domain forces -- to execute regional plans from shaping all the way through kinetic contingency operations. They see cyberspace as another operational domain that they must integrate with the physical domains that they essentially own. So they see a more regional-focused command-and-control structure as necessary for cyber.

Many command-and-control proposals have multiple variations, but they essentially boil down to two: a centralized and a regional focus. The regional-focus model is the Special Operations Command, the SOCOM model. Whereas the more centralized model is the Transportation Command, or TRANSCOM model.

Let me describe each of these a little bit.

The SOCOM model -- the key feature on the SOCOM model is a regional cyber component. It's similar to the air component or the land component or the maritime

component. It puts it on equal footing, and treats it very much the same. The primary relationship between the geographic combat-and-command, and the regional Cyber Command component is the strongest relationship. Just like in the SOCOM model, that's where the strong relationship is. It's a regional focus.

They will have at least operational control of the regional cyber forces and, thus, the networks. Cyber Command would assist the regional cyber components with interagency coordination and de-confliction. But, again, it's a regional mission. Cyber Command would also be responsible for any time a cyber operation would cross those regional boundaries, however.

In support of contingency operations, and the stand-up of one or more joint task forces -- the JTFs -- Cyber Command would reinforce this regional component, as necessary, to support this geographic component.

The advantages of this model is that it's a proven model. It's combat proven. Most recent successes have been touted in Iraqi Freedom, and are very visible there with the integrated and joint effort that happened between Special Ops and conventional forces in the Iraq theater.

It also treats cyber operations just like operations in the physical domains. Again, it's a cyber component. It maintains unity of command, and that's the big thing for the geographic component commands, because that, to them, provides the best opportunity to make sure they get an integrated effect.

The disadvantages -- as I've alluded to -- is that the SOCOM model is a regional model. And while that's a great fit for Special Operations, where nearly all of their operations are regional operations, cyber operations are just the opposite. Most cyber operations are going to be global -- have a global effect. So, in that respect, it's not a good fit.

It is also unlikely that we are going to see the authorities to execute cyber operations delegated down to that regional component command, because of the viral nature or the sensitivity of some of the techniques, as well as de-confliction with the

agency partners such as CIA, FBI, NSA, Homeland Security. Because of that de-confliction and coordination that has to go on, again, it is unlikely you're going to see a lot of the authorities delegated down.

The next -- and probably the most important -- is the significant resources required. If you're going to stand up a regional component, cyber component, in each of the geographic components -- all of the unified commands, for that matter -- you now have to have a significant manpower pool, as well a restructuring of the networks to create a regional joint operations area. And that is not a small feat.

And, lastly, Cyber Command is still responsible for operations across the geographic boundaries. So, since most of operations are likely to do that, again, there is little -- there is a significant cost to generate a SOCOM-like model, for little gain.

The other model is the TRANSCOM model. It's much more centralized. In TRANSCOM, they maintain operational control of essentially all the assets that support mobility operations around the globe. A few assets may get chopped to a geographic commander, but those are for only intra-theater mobility missions, and it’s the exception, not the rule.

This centralized control allows much more flexibility in supporting multiple customers and juggling global priorities, similar to Cyber Command and what they have to do. But they -- so, in this model, Cyber Command would retain operational control of all the cyber forces.

In this model there's a joint synchronization center that coordinates cyber requirements for Cyber Command. It belongs to the geographic component command and does that coordination. During contingency operations, you'd have a director of cyber forces that would work for the Joint Task Force, and they would coordinate cyber activities. And if you look at the diagram, there are a bunch of lines out of that individual, coordinating all the activities for cyber for that Joint Task Force. The common thread through all this is coordination.

The advantages? It's a centralized-control model. It works well for Cyber

Command to be able to shift effort, as required, for global priorities. It allows Cyber Command to better coordinate and de-conflict operations. And a majority of the Forces would reside where the authorities are expected to reside. It's the most efficient use of a limited number of cyber forces.

The disadvantages are that there's no unity of command for the geographic commander. It creates challenges to integration with the physical domains. This is exacerbated -- because if you're not going to have unity of command, you at least want unity of effort. But this doesn't provide that, either. Because of the massive integration, or coordination that has to take place with the TRANSCOM model, those lines are blurred and, really, prevents, or is a barrier to having good unity of effort.

So neither model is a great fit. We need a command-and-control structure that will enable global operations, while still facilitating regional integration with physical domains.

My proposal and recommendation is a hybrid model. It capitalizes on the advantages of both models. It has a TRANSCOM-like centralized command-and-control structure which enables missions and extensive interagency coordination, but it has a much more defined SOCOM-like component than TRANSCOM has.

The difference is that this component belongs to Cyber Command, not to the geographic commander. However, the geographic commander will have tactical control to direct operations within cyber, and make sure that their concerns are addressed. This avoids the massive coordination of TRANSCOM model, and facilitates integration of cyber-operations with the physical domain operations.

This structure ensures unity of command for a majority of cyber operations -- those at the global level -- while ensuring unity of effort at the geographic level.

While this hybrid command-and-control structure is the basis, DOD can avoid another, hopefully, Kasserine Pass, and proceed toward the goal of achieving cybersecurity.

MR. FRIEDMAN: Thank you. That was very interesting, and excellent segue

on the topic of how to achieve cyber-superiority, and what that might mean.

And so we invite Lieutenant Colonel Carter to talk about some of the work he's done on that.

LIEUTENANT COLONEL CARTER: Thanks, Allan. And, Dr. MacKay, thank you for being here. I look forward to your comments. And, Colonel Hathaway, it's a pleasure to share the podium with you.

And so, as we start our discussion to talk about our research and our walkabout -- I consider myself on a walkabout, on my journey at Harvard and away from the Marine Corps -- to think about some things that are typically perplexing to the Department of Defense. And one of them is cyberspace.

And so one of the questions that I ask myself is -- and deeply troubling to me -- is about the notion of achieving "cyberspace superiority."

And so I want to start out our conversation by attempting to frame the problem by sharing a comment that was made by Deputy Secretary of Defense Lynn in a *Foreign Affairs* article, really articulating what cyberspace means to military operations. He stated that "DOD data systems are comprised of approximately 3.5 million computers, running thousands of applications over 10,000 local area networks, on 1,500 bases in 65 countries worldwide, connected by 120,000 telecom circuits, supporting 35 major networks, over three router-based architectures transmitted unclassified, secret, as well as top-secret level information." And that all is just on the fixed-site profile.

So as we look at this problem, we can see that the same technological advantages that have transformed our military into what I would argue is the finest fighting force in the world, we also see that the adversaries have an opportunity to exploit our weaknesses.

So I go into my "Problem Statement" by setting the paper up and saying that since the official Department of Defense-designation of cyberspace as a war-fighting, or a separate and distinct war-fighting domain, the Department policymakers, Joint Staff, and particular some of the Service planners have begun to develop concepts and

doctrines to achieve cyberspace superiority. But based on what we know about cyberspace, I asked, "Can that be achieved?"

Our research has two goals. And the first is to clarify what the term "cyberspace superiority" means, and second, to examine the ability of the Department of Defense to actually achieve cyberspace superiority. I base this on the premise that cyberspace is a very complex operating environment, with unique properties and characteristics -- which we heard from Colonel Hathaway's presentation -- influenced by multiple stakeholders. And I would argue that it's misunderstood by many policymakers as well as planners.

So we concluded that multiple factors will impede the Department of Defense to actually achieve cyberspace superiority. I base this argument on the following propositions.

The first one is the bureaucratic organization of the government is not conductive to addressing the cyber threats.

The second, DOD policy and joint doctrine are still in very developmental phase, and therefore inadequate to address military cyberspace operations.

The third -- Department of Defense is tasked to protect national security, and that's the ".mil" domain, but does not manage the assets to provide the function that must be protected; i.e., they have no control over the .gov, .org, or .com domains.

And, fourth, U.S. domestic law, as well as international agreements, limit the Department of Defense from conducting cyberspace operations.

So, in terms of research methodology, our paper takes a systematic approach at examining some of these problems. And we look at a number of things. First, we examine cyberspace domain, its related components and associated terms, to gain an appreciation for how complex cyberspace domain is.

And we take a look at condition versus capability. There's a great debate whether cyberspace can be viewed as a "condition" within a new war-fighting domain, or a "capability" that can be integrated into a time-tested military decision-making process.

In establishing terms of reference, operational planners are incline to view cyberspace in terms of information warfare -- through an information warfare lens, I should say, by simply replacing terms to gain an understanding of how superior -- or the complexities of cyberspace. But I would argue that, in doing so, it's a fundamental mistake that will lead to gross miscalculations, and also yield flawed concepts to drive the planning process.

So there is an important distinction to be made between a "condition" and a "capability." A "condition" refers to a mode or a state, and a "capability" instead signifies the possession of necessary resources or power to achieve your objective. Throughout our analysis, we view cyberspace, or cyber as a condition which operational planners and joint planners need to achieve on the basis for deciding further action.

So we, second, take a look at examining the challenges associated with the Department of Defense efforts to transform cyberspace into a war-fighting domain. Although viewed broadly by the Services in the earlier part of the 21st Century, the term "superiority" -- or, I'm sorry, "cyberspace," we would argue, did not become an official part of the DOD language until the release of the 2006 "National Military Strategy for Cyberspace Operations." Even the recent publication of "Joint Terminology for Cyberspace" lexicon by the Vice Chairman of the Joint Chiefs of Staff, we would argue that the terms and concepts associated with cyberspace still remain very confusing and unclear.

This confusion contributes greatly to our inability to develop plans to synchronize our actions and our efforts in cyberspace. We see the impacts of this confusion as the Services begin to develop their own joint operating concepts for cyberspace operations.

As a starting point for normalizing the terms and related documents, this document -- this lexicon that I referred to -- defines "cyberspace superiority" as "The degree of dominance in cyberspace by one force that permits the secure, reliable conduct of operation by Force, and its related land, air, sea and space forces at a given time and sphere of operation, without prohibited interference by an adversary."

The concept of preventing "prohibited interference" does not mean that no interference exists, but that any attempted interference can be countered, or should be sufficiently reduced to have little or no effect on the success of an operation. And this is where we remain skeptical about the Department of Defense's ability to achieve cyberspace superiority.

Third, we examine cyberspace from a Joint Operation concept that was published by Joint Forces Command. Essentially, the document is the way that Joint Forces will go about cyberspace superiority. And the central idea of the concept is that the joint war-fighter signifies sufficient -- or requires sufficient security capacity and capability to successfully plan and execute missions.

When you analyze the separate components, the nature of the Joint Forces objective is twofold. The first part is to ensure freedom of action for friendly forces. And then the second component is to deny the adversary the same.

So we take a closer look at both to determine the impact of the Department's ability to achieve cyberspace superiority. And by examining the two components' superiority side by side, we see a strategic center of cyberspace superiority as the control for both data, as well as the infrastructure.

Much like Colonel Boyd's "OODA loop" concept, the intent of this concept, or this model from Joint Forces Command is to execute the process faster than any adversary. Information technology conflict in a domain, Colonel Boy's concept of the "OODA loop" contributes greatly to the war-fighter thinking about maneuver warfare. However, because of the ability to, I would say -- for the adversary to overcome the critical components of both time and space, we'd argue that the concept is not an effective tool in cyberspace to determine our ability to achieve cyberspace superiority, or freedom of action. In essence, cyberspace operations can occur in milliseconds, as we've heard, and rarely will be based on actions that can be attributed to a person, an organization or a nation-state.

The key point is cyberspace superiority requires gaining and maintaining

military advantage by balancing the two freedom-of-action concepts. Therefore, achieving cyberspace superiority, we assess, that the Joint Forces must have sufficient capacity, capability, cognizance to gain and maintain military advantages to successfully execute the cyberspace mission.

And, finally, we examine the organization of our government as a critical component of making decisive decisions at the speed of not only war, but at cyber-war.

So, our research indicates that the challenges the Department will continue to face are directly related to the lack of any effective, purpose-built, standing organization or process within the U.S. Government for developing policy, or making decisions about cyberspace. Specifically, we point to a lack of comprehensive cyberspace strategy, a lack of clear policy and authorities, and the absence of an organizational structure to serve as the -- what I like to call the "forcing function" to implement the policy. In our inabilities to govern effectively in cyberspace is that it impedes Department's efforts to achieve cyberspace superiority.

And to illustrate my point, I'd like to take a look at how China views cyberspace. The importance of cyberspace is derived from China's concept of strategy, which is based on the idea of a comprehensive national power. China's cyberspace strategy is based on China's philosophy of chi, one of the three requisites for global governance. Chi is established by identifying an adversary's vulnerabilities, and then assigning and then assigning appropriate tools to exploit and then get after these vulnerabilities.

So if the U.S. took a similar approach to cyberspace as the Chinese competitors, perhaps policymakers would be inclined to create a comprehensive strategy, based on fundamental goals and objectives that effectively shape the international landscape, in accordance with our U.S. national strategy or U.S. national interests.

So I quickly go to our findings. And there are four.

And that is the U.S. does not possess an enduring technical advantage over

the adversaries in cyberspace.

The second is the strategic DOD capabilities rely on the public as well as the private infrastructure.

The third, the Services have a different perspective, I would say, of cyberspace.

And then, four, the lack of system standards -- that's hardware, software, as well as supply chain -- across the Services creates a vulnerability.

So, very quickly, I look at can this be done after analyzing the complexities of cyberspace? And we have four things that we think are critical factors that prevent the Department from achieving their objectives. That's capacity, capability, cognizance, and then governance.

In assessing the four factors, we conclude the Department is unable to achieve cyberspace superiority. So we include these into our recommendations.

And that takes us into the final portion of our paper, about the conceptual framework for achieving cyberspace superiority. And we conclude that the military has limited ability to address these four factors -- or three factors -- that I talked about up front. And it's going to take significant help from the U.S. Government to address the fourth factor.

And I'd say it all starts with a strategy. The U.S. must change the way it thinks about operational environment by taking a holistic, strategic approach to cyberspace. And our recommendations are essentially that broadening the U.S. view for strategic importance in cyberspace, taking some lessons learned, maybe from China, and looking at cyberspace as an instrument of national power.

The second one is develop a national security cyberspace doctrine. And many of you may say that this is nothing new, we tried this in Vietnam. And I'd say you are correct. But the challenge with the Vietnam piece is most of that doctrine was in the classified channels, and it never made its way out. And we can talk about that more in our discussion on President Bush's initiative that's slowly making its way out, as well.

The third one is modernize authorities for military cyberspace operations. Currently, we all know that U.S. Cyber Command does not possess some of those authorities to what I consider to be able to find, fix and finish threats within the domain. And so I'm essentially offering an opportunity -- or recommending an opportunity to develop an ability to hunt on a network.

Fourth is to mandate joint standards. I think it's easy to see, when we look to the Services, and how they field their systems down to the tactical and operational level, or fielding different systems. And if we're ever to -- if we're to operate to Joint standards, interoperate at the Joint level, then I say that we ought to mandate some Joint standards across the global information grid.

The fifth is establish a common operating picture. And General Alexander has pointed to this many times that we don't have this, and we're going to have to rely on the public and private sector. In order to do that, I think we ought to exchange L&Os to build trust, as well as facilitate situational awareness.

And then, finally, as we alluded to earlier, we're going to have to grow the force. And when we talk about a capability, we're talking about people, training and equipment. And all of that, in my mind, would equal capacity.

So, in closing, the dawn of the 21st century presents strategic challenges for the United States. And our research has made it clear that achieving cyberspace superiority will be a bold endeavor. Sophisticated threats will require innovative solutions, and demand new approaches in order to mitigate that risk. In essence, the cyber threat environment will demand a new mindset to ensure agility and adaptability for new challenges.

Our national approach to cyberspace must adapt to meet these rapidly changing challenges.

Thank you.

MR. FRIEDMAN: Thank you, Jerry.

So we have two bold endeavors in front of us. We have to figure out how to

do, or how to think about, superiority in the cyber domain, and we have to understand the evolving command-and-control relationship in this domain.

I'd love your thoughts on how we can tackle these bold endeavors.

MR. MacKAY: Oh, to have bold thoughts.

By way of disclaimer, I'm here today as an individual who has an interest in the topic. My comments certainly do not reflect the position of the Defense Intelligence Agency -- although you will pick up some snippets of that as we go through -- nor of the United States Marine Corps or the Marine Corps University.

I think that Lieutenant Colonel Carter may have given us the understatement of the century when he said that the "terms are confusing and unclear." Command-and-control -- I'm not even sure I know what a "cyber force" is.

When you think of conventional military forces, you think of, if you will, the "doers," the war-fighters, and those who support them. They support them in a direct war-fighting role -- weapons maintenance, aircraft maintenance, weapons procurement, things of that sort -- or in a more generalized role, like in one of my other hats, as an attorney.

I don't know that anyone has looked at the cyber world for that. We have CYBERCOM. We have fill-in-the-blank Force Cyber -- Army Force Cyber, Air Force Cyber (inaudible) Cyber, 10th Fleet.

Does DISA fit into that? The Defense Information Systems Agency? Who maintains these systems? What are these systems? We don't even know what we're talking about, ourselves. Secretary Lynn's comment kind of understated by a factor of at least 50 percent the number of countries we do business in. My own agency has computer networks operating in over 130 different countries. And that's just one agency.

So we haven't learned how to count. We haven't defined terms in a way that makes sense. What is "cyber conflict?" We don't know yet.

How do you "command" a civilian? Having been in uniform and now in the civil world, I can tell you from my legal background, "controlling" civilians is difficult enough,

without trying to "command" them.

So we're talking about a command-and-control structure. That makes very good sense. We have identified cyber as a war-fighting domain. And, again, I'm not sure that I know what that phrase means. I know how it relates to the physical world. I understand, I think, John Boyd and some of his concepts. I've spent some time, now, with the Marine Corps, a little more time with the Army, have some nodding familiarity with the Navy and the Air Force -- and each of those military services is optimized to function within a specific physical domain.

But cyber, that has all of the characteristics of a physical domain in the sense that you can go there, you can play there, you can do things -- has characteristics that are absolutely unique. In the world of communications, for years and years and years, we've used telephones that are connected to a wire, that goes to a switching center, that goes out via a wire to another switching center, that goes out via a wire to a telephone in someone's home or office. And up until about 30 years ago, if you were to tinker with those wires, the owner would be very upset. And in some places in the country, you would actually face criminal sanctions.

Now, we have this thing called cyberspace where we have this patchwork quilt of providers. We have governments involved, we have private companies involved, we have universities involved. They all contribute to this thing, but no one of them owns it.

So if it's going to be a war-fighting domain, if it's going to be a place where we're going to exercise superiority, what is it we're going to own, and over what are we going to exercise this control authority? Lieutenant Colonel Carter made a very telling point in his paper, and in his presentation, identifying the mismatch between the defense mission and the reach of the population to be defended. For those of you that had seen the National Defense Strategy -- no, I won't say that. Who knows, I might be considered for some appointed office at some point and it would not politic to say the thought that just came to mind.

Let's be charitable. We'll call the National Cybersecurity Strategy

"aspirational." That's a fancy word that means hope. Some of you may remember General Powell saying, "Hope is not a strategy."

We have a responsibility to defend, within this context, the Department of Defense and its constituent elements. What are those? Well, it's kind of easy to define the people who wear military uniforms. That works fairly well. Then you expand it out to the next circle, for the people who work in military facilities, you know, that are owned and operated by the Department of Defense. That's fairly easy to define.

Where do we get our cyber toys? Mine come from Dell, because I happen to like Dell. I use Cisco routers at home. Where is Cisco building its routers? Not in the United States.

We have this giant industrial base that supports this domain that we are going to attempt to control, but we don't have control over the components therein. Historically, the United States has built its own weapons systems. A lot of other countries buy them -- because, frankly, it's bloody expensive to build a weapons system.

We haven't tried to build cyber weapons -- in the hardware sense -- in any meaningful unclassified discussion. We buy the stuff from somebody else, which means we've immediately lost control.

We have -- I'll put on one of my other hats for a moment, the law. When I first came into the cyber side as an attorney most of my clients were people with their hair on fire, and eating wastebasket-size containers of Tums. Because what they wanted to do, what they needed to do, in order to be able to attribute and act, we're not even going to characterize it as an attack yet -- and I'm not sure what that means -- but to attribute an act to a location was prohibited by law.

We have fixed some of that now. We do have white-hat hackers. But, as is typically the case, law follows developments in society. Law typically does not anticipate and structure for society. And the few times we've tried to do that, historically haven't worked well in the U.S., which is, I guess, to put it nicely.

At this point, I think I will wind down by saying the job of cyber is that it gives us

a domain that is probably unique in military history. Over the centuries there has been a constant tug of war between -- if you will use terms poorly -- warhead and armor. And warhead always wins, because it's always cheaper and easier to build a bigger warhead than it is to build better armor.

We are now in the bizarre environment that Vince Lombardi, the late head coach of the Green Bay Packers would recognize. He once stated that the best defense is a good offense.

In today's world, virtually the only defense we have is offense, because the offensive capabilities in this world so far outstrip the defensive, that it's not really worth having a meaningful discussion.

And speaking of discussions, it's probably a good time to have one.

MR. FRIEDMAN: I think so. So, I'm going to seize the moderator's prerogative to pick up on the last point, which was actually the first point I wanted to raise, is this tension between defensive posturing and offensive posturing. And I've done a little work on trying to balance out how this would fit, both organizationally and tactically.

But I'd love to look at through a lens of both superiority and command-and-control. Does this distinction of warhead versus armor, does it help us to actually undo some of the work that we've done in sort of binding together the defensive posture and the offensive posture through CYBERCOM.

Is that a useful distinction in helping to tease out some of these problems? Or does that lead us down the wrong path?

COLONEL HATHAWAY: I'll start. With respect to command-and-control, it is something that is easily simplified. And for discussion's sake, it's much easier to simplify it down to go you've got "provide, operate, defend, attack, and exploit" within cyberspace. So it's easy to put everything in nice little categories and leave it there.

The provide and operate? Yeah, that's what we've been doing forever with the Internet and, you know, .mil. That's the part that we were good at, and it is not par of what historically is thought of as a war-fighting role. It's a function, a support function

that's been provided.

Now you get into defend and attack, and that's where it gets really mushy, especially if you try to delineate them out and go, okay, under this piece of command-and-control, we're going to have operate and defend -- provide, operate, and defend.

And then your attack and exploit are going to be your special -- your ninja guys are going to come in and walk in for a contingency operation.

The problem is it's not that clean. Because so much of defense requires to defend, to stop somebody from attacking you may mean you reach out and thump them through cyberspace. Well, that looks awful offensive to them.

So, the defensive actions while, yes, the antivirus software is important, patches are important. The patches usually occur because of a vulnerability that was exploited by somebody that we found out. So all those things are after the fact and reactionary. And it's usually the attackers have moved on to something else because they know that once they pull a trigger on some offensive tool, we figure it out and it's no longer a valid tool.

So, having the ability to reach out and do active defense is a key part of being able to at least approach anything that resembles superiority within cyberspace.

LIEUTENANT COLONEL CARTER: I'd agree with that. I'd certainly agree. And I think we're generally out of balance with the way that we approach cyberspace. And when I say "we," I mean as a nation, as the Department of Defense. And part of that is the restrictive authorities that are placed against the Department. Right now, I think we have a tremendous defensive capability, but the offensive piece is the piece that I worry about and keeps me up late at night.

As we suggested, these authorities prevent us from doing some offensive things which we know in the unclassified realm. But, more importantly, it goes to, in my mind, deterrence. And that deterrence piece, you have to be able to not only the active deterrence, but then be able to follow up with that punishment to keep people in check.

So I do think we need to balance the two.

MR. FRIEDMAN: (inaudible) on the intelligence side?

MR. MacKAY: Actually, I was going to come back at it from your original question. I don't know whether the distinctions are helpful, but they're necessary.

Because as Lieutenant Colonel Carter has pointed out, and Colonel Hathaway has alluded to, we have two completely different authority sets, depending on which environment you're dealing in. If you're in an offensive environment, you have one authority set. And we know how to trace that. If you're in a defensive environment you have a different authority set.

In the world of cyber, you are frequently in an area that has attributes of them both, but is clearly neither. And that is part of the confusion.

If we're going to have the ability to conduct offensive operations, we need to be able to define what they are. There's still a lot of ambiguity there. Intelligence plays into it. The difference between reconnaissance and an offensive act may be little more than a keystroke or two.

Without some form of definition, we have no ability to move forward. And one of the things we have to keep in mind is that if we're talking about warfare, we're talking about people who have to be able to do things very, very quickly -- in the world of cyber, as Colonel Hathaway points out, extraordinarily quickly. We don't have time for the how-many-angels-dance-on-the-head-of-a-pin discussion. We've got to have some bright guidelines for them.

MR. FRIEDMAN: All right, if, indeed, we have time at all to make any decision, in human time.

So, turning it over to the audience, do we have questions out here? Are there concepts that we can further break down and really just make sure we know absolutely nothing about any definitions here?

Yes.

MR. DOWNHAM: Thank you for an interesting talk. I'm Gene Downham from the Joint Warfare Analysis Center.

Most of the discussion from the panel seemed to be addressing the domain of cyber conflict that was more the equivalent of hot war. I want to talk more about the domain of ongoing competition for technological and commercial advantage, and just get the opinion really from any of the panelists as to how we should structure command-and-control in this sort of ongoing competition.

Is that the domain of the intelligence community? If so, is the intelligence community structured properly to address it? What's the DOD role in that? And what's the role of the private sector in that?

Thank you.

COLONEL HATHAWAY: There's no quick answer to that one.

I think we see when you look at where CYBERCOMMAND is located in the NSA building, I think that goes to some of what you're getting at. I mean, somebody may be sitting down and doing an exploitation job under Title 50, and then go, okay, now I'll switch hats. Now I'm a Title 10 kind of guy. Send.

There is some dual-hatting that's going on with respect to that. And so I think, just our structure that we have set up, I think is somewhat necessary. Because, as Dr. MacKay talked about, some of the legal issues involved with a lot of the things that go on in cyberspace -- and a lot of that is undefined still, I think, today, how well we do in there.

I think what's going to have to happen is we're going to have to really define out exactly what we want to do, and get those permissions, almost one by one. And what that will take is a little bit of a bunny-trail here, but that's going to take, I think -- as we do our war plans, our operational plans -- which include Phase Zero operations, the steady state -- those things will have to be planned in and get pre-approval. Because of the time constraint, you're not going to have time to go ask, in many cases, ask for permission if you're trying to fend off an attack.

But that goes to another issue, and that's -- I mentioned the Phase Zero operations. The stability ops that are going on in all of the geographic commands

around the world is that just because the physical domains are operating in Phase Zero, many argue that cyber is already in Phase Two, seize the initiative.

And so we see almost a different level of warfare, if you would, going on in cyberspace already, in what we consider kind of a steady-state timeframe. So it becomes very difficult and hard to comprehend

That doesn't help much.

LIEUTENANT COLONEL CARTER: I'll just take a quick stab at the question. Very interesting one, and one I think we all ponder, about the intellectual property, and where the U.S. stands in the world.

I think we all know that we can't turn a blind eye to how China is absolutely, some would argue, out-competing us in cyberspace. And so, in terms of how do we remain one of the relevant superpowers on the international scene -- if not the superpower -- it's going to take an interagency approach. I can't believe I'm saying that, but it's true.

I think, across the board -- we talked about how complex the domain is. I think it's going to take the interagency -- that's both public and private sector, as well as the federal government -- to come together to figure out this problem together, as a nation, as we move forward, as opposed to, you know, the stovepipes that we traditional have come to love, I guess.

MR. MacKAY: We touched on briefly about the command-and-control, and its relationship to the intelligence community.

One of the overarching challenges we have in the world of cyber is that every entity that looks at it tends to look at it through its own lens and see it in its own environment. So the war-fighter wants to control the domain, because that's where they're going to fight. The intelligence community will want to control the domain, because that's where they will collect intelligence.

I would not give the intelligence community that responsibility for several reasons. One is the possible lack of talent. Two -- you notice I wasn't smiling there.

Two, and perhaps more important, the intelligence community needs to be perceived as, and actually needs to be, a neutral provider of data. Giving them control of a domain, no matter what the domain is, immediately calls the reporting on that domain into question.

MR. FRIEDMAN: The one in the middle there.

MR. NEWBURY: Brian Newbury, from the Wilson Center. Just real quickly, a re-attack on the authorities question. I do always hear that is one of the biggest stumbling blocks. This question is for any of the panelists.

Do you think, at the end of the day, it's going to take a cyber-Pearl Harbor or a 9-11-type event to really get everyone's attention and cut through the chaff, and start to get authorities out there for folks to do what they need to do?

COLONEL HATHAWAY: I think it is going to take some large event that's really going to have to break some of this stuff loose. Because of the sensitivities of unintended damage that you could have with cyber operations, I don't see those things easily being released.

We do see some actions going on in some areas around the world, whereas a fairly small operation that can be -- can be -- somewhat constrained in its collateral damage. And those are being delegated down.

But for the vast majority, those authorities are being held very high. Sometimes CYBERCOMMAND -- and many times CYBERCOMMAND doesn't even have the authorities, that they have to go ask for them from much higher.

So, I think it is going to take something like that to bring the attention to these capabilities, and the willingness to put up with some collateral damage.

MR. MacKAY: If we're going to use cyber as a form of warfare, we're going to have to be able to fight it into the long-armed conflict. And the challenge we have now is that where we can measure effects of a weapon in the kinetic world, we still have great difficulty doing that in the cyber world, as Colonel Hathaway has pointed out.

We have great difficulty confirming the legitimacy of a target. We have great difficulty identifying the actor to be struck. We can put all the authorities we want

downstream, but until we can solve the targeting issue and the collateral damage issue, we're not going to help ourselves. They come hand-in-hand.

MR. FRIEDMAN: Question in the back corner?

MR. BARTHOLME: I'm Jason Bartholme, U.S. Air Force. I guess my question is for the panel at large, and this gets back to a little bit of the definitions struggle we've been having.

It strikes me that, when you think of cyber, you have sort of the abstract flow of information across the internet and software, and sort of the soft side of it. But then you have a really significant brick-and-mortar side of it where -- the gentleman talked about components' being manufactured in different parts of the world -- and the tools that are actually being used to conduct attacks.

I guess the question I had is that do you all see a future where there will be a co-mingling of kinetic forces and sort of non-kinetic forces, where cyber, and the umbrella of cyber, embraces both the physical and kinetic targeting of these infrastructure targets, alongside the sort of ethereal soft side of things?

COLONEL HATHAWAY: I will tell you, that's where the geographic want to go. I mean, that's their goal, is to be able to get to that ability, that level of integration. That's a -- it sounds very easy, but it is not. It is extremely complicated for all the reasons we've discussed, especially authorities, in that respect.

So -- but that is the goal. As you get this co-mingling of capabilities, that you have a cyber effect enabling a kinetic effect, or maybe vice versa. For example, the Israeli attack on the Syrian -- suspected Syrian nuclear facility that was enabled, that was essentially a small raid by a few fights of their Air Force fighters that could or that would have otherwise -- it was enabled by cyber. Cyber basically disabled the Syrian air-defense system. So they were able to go in and strike that facility and go out unscathed. The Syrians sat back and looked at blank scopes, thought it was another quiet night.

So that is just an example of the ability to integrate those two capabilities, and

really what everyone, I think, within DOD is after -- as well as protecting our sown information. But that, again, is not easy to do with the authorities.

MR. BUNNING: Scott Bunning. I'm a military fellow at RAND. I had a question for Lieutenant Colonel Carter.

A lot of policy on cybersecurity, especially in the civilian sector. There's also a term I heard of "cyber resilience." You know, in the military kinetic forces we talk about "operating in a denied environment." I mean, if they're jamming our radar, how do I work through that?

And I think also in the cyber forces, or in policy, especially from a military-DOD context is cybersecurity or cyber resilience? Can you comment on either one of those concepts?

LIEUTENANT COLONEL CARTER: Yes, thanks for the question. And I think you're absolutely right, in terms of resilience.

I think we all know it's not about when we get hit, it's about how -- or it's when we get hit. And so we ought to, in my personal opinion, focus on the resilience. And that is the recovery, and then how do you get back to business?

And so I think a large part of our effort -- as we're talking about these defensive and offensive components, and freedom of maneuver, we have to absolutely focus on the resilience piece.

MR. FRIEDMAN: Yeah, the center, here.

MR. YOUNG: Zach Young from Harvard.

So, we're arguably more reliant on cyber technologies than other countries. And we're faced with these tremendous challenges and we don't know how to solve them. So kind of to hedge against the answer to these challenges, do you think it's wise to try to reduce our reliance on cyber devices?

COLONEL HATHAWAY: Good luck with that. (Laughter) I don't think you could convince anybody to stop buying the iPads or the iPhones or any of those other devices. Which really brings another spectrum in the case. And you're talking to all the

electronic spectrum. And that goes to where does cyber end? And the confusion of, again, go back to the terms, defining "cyber" to begin with.

The Navy, in fact, has taken a different tack. They include electronic warfare, under 10th Fleet, which the other services do not. So a little side note there.

But I don't see us having the ability to stop our reliance. I mean, first of all, you go to the discussion that Jerry brought up, which is the OODA loop, Boyd's OODA loop. And if you want to stay ahead of your adversaries, and stay inside of their decision cycle, that's going to require even more reliance on these types of -- this type of technology.

So I don't see us going backwards.

LIEUTENANT COLONEL CARTER: Zach, I agree. And I don't think we should. We ought to embrace this technology.

And I go back to, you know, we consider cyberspace as a man-made environment. And so all these problems that we're having, I think that we can overcome. I'm confident we can. We just have to have the will and the patience to overcome some of these things.

So I certainly don't think we ought to go backwards. I think we ought to embrace some of the research and technology, get our acquisition cycle fixed to get ahead of some of these things. And then, really, the partnership -- I can't underscore that enough -- that the partnership between the private, public, as well as the government piece is absolutely key.

COLONEL HATHAWAY: If I could just add one other point, though, I think we have a duty to make sure that we understand the vulnerabilities, though, and that we make sure we have a backup.

Because we certainly don't want to be sitting back completely crippled because I can't get on the computer. So, therefore, we don't command and control, we don't execute. We have all this great technology that we can't use because it's been crippled. So, we do need to be at least aware of the vulnerabilities, and prepared to take backup

actions.

MR. MacKAY: To be brutal for a moment, even if we did, no one else would.

Estonia has been there ahead of us. They are far more wired that we are. They've been terribly victimized by an anonymous attack coming from a country to their east.

And, as a result, they've taken defensive measures. They've learned. So will we.

MR. FRIEDMAN: And I just want to point out that the way that you change a relative disadvantage gap is you can make yourself less dependent, or you can sell some more things to other people so that they're more dependent. Just another option that might work well.

And there's, I think, for a number of the adversaries that we might be talking about, we might have a strategic advantage there, if both of us are dependent on systems.

I think we have time for maybe one or two more questions. So let's take -- there was a question there. And if there's maybe one more, we can batch them.

MR. HUNTSMAN: Thanks. Steve Huntsman from Equilibrium Networks.

Colonel Hathaway, I'd like to pick up on the point that you just made, where you talked about having a backup.

And one thing that you see a lot in viruses is polymorphic code, where the virus itself, or the worm, will, you know, change its behavior autonomously, and the code will, you know, switch between the different sections.

Now, there's no reason, in principle, that we can't do that with the systems that we use in DOD, using the firm-ware on the routers, the software that we use, have it be polymorphic. And there's going to be some overhead in the design of that code, but DOD can mandate that if you're going to see to DOD, you have to make this code polymorphic -- and open-source, moreover, so that we can take a look at it and introduce our own capabilities into that code.

And what I think that might do is introduce an element of strategic ambiguity to an adversary, where they say, "Well, we're going to try and take this guy down, but we don't know if he's going stay down, because he can just switch stuff out."

And so I was wondering if you could comment on that.

COLONEL HATHAWAY: Sure. I think what you propose is a great idea. The problem is, since we've gotten away from, you know, in many cases, the "mil" standard that cost us a fortune within DOD to buy more off-the-shelf technology, you know, we have gotten away from the capability to do what you're talking about.

So -- and, again, with this mismatch of networks, and different routers and servers out there, it would be a long process to do that. But I definitely think it would be worthwhile, if we're really going to try to defend the networks.

And that goes a little bit back to the kind of the restructuring of the networks. I mean, cyberspace is a man-made domain. We built it, we can change it. It doesn't mean it's easy to change. But it can be changed over time to be more adaptive and reactive, without waiting on the man in the loop to try to fix it.

MR. FRIEDMAN: All right, I think we might have time for one more quick question.

Yes.

MS. MARCONI: Yes, hopefully, this is a quick question. Janice Marconi, Marconi Works International.

Different strategies, some of them tend to be stuck in the website browser mode, where all of a sudden things are changing so rapidly we're into an apps world.

Are we really -- are we falling behind? In other words, if you have -- anybody who has their iPhone, any one of the things, there's tens of thousands of apps that they're capable of.

Which means -- I finally bought a book that's -- what is it? -- *The Idiot's Guide to Developing Your Own Apps*. And I'm having fun doing that, which means -- and I'm not that capable. I just thought I'd go through the exercise. Which means people that

are far more capable are developing apps.

How does that fit within a cyber strategy?

MR. FRIEDMAN: So, in two minutes, I'd like you to address the mobile threat. (Laughter)

MS. MARCONI: Sorry about that.

LIEUTENANT COLONEL CARTER: I'll take 30 seconds of it. I'm not sure we can address it.

But I would go back to one of my recommendations about growing this force, and keeping some of a resilient force that is capable of keeping up with some of these challenges. I'd go back to research and development, the acquisition piece of it, to try to stay ahead of this.

I don't have a solution today. But we have to grow, in my personal opinion, that professional force that is able to keep up with this technology as it continues to move forward.

COLONEL HATHAWAY: I will just say that the changing role -- I think we are, especially within DOD, lag behind, because of our acquisition process. And just the behemoth that that is.

I think transitioning to something like the apps, to where basically you're talking about more of the, almost the cloud computing, where you get the computer -- that I really don't need -- off my desktop. And I now have a thin client that can access Zypper, secret Internet, top-secret, unclassified, all on one work station. And all I'm running is apps.

It makes it much easier to defend that, because the server is in one place, and it's only one -- I'm exaggerating. But it's much easier to defend something like that than the, you know, millions of computers sitting out there on desktops, much easier to keep them up-to-date, defensive-wise.

So I think that is a key leap that we need to make within DOD, which will help us significantly in our defense.

MR. FRIEDMAN: All right. And Bruce, very quickly, last word?

MR. MacKAY: I think what some might characterize as a vulnerability there, I would characterize as a strength.

In the 1950s and early 1960s, the repository of computer expertise in the United States was at the National Security Agency, because computers were big, they were expensive, and very few people had them. As a result, we hired people that were reasonably intelligent and then locked them in dungeons and fed them code until they became proficient.

We don't have to do that anymore. The world is full of people who are proficient in code. *The Dummies Guide to Programming*, you're doing it on your own. All we have to do is find a better way of capitalizing on the capability and putting it to work for us.

MR. FRIEDMAN: All right. I'd like to thank the panel for an excellent discussion, attacking some really hard problems. And also all of the fellows, for putting together this excellent conference.

So please join me in thanking the panel. (Applause)

SPEAKER: A quick lunch announcement. If you RSVP'd for lunch, it will be found in the hallway to my left. And if you will just bring it back in here, Major General Lori Robinson will be addressing us in about 20 minutes.

(Recess)