Admiral Michael S. Rogers, USN

An Interview with Michael S. Rogers

Joint Force Quarterly: *You are in a unique position in that you wear three hats: commander of U.S. Cyber Command* [USCYBERCOM], *director of the National Security Agency* [NSA], *and chief of the Central Security Service* [CSS]. *The newest of these three, of course, is U.S. Cyber Command. Can you outline what your command's mission and focus are, or what you think they should be?*

Admiral Michael S. Rogers, USN, is the Commander of U.S. Cyber Command, Director of the National Security Agency, and Chief of the Central Security Service. He was interviewed in his Pentagon office by William T. Eliason, *Joint Force Quarterly* Editor in Chief.

Admiral Michael S. Rogers: We are three organizations brought together under one leader because of the great synergy and complementary nature to the mission set among the three organizations. It was a very conscious decision to bring them together under one individual. You really get a lot of synergy by doing that, and you increase capability end-to-end as opposed to breaking it into three different components. Of the three hats, the two that I really focus on externally are commander of USCYBERCOM and director of the NSA.

USCYBERCOM has three primary missions. The first is to operate and defend DOD [Department of Defense] information networks, and to protect our information, data, and weapons systems. A lot of people tend to focus on the network piece, and that's a very important part, but we've also got to be mindful that it's about more than just the network. It's data, but it's also those combat systems that have vulnerabilities within them that we have to defend. The second mission set is to create the dedicated cyber mission force—much of it under our operational control—that DOD will then utilize and execute from the defensive to the offensive to support the combatant commanders. Our third mission is—when directed by the President in response to or in anticipation of cyber activity of significant consequence—to be DOD's response element to try to forestall, if you will, attempts to penetrate, destroy, damage, or manipulate U.S. infrastructure, such as the power grid or financial networks.

For the NSA, we're best known as a foreign intelligence organization. We use signals intelligence as a tool to generate insights into what nation-states, groups, and actors are doing that are of concern to both us as a nation and to our friends and allies around the world, and to help ensure the security and safety of U.S. personnel wherever they are in the world. The second mission set for the NSA—and the one that I think is increasingly relevant in the future, not that I think foreign intelligence isn't, but it's certainly being called upon more and more—is information assurance. We developed the cryptographic standards, for example, for all classified systems within DOD. We partner with other areas of the Federal Government to develop the same thing for the U.S. Government, and then we also partner with others to help develop the cryptographic standards more broadly for us as a nation. In addition, we help provide capability that defends DOD networks. We take our foreign intelligence insights into what nation-states, groups, and actors are doing within this cyber arena and we ensure that they get to a broad audience both within the broader U.S. Government and then out into the private sector.

Increasingly, the other aspect of our information assurance mission is NSA's ability to do big data analytics—that is, really in-depth digital forensics—and to provide expertise as to how somebody got into your network, how do we get them out of your network, and what should your network configuration look like to make sure it doesn't happen again. As part of that information assurance mission, NSA has increasingly been called upon to provide expertise by partnering with USCYBERCOM to support DOD, and to support activity across the Federal Government, in the private sector, and in partnering with the FBI [Federal Bureau of Investigation] and Department of Homeland Security [DHS]. I never thought, for example, that as director of the NSA I would be dealing with the aftermath of a major penetration and destructive act directed against a motion picture company. But that is exactly what happened in the case of the [Democratic People's Republic of Korea's] destructive hack of Sony. In partnering with the FBI, we were asked to bring our capabilities in order to figure out what happened, how it happened, and how we can make sure it doesn't happen again.

JFQ: *How does your mission at USCYBERCOM differ from those of your brother organizations, apart from what you just described?*

Admiral Rogers: USCYBERCOM is specifically focused primarily within DOD for most of its missions. There's one exception: defending critical U.S. infrastructure. The biggest difference, though, is that USCYBERCOM is a traditional Title 10 military operational organization. NSA is part of DOD and is an intelligence organization. Most of what we do at NSA is under Title 50, the part of the U.S. Code that addresses the conduct of intelligence operations. They're related but different, operating under two different authorities with different concentrations. As a result of those authorities, USCYBERCOM is a traditional military operational organization. It's just focused on a very particular domain—in this case cyber—but it does that on a global basis. That's another thing that makes USCYBERCOM a little different: we are defined by our mission, not by geography, as opposed to organizations like U.S. Central Command or U.S. Pacific Command, where you're defined in some ways by your geographic area. We are defined by our mission, and we do our mission on a global basis. Those are the really big differences. And then I remind people, "Hey, look, the fourth star comes from being the commander of the U.S. Cyber Command and not from being the director of the National Security Agency."

JFQ: *You recently signed the USCYBERCOM's Vision statement. The statement aligns with DOD's cyber strategy. How does this vision build on the DOD strategy?*

Admiral Rogers: We partnered with others to help in the development of the strategy. It's a much broader team than just us. I don't want to pretend otherwise. The DOD cyber strategy is designed to articulate in a broad manner what we are trying to achieve within cyber from a departmental perspective, and what are the basic goals that we are going to achieve to meet that strategy.

I asked our team at USCYBERCOM to think about how we would execute our set of responsibilities within that strategy. We needed to develop a vision that included a solid commander's intent and a broad scheme of maneuver for our assigned forces that was easily understandable by the command, our partners inside DOD and across the U.S. Government, our industry and academic partners, and our nation's allies and security partners around the world.

I have this discussion all the time with fellow leaders across DOD. This is the one mission set where literally if we have given you access to a keyboard, you now are operating in this domain, and that represents both a potential advantage and quite frankly a potential threat or vulnerability. It is the nature of communications and the flow of information. Cyber and the network are such foundational features that they are inculcated in almost every aspect of our personal and professional lives. Because of this, one of the points I try to make is that our effort has to be so much broader than just the dedicated cyber mission force that USCYBERCOM is focused on building and then employing. Because every single individual with keyboard access is a particular point of vulnerability, we've all got to realize that we're all part of the solution. This isn't a case of "This isn't something I have to worry about. This is for USCYBERCOM to do," or "This is something my chief information officer is going to do." Experience certainly teaches those of us in government, as well as in the private sector, that you can have the greatest technical configuration in the world, all of which, if you're not careful, can be undermined by the actions, choices, and behaviors of users. We've seen that with spear phishing. We've had to deal with that on a significant scale in the Defense Department.

JFQ: *You mentioned defending the Nation's vital interests in cyberspace. Can you describe in general terms how your command works that problem set, especially since most of cyberspace is not in DOD networks?*

Admiral Rogers: If you look at the USCYBERCOM Vision, one of those foundational tenets that I said is going to drive the way we approach this, that is, the scheme of maneuver and what

U.S. Air Force Airmen set up radio frequencies kit during weeklong annual exercise Vigilant Shield 15, emphasizing integrated DOD and civil response in support of national strategy of aerospace warning and control, defense support of civil authorities, and homeland defense (U.S. Air Force/Justin Wright)

commander's intent is, is that partnerships are everything in this mission set. And those partnerships can't be just within DOD. We've got to think more broadly, both across the government and more widely in the private sector. So if you look at key partners for us, they not only go to the [combatant commands], the Services, and our own subordinate commands, but they also go to other elements in the Federal Government such as the FBI and DHS. They go to private industry. I remind people that we're an organization that applies technology to attempt to defeat technology and attempts to use technology against us.

Much of that technology is developed in the private sector. It didn't come from the government. It's not something that DOD developed. So our ability to partner with the private sector is really important for us. It's why, for example, DOD created the Defense Innovation Unit–Experimental [DIUx] construct in Silicon Valley. It's why USCYBERCOM has structured and created a similar effort aligned with DIUx but slightly apart from it in what we call "the point of partnership." We decided this was a worthwhile endeavor when we asked ourselves, "How can we build on DOD presence in Silicon Valley in the form, for example, of Reservists who are working there in the tech sector, and could we use that example as an initial proof of concept?" If we make it work, then there are a lot of other pockets of really high-tech activity, technological expertise, and industrial capacity that we could partner with. For example, Austin, the Triangle, Boston, and you could make a case for the DC-Metro area, particularly Northern Virginia. There's a pretty good technology slice out toward Washington Dulles International Airport where we could find partners.

JFQ: *As your command works on turning strategy and plans into operational outcomes, what are some of the challenges of becoming effective at the operational level of cyberspace?*

Admiral Rogers: Our number one priority is the defensive mission. The challenge for us on the defensive side is trying to overcome decades of investment in which redundancy, resiliency, and defensibility were never core design characteristics. When we built the networks that we take for granted today, to include the majority of our weapons systems, it was about efficiency, effectiveness, cost, and operator ease of usage. It wasn't, "We've got nation-states, groups, and individuals attempting to penetrate these systems on a regular basis and we've got to build a system that makes that tough." It was not a core design characteristic. It was a different world then. But we're living in a world now in which much of the infrastructure that we take for granted, that we use everyday to execute our operations around the world, was built around a different environment and a different set of premises. Our challenge now is to overlay defensive capabilities on those structures even as we work to change them from the ground up. We're trying to defend a set of networks and a set of weapons systems and their capabilities in which defensibility was never built in. The system just isn't as efficient, and it doesn't scale well.

There is also the question of how to educate a workforce. Again, when every individual becomes an operator in this environment, we're often only as strong as our weakest link in the interconnected digital world of the network and our weapons systems. When operators don't make smart choices, you start to have significant operational impact, and we have already experienced that across DOD concerning recent spear phishing issues. Frankly, when I talked to the individuals who had clicked on the links, I asked, "Could you give me a sense of why you opened this attachment?" These were not junior, inexperienced people, mind you. And they said to me, "Sir, it was early in the morning and I had my head down and I'm blowing through my emails and I've got to keep moving. I've got to get ready for my first meeting." You can have the greatest system in the world, but it's fundamentally undermined by an attitude of "I'm in a hurry; I don't have time." In the world we're living in now, do our personnel really believe we can operate as a Department if the premise is, "I only have time for this under certain conditions"? And it isn't that they're bad people. I don't mean to imply that for one minute. But we need to embrace a whole different thought process.

We have created a culture in DOD where we literally give probably a million people a weapon in some form, and yet we've taught them, "This is something we've given you for a specific purpose and it should be used in a very controlled manner under very specific circumstances, and here are things we will not tolerate." For example, we all know that the accidental discharge of a weapon is an offense punishable by a court-martial. DOD culture teaches us that you use the weapon you've been given for a specific set of purposes within a lawful framework and a specific set of authorities. You don't take that weapon and just decide, "It's late at night, I'm on the post, it's dark and cold, I'm in the eighth hour of a 12-hour watch, and I'm just tired and bored. Hey! Let's do a little quick draw." We don't do that because no one wants to shoot someone accidentally or be shot by the person involved in this quick-draw scenario. We also know that, culturally, it's not tolerated, it's unacceptable and unprofessional, and you will be held accountable. We've got to, over time, do the exact same thing at USCYBERCOM. You can affect a significantly large number of people and potentially cost the government significant money just by not paying attention.

JFQ: *One of the challenges any joint command has is how to work in support of the joint force objectives. How will you at USCYBERCOM work to this end of working with the joint force?*

Admiral Rogers: I think that's one of the main strengths of the current construct, and I say this as someone who has worked this from a Service perspective regarding generating capability to provide to a joint commander to employ. When we first approached cyber in DOD, we were certain that the operational capacity of this capability needed to be done within a broader joint framework. We said from the beginning—even with this new mission set—that we've got to build it that way from the ground up. We brought in the Services, and it was a combination of the Services and the joint world that wanted to mandate a joint training set of requirements so that every Service is generating capacity to the same standard. We needed to build a common scheme of maneuver across the Department so that every Service is generating teams to a single blueprint. That's proved to be very powerful because it gives us maximum flexibility and because it makes us much more efficient with resources. We build to one standard and one model across the entire Department.

In addition, we also needed a total force solution regarding how to do this. That solution has to involve the Active Component, the National Guard, the Reserves, and a civilian role. To maximize effectiveness, we needed to bring together all of those key parties to the fight. The answer can't be all civilians or all contractors or that we'll simply make it a Title 10 act of force so that we don't need the Guard or Reserves. During these discussions—I was in a different role then and more junior—we asked, "How do we look at this as a more integrated enterprise across the Department and do it from the very beginning, not as an afterthought?" The total force package allows us to achieve a greater range of expertise and capability than we would if we just sub-optimized any particular element.

JFQ: *What effort is your command undertaking to get your stated goal of full-spectrum capability and capability development?*

Admiral Rogers: We're building capacity in terms of the teams. The Cyber Mission Force is approximately 6,200 people and 133 teams, and each team has a specific mission. There are three different types of teams, aligned along those three different missions we talked about initially. We've tried to optimize the teams, their people, and their tools by the mission we've assigned to them. Again, it's not aligned with the way we do things with the rest of the mission sets within the Department. We're generating a cyber mission force capability mission. We've identified the tools and capabilities, and we continue to get more insights as we actually use the force. For example, what are the additional enabling capabilities and tools they need? Experience is helping us really refine the defense capabilities that offer the greatest return. If we're not careful, cyber could become a massive cost sump that consumes a huge amount of resources. We've got to be good stewards of the resources allocated to us because we're in a declining budget environment. Requirements far exceed resources across the Department as a whole, and as important as cyber is, I also remind the force that no one is going to write us a blank check.

What we owe the Nation is a prioritization of what we think we need, and how we prioritize it. If you'll remember, defensive priority number one is generating that range of options to include the offensive piece, which is the priority number two mission. We have to make sure we're aligned appropriately. We've discussed the force, the improvements we think we need to make concerning both the way our networks are configured and the way we're building them as we bring the Joint Information Environment online. We've also asked ourselves how we change culture. As much as people love to focus on technology when it comes to cyber, I remind them that in the end, this is an enterprise driven by both men and women in the workforce, and it's significantly affected by the choices that they—the operators of those keyboards I mentioned earlier—make. It's also largely driven by what they do. If we don't set an expectation, if we don't train and educate, if we don't make the workforce aware of what the implications are for our set of missions as a Department and the individual actions and choices they're making, then we are sub-optimizing, and it's like fighting with one hand tied behind your back. You can have the greatest system in the world, but if you have a workforce that continuously chooses to make bad choices in what they're doing everyday on the network, it makes the defensive problem incredibly hard. At the same time, on the acquisition side, we need to ensure that defensibility, redundancy, and resiliency are built into our networks, weapon systems, and platforms from the ground up and not treated as a capability to be bolted on afterward.

To give commanders and policymakers a greater range of options when using cyber as a tool, what are the capabilities we need to be generating? We're in the midst of working that out. When our commanders and national policymakers ask DOD for a set of options to respond to an event, we want to be able to offer them a wide range of capabilities. We're in the early stages of this journey, but we know where we need to get to.

JFQ: *Can you outline the enablers your command is likely to bring to the joint force commander to assist in meeting this joint force mission?*

Admiral Rogers: What I tell my fellow operational commanders is USCYBERCOM was created in no small part to help combatant commanders achieve their mission sets. This includes defending key cyber terrain and ensuring that their command and control and the capabilities that they count on—from their networks to their weapons systems—are fully available and ready to operate as designed in the time and place of their choosing. In addition, we want to be able to generate capabilities that meet their specific operational needs, not what I think they need. USCYBERCOM exists to help ensure the success of our fellow operational commanders. And we are focused just on one particular domain and on one particular set of tools and capabilities, just as U.S. Special Operations Command, for example, is focused on its own mission.

JFQ: *What level of success has your command had so far in support of your mission, and can you assess how far along you are toward achieving your vision?*

Admiral Rogers: I would contend first that we have to acknowledge that we are not where we want to be, both as a Department and as an organization. One of our challenges is figuratively building and flying the plane at the same time. If you look at the way we normally generate force capability as a Department—a fighter squadron, carrier strike group, a Marine Expeditionary Unit, or a BCT [Brigade Combat Team]—we generally will do the individual training, bring the individuals together as a unit, give them their equipment and their table of equipment and organization, make sure they're outfitted in accordance with their mission, and then spend a period of time training them from an early preliminary stage to where they are ready to operate in a complex, multidimensional environment. Then we deploy them or employ them. Generally, we employ them only after we've completed those preparations. We're not going to take a brand new BCT that has not even completed its training but has its initial cadre of people and, for example, deploy them to Afghanistan or Iraq. But that's the normal scenario we're using in cyber because there's such a mismatch between requirements and capabilities. Because we're still building this, as soon as we get an initial cadre we're putting the team in contact and working against opponents, while at the same time we've got to get more people to finish building out the team. We've got to finish their training. We've got to get them into exercises. We just don't have the time—we can't afford to wait. So it's a different model that is not an insignificant leadership challenge, whether you're running one of those 133 teams or you're the subunified commander trying to put it all together and generate capacity and apply it now as opposed to waiting until all the man, train, and equip work is complete. And when I say "waiting," I remind people that we made the decision to start building this dedicated cyber mission force in fiscal year 2013.

We gave ourselves between 2013 and 2016 to start to build. And our experience in cyber is no different from the more traditional domains. It takes us, depending on the skill sets, anywhere from 6 to 24 months to provide individuals with their initial cyber training, and that varies based on whatever their particular missions or skill sets are. Once we give them basic individual training, then they're ready to train as a unit. Our experience has been that it takes about 2 years. We started the first build in 2013, which meant the first operationally ready people started showing up in 2015, and it'll take us until about 2018 to finish the build so that the teams are trained and equipped and ready to fully employ. In some areas we're slightly ahead of schedule, and in others we're slightly behind.

Overall, we've probably exceeded expectations because we're creating something completely new and we don't have a model to use. I'm satisfied with where we are in generating capability and I'm pleased with our defensive focus. I think experience is giving us a sense of where to find the greatest return on investment and where we need to focus. It's not a question of not knowing what to do; it's the time needed to generate the capability and the necessary resources.

F-15E Strike Eagles participate in Red Flag 15-1, featuring aircraft from 21 different Air Force squadrons, offering realistic combat training involving air, space, and cyber forces from the United States and its allies (U.S. Air Force/Aaron J. Jenne)

It can't be done in a few years. As I said in my last testimony before the HASC [House Armed Services Committee] and SASC [Senate Armed Services Committee], we're dealing with decades of investment choices, and I can't overcome that in a couple years. It's going to take us some time. Meanwhile, we've got to be held accountable for execution of our mission set.

JFQ: *Each of the Joint Chiefs of Staff whom I've interviewed has mentioned sequestration and how difficult it is to deal with. Obviously you're a growth industry at the moment, but even in a growth industry you still have to have someone pay the bills. And if no extra money is coming in, how do you connect these two dots?*

Admiral Rogers: Look at the government shutdown in 2013. We assessed that it probably cost us 6 months in generating the Cyber Mission Force. When the government shut down we had to close all the schoolhouses, and because we didn't know how long the shutdown was going to last, we said, "We've got to let people plan here and we can't just jerk them around." We sent people home. We had people who were physically traveling to start schools and training. We had to stop exercises. That simple, short shutdown probably cost us 6 months because of the unknown. Then we had to take time to bring the schools back online. We had to rework temporary duty plans, we had to rework range access time, and we had to rework exercises. One of the points I tried to make when I testified before the HASC and the SASC last week was that a lot of people tend to focus on the technology. It's not that the technology isn't important. But I remind them that USCYBERCOM, at its heart, is an enterprise driven by dedicated men and women. That's our edge—their motivation, their commitment, and their focus on the mission. And particularly for the civilian part of the workforce, they could be making a whole lot more money in the private sector. Within this career field you don't have problems getting jobs outside of government. What has helped us is the mission and the sense of serving something bigger than yourself. You're doing something that makes a difference, something that's important to the Nation.

During the week leading up to the continuing resolution in October 2015, and with just a hint of another potential government shutdown, there was more perturbation in our workforce where people started reaching out to me, particularly on the civilian side, saying, "Sir, this would be the second time in 2 years and, quite frankly, I can't build a future for my family with this kind of uncertainty. I have a mortgage to pay. I have children in college. I have bills. And I have a dream

Harpoon missile launches from guided-missile cruiser USS *Shiloh* (CG 67) during Exercise Valiant Shield 2014, focusing on real-world proficiency in sustaining joint forces at sea, in air, on land, and in cyberspace (DOD/Kevin V. Cunningham)

for what I want for my family. I can't meet these responsibilities if I'm working in an environment where, just on a casual whim, politicians say, 'Hey, we'll just shut the government down and go home. We might pay you, we might not pay you, but we're not making any promises or guarantees.'" And during a shutdown you can't legally be at work, so I don't care how motivated you are or how much you love what you do. If you show up, we have to make you go home.

Sequestration is hard for us to overcome. It really demoralizes the workforce, both civilian and military, who ask, "Is this something I want to build my professional life around?" I tried to tell our congressional oversight organizations, "This is where you can really make a difference for us: mature, steady funding at a level you determine. There's a cost to sequestration, and the perturbation has a human dimension to it."

JFQ: *You're a graduate of the National War College at the National Defense University* [NDU]. *How has your joint education experience had an impact on your leadership approach, especially as you mentor your workforce?*

Admiral Rogers: I've always been a firm believer that education never stops. Learning never stops. It doesn't matter how senior you are. It doesn't matter if you're enlisted, officer, civilian. Learning is a lifelong commitment. Education is an important part, and it's a very important part of that learning dynamic. Each of us has to commit to the fact that the U.S. Government, the military, and the Services aren't necessarily going to teach us everything we need to know. As professionals, each of us has to invest in ourselves and with our own time in the quest to learn. It drives what you read. It drives how you spend your time. Do you go to symposiums? Do you go to conferences? It's all part of professional development and it's something I always thought was important. I loved my time at NDU. I had just made O-6 when I was at the National War College. It gave me a chance coming off sea duty to step back and think. I went from there to the Pentagon, where I was exposed at a much more strategic and broader level to policy, resources, and operational topics that, frankly, I didn't have to worry about when I was a tactically oriented person, which was what drew me into the military in the first place. It's why I wanted to join the Navy. Being at sea is what I love.

I remind people that education doesn't necessarily give you all the answers, but it teaches you how to think about generating answers. It gives you a frame of reference. And it reminds me that even as we often think that right now we're dealing with the toughest issues, the one thing that's been truly constant is the nature of man—the way people respond to challenges, the insertion of new technologies into societies. Do you think it's a new phenomenon? I don't think so. There's great insight to be gained by studying how societies and militaries have dealt with both the injection and the development of game-changing technologies before. How did these changes affect them? What kinds of choices did they make? What did nation-states, groups, and other actors do in response?

I've just had my 34th commissioned anniversary and I think I have—more so than many—11 or 12 years of joint time. I loved my joint time. Don't get me wrong. The knowledge and insight I learned from a Service perspective about what it means to be a Sailor and about what it means to be a maritime professional are foundational for me, and the joint world allowed me to build on that and to apply it in a broader context. But that joint time also helped me learn about the things the other partners bring to the table. How can you maximize all those capabilities to achieve the broader mission? That's really been the power of the joint side. I've got great pride in my Service and I am proud to call myself a Sailor. But I also love the fact that I've met some amazing men and women in the Army, Marine Corps, Air Force, and Coast Guard who make you say, "I'm glad we're on the same team. You guys are really good at what you do."

JFQ: *Is there anything else you'd like to discuss that we haven't already talked about?*

Admiral Rogers: One thing that I find heartening is that I've been in command 18 months (I've been working in cyber off and on in the Department for about 10 years), and I have not run into a scenario yet where we didn't have the level

Exercise Cyber Guard 2015 includes joint Service and civilian personnel performing operational and interagency coordination as well as tactical-level operations to protect, prevent, mitigate, and recover from cyberspace incidents (DOD/Marvin Lynchard)

of expertise that we needed within the organization. Sometimes we didn't have enough of it—it would be one or two people—but we're building from a really good place, and I love watching the ingenuity, agility, and innovation that the men and women accomplish here. Every time we go into contact with these opponents, we learn and we change. What we're doing now is different from what we were doing a year ago. We are always asking ourselves, "What have we got to change? What do we have to do differently to stay ahead of these adversaries? What are their TTPs [tactics, techniques, and procedures]? Should their TTPs shape the way we structure ourselves, the way we align ourselves, the way we organize, the command and control construct we use? What are the tools and the capabilities we need?" This professional environment has such a dynamic, constantly changing, agile, and innovative mission set.

USCYBERCOM is only 5 years old. Because we don't have the history and we're building the formal structure from scratch, we get a little more flexibility. We have a lot more options. When I started in cyber in the Department 10 years ago, my takeaway was that this was so fundamentally different it was going to require developing a different lexicon, different terminologies, fundamentally different approaches, and a different organizational construct. For example, I was really concerned at the time about how to develop a workforce to execute the mission set within the normal structure we use in the Department, where it's shaped like a pyramid. That is, it's up or out. You tend not to do the same thing for years at a time. This is particularly true for officers—we want to broaden you; we want to give you a greater set of experiences. So my concern with that "pyramid" was, "Is that really fundamentally compatible with what we think we need in cyber?" As I look back on it 10 years later, I've come to the conclusion that cyber is an operational domain in which we do many evolutions that are similar to what our counterparts do in the other domains. For example, we do maneuver, reconnaissance, fires, and defend key terrain. We need to maximize in cyber the utility of a common joint terminology, a lexicon, and command and control structures such as those that DOD uses to execute missions across the other domains. That will help us assimilate a much broader workforce. If we treat this as something so specialized and so different that only a handful of people truly understand, we'll never get to where we need to be. We need to broaden this. We need to make sure people have a broad understanding of it, even if you're not involved day to day in this specific mission set. **JFQ**