Chief of Naval Operations
Adm. Gary Roughead
Remarks Delivered at CSIS: "Information Dominance: The Navy's initiative to maintain the competitive advantage in the Information Age"
October 1, 2009

Well, I think that as Mareen [Mareen Leed] alluded to the places I grew up have properly prepared me for my life in Washington, so I'm in good company there. But it really is a pleasure to be here with you and of course as Mareen mentioned I have Vice Adm. Jack Dorsett, who is our Director of Naval Intelligence and who figures very prominently into the moves that we are making within the Navy, within my headquarters, but within the Navy structure writ large and our approach into the wonderful world of cyber.

As Mareen also mentioned, that embracing in the international life, next week, we will be hosting as we do every two years, the International Seapower Symposium in Newport, Rhode Island. Four years ago, we had 76 countries there. Next week, 106 countries will assemble in Newport, Rhode Island with what we believe, 100 chiefs of maritime service to be there. So that is a pretty significant event for us. But the reason I mention it is, because in preparation for it, I was looking back at a speech that was written for one of my predecessors for the first International Seapower Symposium in 1969, a speech written for Adm. Arleigh Burke. And I was really struck that I could take that text and deliver that speech next week and it would be dead on target. And so I think it makes a lot of sense to me, to come here to talk about the future in a place that is so tied to Adm. Arleigh Burke because he was one of the co-founders [of CSIS], so it's just kind of a connection that I've enjoyed.

I would like to take this opportunity, as I've said, to talk about what I think are some rather significant moves we're making within the Navy to better man, train and equip the United States Navy for the fight that we're in and for the challenges that we're likely to face in the future.

I came into my current position having spent the past few years with the operational forces of the United States Navy in the Atlantic and in the Pacific, in joint positions and in Navy positions and it was in that period of time that I had a wonderful vantage point on the uses of information, particularly in an operational sense. How we gathered it, how we processed it, how we managed it, how we exchanged it, and most importantly how we then tried to use it.

I also have had the insight recently of being able to make several trips to Iraq and Afghanistan to see how particularly, in the area of special operations, that we have been able to fuse information and intelligence into operations in ways that we have never been able to do before. And in ways that have made our forces there extraordinarily more effective where we can use the power of the networks to get the information, the right

information, to the right person at the right time to be able to do the right thing. And even though we have been moving along these last couple of years, I don't think that we in the Navy have gone far enough. And, it became clear to me and this idea really has been germinating now for about three years that we really needed to transform our strategic concepts, the institutions, the organizations, the capabilities and the processes, and I think possibly most importantly our culture. If we as a Navy are to remain dominant in this information age, this cyber age, or whatever moniker you choose to put on, I think that we have to take advantage of the new opportunities that exist such as the vast stores of collected data. Information and intelligence that often lie at rest, unrecoverable, unavailable and untapped. To take advantage of the ability to filter, to analyze and then disseminate that information and to leak that information, the appropriate information to either kinetic or other decisive effects in real time. To take the opportunity to communicate more broadly with people and with more people, and also in that exchange of information to better understand the cultures with which we will operate and to take the opportunity to share that information in ways that we can foster relationships and build the capacity of other militaries and particularly in our case, other navies, that may not be at the same place where we are. And to be able to do that in a way that we're not constrained by the barriers that often fall into the path, either because of security issues or policy issues, and I think that it has been reflected that there is great power in that latter piece with the work that we have been able to do in a very short period of time in areas such as maritime domain awareness and how we exchange that information with other partners, with other navies, with other countries that can contribute and foster increases in defense capabilities and security capabilities.

There is no question that as we move off into this area, that there are vulnerabilities associated with it. One of the vulnerabilities is our dependency- that the Navy does require unfettered access, unlimited access to assure communication and capabilities in cyberspace. We need that to operate. The vulnerability too, that cyber in and of itself is of outer space. You know, first we learned how to fight on land and then we went to the seas and then the skies. And now we are going to be fighting in this newer domain and we are fighting in this newer domain. In the business of ships and aircraft, submarines, I think that there exists between the United States and other navies around the world, I'm quite comfortable with the capability gaps that we have in those areas of ships, submarines and airplanes. But in cyberspace, that is a much more contested space and the question for me has been, 'do we enjoy that same capability gap there?' And we must be prepared to operate in cyberspace when it's denied and then we must be able to also deny space when it's required or when it's appropriate.

And the other vulnerability is the speed of action and response. We can make pretty quick decisions in combat today, but I believe the pace is only going to get faster and faster and faster. And as I've looked at this, it also was apparent to me that cyber is going to be particularly challenging for us because the nature of the cyber domain is pretty unique in many ways. I'd say the first is called the low bar of entry. You don't have to travel or pay to have great technology to enter into this battle space. So it's a pretty low entry fee to get into.

The second is that speed, and I touched on speed earlier, but speed in cyberspace takes on a new meaning. We used to be able to think in terms of speed of weapons and how fast they were and we could talk in minutes and then it became seconds. But as someone pointed out to me, in cyberspace when you can do a Google search that can scour the web and come back with 309 million results for the word "Google" in one tenth of a second, that speed is almost incomprehensible, if not incomprehensible.

And that also we are going to be in a domain that in ways is self-governing.
The internet grew on its own out of a need to share information among U.S. government labs and it has been growing and morphing ever since.

And then the fourth being that cyber is going to be a pervasive, a persistent and an adaptive domain. People are always in it. They are never absent from it, so there is always someone in that space all the time. And, it affects our lives in some pretty extraordinary ways. And it is going to constantly be adaptive and because of that adaptation, there is a reason I think why Microsoft has had to go to "Patch Tuesdays" instead of a "Patch a month." So these are some of the challenges that I think are with us and in a way shaped my thinking as we move forward.

But I would also say that the United States Navy has been no stranger to the world of networks and information and clearly as a service that relies heavily on technology, we have always had the challenge of communicating over long distances. From the first time we started going to sea and to show that I'm not exactly that far forward a thinker when it comes to cyber, one of my favorite quotes, I'll also go back to Adm. Arleigh Burke when he said, "going to sea used to be fun and then they gave us radios."

Some things haven't changed as I've said. But in a way, the Navy was the first to move to network operations. In fact, the first course that I attended as an ensign in the United States Navy on my way to my first ship was a course in the Naval Tactical Data System, NTDS. So even from my earliest days, we have been involved in networks and the sharing of information in an electronic medium.

We have been operating with integrated sensors and networks that bridge information and operations between our ships, our airplanes, our submarines and now our unmanned systems, guided missiles, satellites, facilities ashore and our computer networks.

In the time that we have done business in these domains, we have developed important relationships with other institutions. Organizations like DSLC, NSA [Defense Security Learning Center, National Security Agency], and that too has kind of shaped who we are, how we think and how we do business. And we as a Navy have also had some pretty proficient operators. And we have instituted some fairly top-notch schools in the area of cyber operations and cryptology. Adm. Grace Hopper, one of our earliest luminaries, is someone who is somewhat reigned in this. We in the Navy were designated the executive agent for Joint Cyber Warfare in 1999 and we established the Joint Schoolhouse in 2001. And then in 2004, we stood up the Cryptologic Technician Network rating, specifically focused on cyber operations. And outside of cyber a very important dominance the Navy

has, I would say, the lead in intelligence, communication, information operations and oceanography professionals within our cadre- officer and enlisted.

And I believe that all of these efforts for the last decade have positioned us to lead in cyber in a way that the nation would expect.

So, while we are well-positioned, and we have experience and we have talent, I'm not sure we have taken enough of a bold or comprehensive approach in one that can really leverage the world of cyber in our operations to ensure that we have the access and to enable better decision making on the part of our operators.

And this is why I directed the reorganization of my staff and made three, what I consider to be important moves for the Navy.

The first is on my staff to combine the Director of Intelligence and the Director for C4I into one entity. Into now, instead of an N2 and an N6, it will become an N2/6 or the Director for Information Dominance. The legacy platform-centric approach that has been a part of our Navy for so many years, the ships, the submarines, the airplanes, I believe, is a way of the past. Those artificial divisions and some cases they have been not too artificial, particularly as you get into budgetary issues, have really caused us to sub-optimize our ability to aggregate combat capability and the movement of information in ways that can maximize the effectiveness of the fleet, of the unit for the individual. So we are bringing together the resource sponsorship for all of our information-related capabilities into one entity and that will include intelligence, networks, electronic warfare, cyber, meteorology and oceanography, space and unmanned systems. They will all be resourced in one organization and we will manage those capabilities collectively and ballistically to achieve information dominance for the Navy and for joint inter-agency partners. The reorganization is moving quickly, as it should, and will be complete by the end of this year and N2/6, or the Director of Information Dominance, will be the one making the major investment decisions as we compare our 2012 budgets. Someone asked me this morning, 'where are you along this timeline?' and I think the quote from Hernando Cortes applies, "we burn boats, there's no going back." So Jack [Vice Adm. Jack Dorsett], you're the helmsman.

We are also establishing a Fleet Cyber Command. It will be the service component to U.S. Cyber Command at Fort Meade. It will be dual-hatted as the Commander, Fleet Cyber Command, and Commander, Tenth Fleet. It's a similar model, organizationally and functionally as we have with NAVCENT and Fifth Fleet. So one entity, but basically two functions that will enable Fleet Cyber Command to execute the operational missions required by U.S. Cyber Command and by the Navy. I'm often asked, 'why Tenth Fleet?' It has some historical roots. There was a Tenth Fleet in the United States Navy at one time. In WWII, there was a new threat that came on to the scene that was strangling Great Britain and seriously affecting our ability to control the seas. That threat was called a submarine. We couldn't get our head around how to get after these submarines. We had some information, so intelligence in the operations, so Adm. Ernest King stood up Tenth

Fleet and we were able to overcome the submarine threat that existed at that time. So Tenth Fleet will be reactivated as Cyber Fleet.

While N2/6 will focus on the investments that will ensure our dominance, Fleet Cyber Command will focus on the operations. Fleet Cyber Command will be the cyber operator for the Navy. I think as in all things for me, the most important element in any organization is the people. And that I think is the most important change that we are going to make.

The technology I believe is going to be available to us. But people who will operate in this domain will be at a premium because there will be great competition for their intellect, for their experience and for their competence. So people are going to be the key. So what we have done is to take our already very proficient and experienced operators and create with them and with others an "Information Dominance Corps." Right now we have a lot of ratings, a lot of specialties within the Navy that in and of themselves are a bunch of different communities, a bunch of different structures if you will. And we will combine them into an Information Dominance Corps- it will include our Information Professionals, Information Warfare, Intelligence, Cryptology, Aerographer's mates, IT [Information Systems Technicians] Professionals- they will all be combined into an Information Dominance Corps. And when you add that together, it will constitute about 44,000 Sailors in the United States Navy. They will retain their individual identities, but they will be managed as a corps, they will develop as a corps and they will fight as a corps.

So the goal in doing this is to ensure the commander gets the right information to the right place at the right time so that they can effectively perceive, understand, reason, decide and as the culture of the Navy, command. That's what all of this is about. These are important changes that I believe we needed to make, that we now have made to realize a more effective operational environment for the Navy. So I'm pleased that we are underway, and as I've said, this is where we are headed. And with that, I will take any questions that you may have. Thank you.