OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE

Remarks by Mr. David R. Shedd
Deputy Director of National Intelligence for Policy, Plans and Requirements

Air Force Association Space and Cyberspace Warfare Symposium

Keystone Resort, CO

June 9, 2010

AS PREPARED FOR DELIVERY

Why is the head Policy wonk from the Intelligence Community here talking about space and cyberspace? Why does the Intelligence Community care and what is our stake? What can he possibly tell us that we don't already deal with every day? So that's my challenge today. And hopefully, upon meeting that challenge, I can challenge you as well.

Let's start with space. There is much discussion in Washington right now about space, how space fits into our national priorities, and what our role as a nation should be regarding space. The terms space domain, Global Commons, space AOR, and space mission area are being weighed as we continue to work on a new National Space Policy. But to boil things down to what matters to the Intelligence Community, to what matters for intelligence *collection*, space is a place. Not a domain, not a mission, not an AOR—we don't think of it as a Global Commons. It may well be all of those, but for intelligence purposes space has been a relatively quiet, dark place from which to collect information. We collect information from areas denied to us from other means. We collect information on a global scale. We are often the first source of information after a natural disaster when roads are destroyed and telephones don't work, and we can be anywhere on a moment's notice to support our warfighters and peacemakers with battlefield information and verification of treaty compliance.

What better place to be to collect secrets than a quiet, dark place? We went to space on the words of Dwight Eisenhower who declared that "Nobody wants another Pearl Harbor." Our mission has been to keep a watchful eye on the developments across the globe and help our nation avoid surprises. But over time the space environment has changed, and just as we have found great benefit in being there, others have sought the same advantage. Still others recognize our substantial reliance on being in space and are actively developing the means to deny us that advantage should it meet their objectives to do so.

We no longer hear the term sanctuary applied to space. Indeed, it may never truly have been that. Instead, sanctuary has been replaced with the words congested, contested, competitive, and complex. In addition to worrying about the next Pearl Harbor on Earth, we now must also consider the potential for a space Pearl Harbor.

For the past few years we have been grappling with the same questions as the military: How will we know if a space asset has been attacked? Is it feasible to protect spacecraft? What is up there with us and what is it up to? Thankfully, the Intelligence Community and the Department of Defense are cooperating on several joint initiatives to derive answers to these questions. Most of these initiatives focus on the improvement of Space Situational Awareness. The cooperation here involves primarily the sharing and integration of information from DoD's space tracking and space weather sensors and the IC's foundational intelligence on potential threats.

So principally, our interest in space from an Intelligence Community perspective is staying there, understanding what is going on around us, and continuing to accomplish our collection mission. When we boil it down, not so different, I suspect, than the military interests.

As I mentioned earlier the Administration continues to work on a National Space Policy; concurrently the Office of the Director of National Intelligence is also working with the Office of the Secretary of Defense on a National Security Space Strategy which will put some texture to the broad guidance of the national policy. As a nation we have made the assertion in our policies that we consider attacks on our space assets an infringement on our rights. In the strategy we will consider both how to deter and dissuade such attacks and what options to offer the President in the case where our best deterrence and dissuasion fails.

And on that happy note I will turn to cyberspace and my remarks will sound nearly redundant. One big difference is that I am not aware that cyberspace was ever considered a sanctuary. From its earliest days cyberspace has been recognized as a congested, contested, competitive, and complex environment. And that situation has grown exponentially worse in recent years. The news is filled with all manner of stories about the challenges we all face in trying to secure our networks.

The Intelligence Community's interests in cyberspace can be coarsely sifted into two piles: cyber security and cyber exploitation, or protecting what we have and taking advantage of the other guys' failure to do so. And, like space, there is the same attempt to define cyberspace a global commons, a mission area or an AOR. Here again, for the IC at least, cyberspace is a place from which to extract information and through which to move and share that information.

There are some incredible things going on in the Intelligence Community regarding information extraction from cyberspace, the details of which I cannot discuss at this symposium. I will, however, spend some time on the cyber security activities that we along with several other federal agencies are engaged in, especially in response to Presidential direction.

The Director of the CIA, Leon Panetta, recently described cyber security as the "confluence of two major mission areas…counterterrorism and counterintelligence." Staying "one step ahead of our adversaries" is the challenge, he said. To that end, President Obama has identified cyber security as one of the most serious economic and national security challenges we face as a nation and has accepted the recommendations of a Cyberspace Policy Review that range from conducting basic cyber security awareness initiatives, to innovation and technology solutions, to unity of effort across federal state and local governments in responding to cyber incidents. Implementing these recommendations has become the primary responsibility of the Comprehensive National

Cybersecurity Initiative or CNCI. The Office of the Director of National Intelligence is actively engaged in that initiative.

Understanding what is going on around and potentially inside our networks is a key component of cyberspace security. Just as space situational awareness informs our operations in space, we need that awareness in cyberspace to assess, defend, and continue the operation of our networks. So there are numerous analogous aspects of space and cyberspace. Both have global reach. Both are now essential to our way of life. Both are incredibly fragile and subject to ongoing interruption.

It's not hard to draw the corollaries then between intelligence and defense interests in space and cyberspace. As an audience principally of warfighters, not intelligence analysts, allow me to draw the connection between our communities, to highlight the key aspects of our relationship in this space and cyberspace realm, and offer some challenges where we need to close ranks and work together to solve some very daunting issues.

Consider the relationship between intelligence and warfighter as that of service provider and client. Intelligence has the task to provide indications and warning of attack; to characterize foreign capabilities; to define what needs to be defended or, in some cases, targeted; to attribute actions taken against us; and to assess the effectiveness of actions we chose to take. At the same time we must assess the threat to our space systems and cyberspace networks and take appropriate steps to protect them while still providing at least basic, core services.

And the warfighter maintains space and cyberspace assets as well, and they also must be protected. And while there is general acceptance that space and cyberspace are thoroughly inter-related; our treatment of them as distinct elements causes us to over-look that inter-relationship. In fact, this past month the Air Force Space Command's Schriever wargame series combined cyberspace and space in their scenario. At the opening of the game General Kaehler noted that "A battle that ends in space begins in cyberspace." Another key issue from the game was the recognition that battles in either space or cyberspace with a near peer adversary have global consequences and quickly involve the US homeland. Space assets, especially intelligence surveillance and reconnaissance satellites that were degraded or destroyed over the AOR for the Schriever scenario were unable to execute other important missions. Direct TV broadcasts were jammed, bringing the fight home to Joe six-pack. Cyber attacks were targeted at Blue networks in the US. Power was lost intermittently along the eastern seaboard. I'll save the rest of the story for a later briefer, but it is important to understand that we find ourselves in much different world today than we did even five years ago. We are so interconnected and dependent on space and cyberspace that even minor disruptions can have a significant impact.

But just one more Schriever 10 observation before I leave that topic. This year the IC participation was the most robust ever. We filled an entire corner of the game floor and had liaisons moving about and among all the other cells. Like good intelligence officers we also stayed at the same hotel as the Red Team, hoping to pick up the next day's move over dinner or other social venues. And our involvement helped to bring forward several findings that are part of the IC out brief slides and will be briefed soon to the Intelligence Community leadership.

It’s those opportunities to closely interact where the warfighter and intelligence analyst have the best chance to learn from one another. Too often we meet on the battlefield and we ad lib extraordinary ways of moving and using our information. But without the imperative of contact with an enemy, we allow our communities to languish and even suspect one another’s intentions. In part, coming to Keystone and sharing my thoughts on space generally and cyberspace specifically was very important to me.

In a time of shrinking budgets that’s the natural course of things—clam up; protect what’s yours. So my first challenge to you all is to resist that reflex. Within the relative calm of the DC Beltway or beautiful Colorado, the enemy is the shrinking resources and we are surely in contact with him. So closing ranks together and defining smarter ways to operate is one challenge. Whether that is improving Space Situational Awareness through greater cooperation or defining the means for a common Cyber Situational Awareness picture, we have the opportunity and indeed the responsibility to find the economies of scale, the reinforcing mechanism of combining sensed environment with foundational intelligence.

For cyberspace in particular both the IC and Defense can draw together our limited yet shared experience to develop a common understanding of the operational environment—develop a Joint Intelligence Preparation of the Environment tailored for cyberspace. This will add credibility to our planning efforts and help dispel the myth that cyber tools are hammers looking for a nail.

Cooperating on the development of strategies to implement the broad guidance of our national policies is another area. While we may have different approaches to international engagement, in the area of national strategy development the IC and the Defense Department have been closely engaged, an example of which is the joint National Security Space Strategy. This joint activity has allowed us to identify further avenues of cooperation with continuous progress in areas where our interests may diverge.

It is here that I offer a second challenge. The Intelligence Community’s primary role is to inform policy, an area in which we need to broaden our engagement, especially in the area of declaratory policy, deterrence, dissuasion, and courses of action for both space and cyberspace. We do not have a well developed or a shared understanding of how to communicate our intentions for space or cyberspace to other nations, and to back up what we say. Unclear messages and inconsistent actions can lead to miscalculation and mistrust. Together we need to develop a clear view of what we are defending, what our thresholds are to define when those defenses have been breached and what appropriate courses of action across the spectrum of soft through hard power we can recommend to the President.

Space and now cyberspace are often compared to other global domains such as air, land, and sea. But a substantial and very important difference is that we do not have hundreds of years of trial and error, of theory put into practice to rely upon in space and cyberspace. And while the analogies sometimes work in very narrow applications, the differences are great enough that these comparisons are inadequate when applied more broadly. Without an examination of each domain or environment and its dependencies, we cannot hope to achieve sound implementation of our policy goals.

So I will leave you with those challenges. I ask you to pay close attention to the discrete findings of the war games and exercises we conduct. Look for those opportunities where we can enrich each others' understanding of the issues we face and exploit every chance to engage one another in dialog or other productive cooperation to produce an outcome that gets us closer to a solution set.

Your invitation to the ODNI policy office to speak at this forum is one such opportunity, and I applaud you for taking advantage. And while my accepting the hardship assignment of traveling to beautiful Keystone, Colorado in June may seem self-serving, I am here to learn just as all of you are. I have enjoyed the speakers that came before me this morning. My only regret is not having more time to spend here as I return to Washington to assist in the hoped for imminent confirmation of Jim Clapper as the next Director of National Intelligence.

Thank you and I welcome any questions or comments from the audience.