Space and Cyber

Shared Challenges, Shared Opportunities

Edited Remarks to the USSTRATCOM Cyber and Space Symposium

15 November 2011

Madelyn R. Creedon
Assistant Secretary of Defense for Global Strategic Affairs

I very much appreciate the opportunity to discuss the many challenges facing us in space and cyberspace and the strategies the DoD has developed and published over the course of the last year. These strategies set out a good framework to address the many space and cyber challenges. Although there are many physical and technical differences between the space and cyber domains, there are many similarities in the challenges confronting each domain, which have allowed some shared and similar approaches to addressing the problems.

Space and cyberspace are global capabilities and global enablers that together enable the United States, our partners, and allies to maintain a strategic advantage over potential adversaries and enhance our national security. These capabilities allow us to stay on the leading edge. They also enable economic growth, better standards of living, and rapid communications that foster the financial and social links indispensable in our everyday lives. These links also allow us to maintain close real-time relations with our partners. Our cyber and space capabilities are connected in very real ways, both for our war fighters and for our society as a whole.

Cyber and space capabilities are connected operationally. A bit of data from an analyst sitting at a computer may be directed through a local network, transmitted by satellite, and then received by troops in the field halfway around the world. Space capabilities supplement and enhance cyber capabilities, and vice versa. The timing function provided by GPS enables all of the base stations in a data network to stay synchronized.

And the measurements and observations collected by our weather satellites are transmitted and processed through cyberspace, enabling more precise weather forecasts as well as tactical and operational capabilities that otherwise could not be implemented. In many cases, space and cyber capabilities ride on the same infrastructure. That bit of data may ride on fiber for a while before being directed up through a satellite and back down to another terrestrial network. Our space and cyberspace capabilities are distributed, networked, and global; we must utilize and protect them accordingly.

Cyber and space capabilities are connected by common threats. Each of these depends on the electromagnetic spectrum and IT infrastructure that affords us great capabilities but also creates cross-domain vulnerabilities and challenges. An attack on our space capabilities may start in cyberspace, and attempts to hack our cyber capabilities get routed through space.

Low barriers to entry have allowed states and nonstate entities to contest our use of both space and cyberspace. "Low barriers to entry" may sound strange when applied to space capabilities, but counterspace capabilities, as we know, do not always require a space program. Increasingly, satellites are jammed by commercial equipment easily acquired by state and nonstate actors. The low barriers to entry in cyberspace allow a range of adversaries to have effective capabilities against networks and computer systems, unlike those anywhere else—here, cyber criminals, proxies for hire, and terrorists could leverage capabilities that previously only governments possessed. As former deputy secretary Bill Lynn wrote in his latest *Foreign Affairs* article, "The United States is now in the midst of a strategic shift in the cyber threat."

In both space and cyberspace, maintaining an edge is always a challenge. We know our adversaries seek advantage through industrial espionage and the theft of intellectual property, which places burdens on our industrial base. An increasingly more sophisticated international workforce is also challenging our own workforce, seeking to out-innovate and out-develop. We need to strengthen our industrial base through better, more advanced acquisition and export control processes, and remove the outdated restrictions that hamper our industrial base today. In space and cyber, attracting the next generation and retaining the current generation of skilled professionals will continue to be a challenge.

Space and cyberspace are connected in how we have organized ourselves. My office—the Office of the Assistant Secretary of Defense for

Global Strategic Affairs—develops policy on cyber and space issues, along with other global issues, including countering weapons of mass destruction, nuclear forces, and missile defense. Similar responsibilities are found at STRATCOM, executed by the men and women who are the leaders in strategic deterrence and the preeminent global war fighters in space and cyberspace. We are not the only ones, however, who have seen the benefit of organizationally integrating space and cyberspace. Many of my international counterparts on space issues are also my counterparts on cyber issues. This similar organizational integration, while fairly new, will over time, I hope, ensure that both domains are more effective, more resilient, and more coordinated with our international partners.

Not all of the challenges for the space domain are equally difficult for cyber, and the reverse is, of course, true. The two developed differently and at different times. Fifty years ago, space was largely the private preserve of the United States and the Soviet Union. Over time this changed, and today over 60 countries or government consortia operate satellites, and the number of commercial satellite owner/operators continues to increase. Cyberspace moved out of the realm of government control much more quickly than space, as many people both inside and outside governments appreciated the advantages provided by networked systems. Very quickly, the development of cyberspace became characterized by openness and interoperability. We have watched these technologies revolutionize our economy and transform our daily lives, but we have also watched offline challenges move online. Of course, the different physics and technical realities of space and cyberspace result in somewhat different threats. But despite the differences in our use of space and cyberspace, there are many similarities in the challenges.

In the face of these shared and similar challenges, we have developed similar approaches to protecting the strategic advantages enabled by space and cyberspace, as well as protecting the industrial base and the domains themselves. Since last year's separate cyber and space symposia, the DoD has completed the *National Security Space Strategy*—co-signed by the director of national intelligence—and the *Department of Defense Strategy for Operating in Cyberspace*. Both of these strategies start by acknowledging that we are in new territory from a threat perspective. Although we have much more experience operating in space, the threats have evolved fairly rapidly over the past few years and changed dramatically. The Chinese antisatellite test in 2007 was a turning point for space. Today in cyber-

space, we have the opportunity to take actions now to ensure that we can rely on this domain into the future, taking full advantage of the competitive advantage it provides. As it happens, both of these strategies have five strategic approaches or initiatives for addressing these challenges.

Both strategies acknowledge the importance of international partnerships. These partnerships allow us to maximize our scarce resources, mitigate risks, and utilize each partner's core strengths. International cooperation is also important to increase situational awareness in both space and cyberspace so we can understand and differentiate between a man-made disruption and a natural or technical anomaly. Partnering strengthens all of us. And as Gen Bob Kehler, STRATCOM commander, said in May, "We want to work to develop means of collective self-defense in space and [in] cyberspace."

The interoperable nature of cyberspace means that an important part of our international cooperation is sharing the necessary knowledge, training, and other resources with our partners and allies to build technical and cyber security capacity. In the space domain, we seek to expand mutually beneficial agreements with key partners to utilize existing and planned capabilities that make us all stronger and more resilient. Ultimately, international cooperation is vital to maintaining and enhancing the advantages we derive from space and cyberspace. No single state or organization can maintain effective cyber defenses on its own; international collaboration is necessary to address the increasingly congested, contested, and competitive nature of space.

An important part of this international collaboration is emphasizing norms and guidelines for space and cyberspace. Both space and cyberspace strategies emphasize the need to encourage responsible behavior in their respective realms. Practices that promote the responsible, peaceful, and safe use of space will help ensure a space environment that is stable, safe, secure, and sustainable. Moreover, the development and promotion of international cyberspace norms and principles will promote openness, interoperability, security, and reliability. In both areas, government and private-sector actors have an important role to play. And in both areas, there are things that the international community generally agrees are bad, like botnets and space debris. Together, we can work to address these common threats.

Situational awareness is the foundation necessary to maintain and enhance our space and cyber capabilities. Both hostile actions and adverse,

but natural or unintentional, conditions can impact our ability to use space and cyber capabilities. As the tools and techniques developed by cyber criminals continue to become more sophisticated, we must likewise continue to develop our ability to detect and respond to these threats and intrusions while increasing the cost to the attacker. Similarly, our ability to track objects in space and monitor our spacecraft is absolutely vital. We must develop and enhance our capabilities to identify indications and warnings of hostile actions in space, to rapidly warn of these activities to key decision makers, and be able to verify and attribute hostile actions to enable appropriate mitigation measures or response. Space and cyber situational awareness are essential to reducing mishaps, misperceptions, and mistrust.

Both of the DoD strategies recognize that even as we promote responsible behavior and enhance international partnerships, we must also prepare to operate in a degraded environment should deterrence fail. Resilience is a key concept in both strategies; we must ensure that the functions necessary for mission success endure in spite of hostile action or adverse conditions. Resilience can be enhanced through cross-domain solutions or alternative government, commercial, or international capabilities. Both strategies make it clear that if our capabilities in either area are attacked, we reserve the right to respond at the time and place of our choosing and not necessarily through the domain that was attacked.

Both strategies also address challenges to our industrial base and propose new ways of working with industry to meet these challenges. The strategies start with the need to encourage development of a future workforce by attracting students to the science, technology, engineering, and math (STEM) fields and then ensuring that they continue in relevant careers. These careers can be in the military, as government civilians, in defense and other industries, as well as the scientific and academic communities, as all are needed to ensure a strong future. As Secretary Panetta recently said, "Over the past two decades, our military has made particularly striking advances in precision-guided weapons, unmanned systems, cyber and space technologies—but our advantages here could erode unless we maintain a robust industrial and science and technology base. If we lose that base, it will impact on our ability to maintain a strong national defense—it's that simple." The DoD needs to maintain a strong, capable industrial base that is robust, competitive, flexible, and healthy. We can do this through improved acquisition practices that take advantage of

the creativity of the private sector and harness the power of emerging concepts.

The technologies may be different, but our approaches to space and cyberspace are often similar. We cannot artificially divide the two. Although some details vary, and some difficulties for one may never challenge the other, I urge you to think about how these two domains interact and complement each other and how our efforts can do the same. Both our space and cyberspace strategies note that capabilities in the respective domains have greatly enhanced our national security. Both also note that those benefits go well beyond national security and that the United States is not alone in benefiting. The *National Security Strategy* states, "Neither government nor the private sector nor individual citizens can meet this challenge alone—we will expand the ways we work together." That was written in reference to securing cyberspace, but I believe it applies to space as well and to the intersection between the two. I challenge you to help identify those tough questions, like cross-domain deterrence, and explore how the similarities between space and cyberspace can and should inform our policies.

Madelyn R. Creedon
Assistant Secretary of Defense
Global Strategic Affairs