

# U.S. SPACE COMMAND: Warfighters Supporting Warfighters in the 21st Century

Lieutenant General Edward G. Anderson III, U.S. Army

**F**UTURE HISTORIANS will know the 21st century as the century of “space and information.” The U.S. Space Command (USSPACECOM) is the Department of Defense’s (DOD’s) key player in charting our nation’s course in space and information.

Furthermore, USSPACECOM is the single point of contact for all military space operations. In the Unified Command Plan, the President of the United States directs USSPACECOM to advocate space operations and missile warning requirements for all commanders in chief (CINCs). USSPACECOM conducts space operations in the mission areas of space support, force enhancement, space control, and force application. It also plans for and develops requirements for strategic and tactical ballistic missile defense. Most recently, USSPACECOM was identified as the military lead agency for DOD’s computer network operations (CNO) mission.

Ten years after the Gulf War, the huge advantage space brings to warfighting is apparent. Space provides time-critical information to frontline commanders. Space operations were crucial to success during air operations over Serbia. As a result, space-based capabilities have become an integral part of U.S. military operations. Similarly, the United States must protect its critical information infrastructure to assure information superiority as well as develop appropriate strategies to exploit the vulnerabilities of our adversaries’ space and computer network capabilities.

## **The Importance of Space and CNO**

Space is an economic center of gravity. The domination of space by the United States and the former Soviet Union ended with the fall of the Berlin Wall. Today, the international community has more than 700 active satellites in orbit; the United States owns and operates more than 300. In all, 31 countries and

---

*USSPACECOM recently assumed the responsibility as the lead military organization for the CNO missions of Computer Network Defense (CND) and Computer Network Attack (CNA). . . . CND is USSPACECOM’s first priority to protect and defend the DII from disruption, denial, degradation, or destruction. CNA complements CND by disrupting, denying, degrading, or destroying an adversary’s information infrastructure.*

---

12 international consortiums have some form of space program. During the next 10 years, predictions are that approximately 600 to 1,100 new satellites will be launched. The world’s space industry has more than 1 million employees working in 20,000 companies and is expected to grow about 15 percent this year. In fact, entire new industries have been created around space applications. For example, the global positioning system (GPS) industry alone generated more than \$8 billion in revenues last year. Direct Broadcast Satellite (DBS) services such as Direct TV and Dish Network drove the industry revenues to unprecedented heights in 2000. DBS revenues jumped to \$31.5 billion in 2000, up from \$22.5 billion in 1999. It is clear that space has evolved into an economic center of gravity.

Space is also a military center of gravity. The United States’ ability to access and use space is a vital U.S. national interest. From precision-guided munitions using GPS to strike in any weather to early warning against enemy Scud launches, U.S. and allied commanders around the globe have recognized the importance of space in combat operations, peace operations, and training.

As the United States begins its fifth decade in space, the U.S. military realizes that space integra-

An Army Space Command soldier prints out a tactical map image downloaded from strategic satellite capability. This type of map is used to assist theater of operations commanders with the most current images as captured from the Earth's exoatmosphere.



US Army

***Hand-held GPS receivers; missile warning DSP satellites; communications and weather satellites; and reconnaissance, intelligence, surveillance, and target acquisition, were space-based capabilities essential to victory in [Desert Storm]. Since then, we have integrated these capabilities into our terrestrial warfighting forces. Space is now better integrated with air, land, and sea operations to enhance the joint and combined warfighting team.***

tion efforts have done two things. First, it has energized the information age, reduced time and space, and enabled instantaneous information. The U.S. military has leveraged this information advantage. But equally important, U.S. efforts have created a new set of weakly defended targets, which if destroyed or damaged, would drastically reduce the United States' ability to conduct diplomatic, economic, and military operations at home or abroad.

Cyberspace is another military center of gravity. Similarly, the explosive growth in information technologies has profoundly affected all sectors of modern society. The information revolution has fueled the United States' amazing economic growth, dramatically improved communications, and allowed businesses to compete more effectively than ever before. Information availability and integrity have become critical to the operational readiness of today's military forces. Nowhere is this more evident than in the U.S. military. Just like space, the United States depends on cyberspace to conduct successful military operations.

In the past, DOD relied on stovepiped systems, local area networks, and a limited number of users to protect its information. However, as DOD be-

comes more interconnected, it has created a shared-risk environment—risk assumed by one user is assumed by all users. In this shared-risk environment, the interconnected systems' security posture is only as good as the weakest system. The challenge is to maintain situational awareness and to actively defend the seams, or boundaries, that connect these systems so these interfaces do not become easily exploited.

The United States relies heavily on commercial systems and the associated telecommunications infrastructure to move information. These systems, along with unique military systems, comprise the defense information infrastructure (DII). Specifically, the DII is made up of approximately 10,000 local area computer networks and more than 2.5 million unclassified computers. The U.S. military relies on DII to move 95 percent of its communications traffic. Like space, our potential adversaries recognize the U.S. military's dependence on DII. It is not a case of defending against kinetic attacks anymore; we are now defending against "ones and zeros."

Today, we are at war. Daily, DOD identifies and records thousands of "cyberevents," some of which are determined to be attacks against computer systems and networks. These cyberevents are actions

Patriot missiles intercept an Iraqi Scud missile fired at Dhahran, Saudi Arabia, during the Gulf War.

Ministry of Defense and Aviation, Saudi Arabia



*Space is a military center of gravity. The United States' ability to access and use space is a vital U.S. national interest. From precision-guided munitions using GPS to strike in any weather to early warning against enemy Scud launches, U.S. and allied commanders around the globe have recognized the importance of space in combat operations, peace operations, and training.*

that could lead to illegal access or denial of service. Over the past several years, there has been a dramatic increase in the number of detected events. In 1994, there were 225 detected events; by 2000, there were 23,662. The U.S. Air Force, U.S. Army, and U.S. Navy recorded a combined total of 600 cyberattacks in 1999 and 715 cyberattacks in 2000 against their systems and networks.

There are two primary reasons for this increase. First, we have improved our ability to identify these events through better intrusion and detection tools, organizational reporting, network hardening, awareness, and training. Second, our adversaries have improved their ability to gain unauthorized access through better hacking tools, organization, and politics. The cyberthreat ranges from inexperienced hackers to nation states. However, nation states are the biggest concern because there is limited knowledge on the types of capabilities they are developing.

## **USSPACECOM**

Established in 1985, USSPACECOM is a relatively new organization. Its Commander in Chief (USCINCSpace) reports directly to the U.S. National Command Authorities. USCINCSpace is responsible for subordinate commands from the

three service components—Army Space Command (ARSPACE), Naval Space Command (NAVSPACECOM) and Space Air Force (SPACEAF)—as well as the Joint Information Operations Center (JIOC) and the Joint Task Force for Computer Network Operations (JTF-CNO).

Headquarters, USSPACECOM, and Cheyenne Mountain Operations Center are strategic operations centers located at Peterson Air Force Base (AFB) and Cheyenne Mountain in Colorado Springs, Colorado. ARSPACE is also located in Colorado Springs. The NAVSPACECOM is located in Dahlgren, Virginia, and our most robust organization, SPACEAF, is headquartered at Vandenberg AFB, California, with more than 11,000 people stationed around the world. Finally, the JTF-CNO is located at Arlington, Virginia, and the JIOC is located at San Antonio, Texas.

As stated earlier, the United States operates more than 300 active military, civil, and commercial satellites. These operations range from low-Earth orbit (LEO) to geosynchronous orbit (GEO). To put these various satellites into perspective, assume a basketball represents Earth. At Earth's surface, air-breathing aircraft operate in the denser portions of the atmosphere that extend out to about 20 miles



***[USSPACECOM is] the military lead agency for DOD's computer network operations (CNO) mission. . . . USCINCSpace's strategic objective is to operationalize CNO into the fifth domain of warfare separate and distinct, but fully integrate it into air, land, sea, and space across the full spectrum of conflict with the ability to leverage the computer network domain to achieve and maintain information and decision superiority for the joint force.***

above the surface. Using the basketball-sized Earth, 20 miles would be about 1/50th of an inch above the basketball. By contrast, the closest satellite orbit to Earth, LEO, ranges from about 100 miles to 500 miles in altitude. This would be about 3/16th to 1/2 inch above the basketball. Most LEO satellites, as well as the space shuttle, operate at 100 to 250 miles, and our weather satellites, such as those in the Defense Meteorological Support Program, operate at 450 miles. GPS satellites fly at medium-Earth orbit (MEO) at 11,000 miles, or about 14 inches above the basketball. At GEO, we operate the Defense Support Program (DSP) and communications satellites. That represents approximately 28 inches above the basketball model, about 22,500 miles.

### **Current Operations**

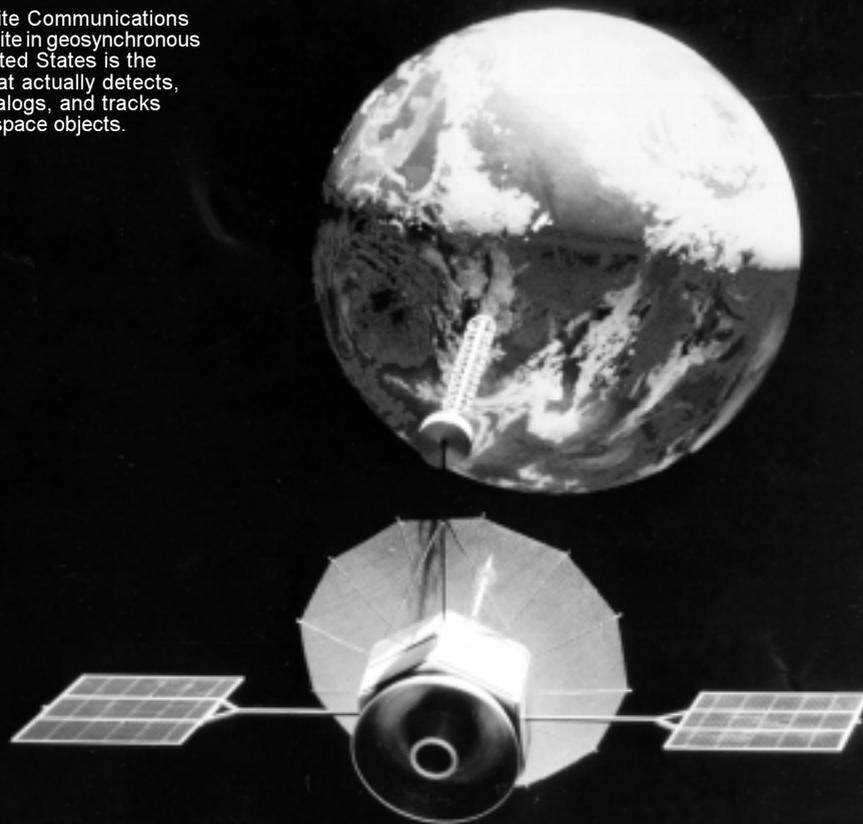
Operation Desert Storm was the first time U.S. and coalition commanders saw the largely unexploited military potential of space. Hand-held GPS receivers; missile warning DSP satellites; communications and weather satellites; and reconnaissance, intelligence, surveillance, and target acquisition were space-based capabilities essential to victory in the desert. Since then, we have integrated

these capabilities into our terrestrial warfighting forces. Space is now better integrated with air, land, and sea operations to enhance the joint and combined warfighting team.

Missile warning, both theater and strategic, continues to be USSPACECOM's top priority. It is a mature mission that grew up during the Cold War—USSPACECOM knows how to do it. Since Desert Storm, USSPACECOM has made much progress in reporting and determining the impact area. With the proliferation of theater ballistic missiles, USSPACECOM is working hard to field the Space-Based Infrared System (SBIRS) to replace our aging DSP satellites. SBIRS has improved detection capabilities that will enhance early warning and space surveillance capabilities, support future ballistic missile defense systems, and provide warfighters with better battlefield situational awareness.

GPS has truly revolutionized how U.S. and allied forces conduct warfare. It provides the necessary elements for precision strike—precise weapon location, weapon guidance, target location, and battlespace timing. The United States' current challenge is to deny its adversaries the use of these position and timing capabilities afforded by GPS dur-

A Fleet Satellite Communications Systems satellite in geosynchronous orbit. The United States is the only nation that actually detects, identifies, catalogs, and tracks all manmade space objects.



U.S. Air Force

***The United States operates more than 300 active military, civil, and commercial satellites. . . . Using a basketball-sized Earth [for comparison], 20 miles would be about 1/50th of an inch above the basketball. By contrast, the closest satellite orbit to Earth, low-Earth orbit (LEO), ranges from about 100 miles to 500 miles in altitude. This would be about 3/16th to 1/2 inch above the basketball. Most LEO satellites, as well as the space shuttle, operate at 100 to 250 miles. . . . GPS satellites fly at medium-Earth orbit at 11,000 miles, or about 14 inches above the basketball. At geosynchronous orbit, we operate the Defense Support Program and communications satellites. That represents approximately 28 inches above the basketball model, about 22,500 miles.***

ing a conflict. A future generation of GPS, GPS III, will give us new navigation warfare (NAVWAR) capabilities to shut off GPS service to a limited geographical location while providing GPS to U.S. and allied forces.

As seen during Operation Desert Storm and Operation Allied Force in Kosovo, reliable and secure satellite communications (SATCOM) systems have been and will continue to be critical to military readiness. The United States' ability to leverage commercial SATCOM to satisfy growing communications requirements is an important dimension to this mission area. Today, USSPACECOM is developing the next generation of advanced military communications satellites to meet future communications requirements of bandwidth, protection, survivability, and interoperability with a blend of military, civil, and commercial systems.

Before we can provide these critical capabilities to warfighters, we must get to space and be able to

operate once we get there. Space support is the answer—it is our assured access to space. In its launch or spacelift role, SPACEAF operates the Western Launch Range at Vandenberg AFB, and the Eastern Range at Patrick AFB, Florida. The Western Range is primarily used to launch polar orbiting satellites and test intercontinental ballistic missiles, while the Eastern Range is used for other types of space launches.

As part of its satellite operations mission, USSPACECOM is responsible for controlling space systems once they are in orbit, making sure they are operating properly and avoiding other space objects or debris. USSPACECOM's worldwide sensor network of radar and optical systems, tracks and maintains a catalog of more than 8,300 space objects that range in size from a ballpoint pen to twice the size of a school bus. The United States is the only nation that actually detects, identifies, catalogs, and tracks all manmade space objects. Space

Minuteman III reentry vehicles streak through the sky near Kwajalein Atoll in the Ronald Reagan Ballistic Missile Defense Test Site.

US Army



***Today, the United States does not have a robust architecture to defend its space systems from attack, nor does it have many options to deny space to others. As seen during Operation Allied Force, the United States needs more options than bombing a satellite ground station. Therefore, establishing a strategy and developing enhanced capabilities remains the primary space control goal.***

surveillance is very important to USSPACECOM's emerging space control mission.

USSPACECOM recently assumed the responsibility as the lead military organization for the CNO missions of Computer Network Defense (CND) and Computer Network Attack (CNA). On 2 April 2001, USSPACECOM formed JTF-CNO to place the CNA and CND missions under a single operational commander. CND is USSPACECOM's first priority to protect and defend the DII from disruption, denial, degradation, or destruction. CNA complements CND by disrupting, denying, degrading, or destroying an adversary's information infrastructure. Since taking on these missions, the challenge is to stay ahead of the emerging threats to DOD networks, to keep abreast of rapidly changing technology, and to coordinate closely with other government agencies and civilian industries actively engaged in this mission.

Placing CNO under a single operational commander enables unity of command and effort, more efficiently uses available resources, eases coordination with the intelligence community, and establishes clearer interagency coordination. As USSPACECOM learns more about the mission and as the nation develops communications and information strategy, the JTF-CNO serves as a pathfinder organization that will adapt to changing threats and to its expanding mission. JTF-CNO may someday

evolve into a subunified command.

USCINCSpace's strategic objective is to operationalize CNO into the fifth domain of warfare, separate and distinct, but fully integrate it into air, land, sea, and space across the full spectrum of conflict with the ability to leverage the computer network domain to achieve and maintain information and decision superiority for the joint force. To achieve this, USSPACECOM has developed a multiphased CNO campaign plan to direct the planning, operational, technical, and programmatic integration activities to operationalize CNO. Today, we are planning for and working real-world exercises and contingency operations. The end state is a robust and threat-adaptive organization.

Space control involves ensuring the United States' use of space while denying its use to the enemy. Space control is and will be very important to maximizing the United States' warfighting capability. Today, the United States does not have a robust architecture to defend its space systems from attack, nor does it have many options to deny space to others. As seen during Operation Allied Force, the United States needs more options than bombing a satellite ground station. Therefore, establishing a strategy and developing enhanced capabilities remains the primary space control goal. Space control does not mean that the United States intends to dominate space. Rather, it means that the United

States will achieve control when, where, and for as long as needed.

Space control consists of four elements: surveillance, prevention, protection, and negation. The key to success will be improving our space surveillance capabilities. Effective space control is only possible by achieving space situational awareness and by knowing the operational environment. The United States must be able to prevent unauthorized access and exploitation of its systems and protect those systems from hostile acts and environmental hazards. Robust hardening and system redundancy are methods of protection, and the NAVWAR program is a good example of preventing an adversary's use of GPS.

Finally, if prevention or protection fails, the United States must negate the enemy's use of space to maintain space superiority. Negation options must cover the full spectrum from temporary, reversible effects, such as jamming or blocking satellite access, to more permanent options such as destroying an adversary's space capability. We are not there yet—much work needs to be done and more resources will be required.

Force application is another mission area that may someday play a major role in space control and ballistic missile defense. Force application is the capability to apply force using space-to-space or space-to-surface weapons. The United States currently has no weapons in space due to U.S. policy; however, the President has tasked USSPACECOM, through the Unified Command Plan, to plan for force application from space. It is working on solution technology and doctrine to employ such systems.

The United States enjoys an advantage over potential adversaries in space operations and CNO. Since Desert Storm, USSPACECOM has devoted considerable time and effort to operationalizing and integrating space into the military's day-to-day activities. Developing and maturing the force enhancement capabilities that provide critical information to the warfighter has eliminated the traditional space stovepipes. As a result, the U.S. military is

more dependent on space and CNO than ever before, and this dependence has become a vulnerability. Potential adversaries recognize this and are seeking asymmetrical strategies or approaches to exploit U.S. weaknesses.

Fortunately, for the past 6 years, USSPACECOM has been looking to the future. USSPACECOM's vision for 2020 and the Long-Range Plan

---

***In 1994, there were 225 detected events; by 2000, there were 23,662. The U.S. Air Force, U.S. Army, and U.S. Navy recorded a combined total of 600 cyberattacks in 1999 and 715 cyberattacks in 2000 against their systems and networks. There are two primary reasons for this increase. First, we have improved our ability to identify these events. . . . Second, our adversaries have improved their ability to gain unauthorized access through better hacking tools, organization, and politics.***

---

(LRP) has established a road for the military space community. Recently, through an effort known as the Strategic Focus, our staff and components examined the LRP elements, including newly established CNO capabilities, to see how well we have implemented our plan. We determined that our components and the services have demonstrated a strong commitment to realizing USSPACECOM's vision by meeting 80 percent of its LRP goals. While analysis has shown that the United States can maintain its overall lead in the future, we found that planning and funding for some systems and technologies require additional emphasis. Efforts are under way to make up shortfalls.

Today, we are at the crossroads. Space and information will be the foundation that will make possible the transformation of U.S. military forces—a critical enabler of decision superiority. There is much work to be done, but USSPACECOM is moving in the right direction to meet the space and CNO challenges of the 21st century. **MR**

*Lieutenant General Edward G. Anderson III, U.S. Army, is the deputy commander in chief and chief of staff, U.S. Space Command; and vice commander, U.S. Element, North American Aerospace Defense Command (NORAD), Peterson Air Force Base, Colorado. He received a B.S. from the United States Military Academy, an M.S. from the Georgia Institute of Technology, and an M.A. from the U.S. Naval War College. He is a graduate of the British Higher Command and Staff College. He served in various command and staff positions, including director, Strategic Plans and Policy (J5), Joint Chiefs of Staff, Washington, DC; commander, U.S. Army Space and Missile Defense Command, Huntsville, Alabama; Assistant Deputy Chief of Staff for Operations and Plans for Force Development, Headquarters, Department of the Army, Washington, DC; and deputy commanding general for Combat Developments, U.S. Army Combined Arms Command, Fort Leavenworth, Kansas.*