



Space, Missile Defense
and Computer Network Operations Challenges:

**Computer Network Operations:
A Critical Element of Current and Future
Military Operations
in Combating the Asymmetrical Threat**

(Third in a series of three Background Briefs based on information
provided by U.S. Army Space and Missile Defense Command)

Computer-based Information Operations could provide our adversaries with an asymmetric response to U.S. military superiority by giving them the potential to degrade or circumvent our advantage in conventional military power.

George J. Tenet
Director of Central Intelligence
before the Senate Select Committee on Intelligence
7 February 2001

Introduction

The conduct of military operations is no longer limited to the traditional dimensions of land, sea and air. Technology has taken the realm of warfare into the space and cyber domains. In today's information age, fighting and winning battles on a traditional battlefield is no longer the norm, but rather the exception. The enemy is becoming increasingly sophisticated and resourceful in his approach and methods in shaping the battlespace through "cyberwarfare." As the traditional geographical boundaries do not exist in the world of global networks, adversaries of the United States are quickly becoming capable of causing millions of dollars worth of damage, disrupting communications and military operations, and in some cases, influencing U.S. decisionmaking processes, most often from safe havens thousands of miles away. Today, the Army views computer network operations (CNO) as an extension of the commander's combat power. The integration of CNO into military operations creates the ability to achieve the information superiority and full battlespace awareness necessary for full-spectrum dominance.

Intelligence sources have revealed that adversaries will continue to seek and develop asymmetric approaches as a means to counter the Army's superior warfighting capabilities. Adversaries understand the importance of operating in the cyber arena. More than 20 nations and a

myriad of nongovernmental organizations and individuals are developing Computer Network Attack (CNA) capabilities.¹ China, Russia, Cuba, Iran, Iraq, Libya and North Korea are developing capabilities to attack military systems. “More and more countries, especially poorer ones, are coming to see the advantage of cyberwarfare methods over traditional warfare.”² Investing in cyber technology is far less expensive, often costing thousands of dollars, compared with billions for a nuclear weapons program.

CNO and Joint Operations

Both *Joint Vision 2020*³ and *The Army Vision*⁴ recognize the need for information dominance—the ability to collect, process and disseminate an uninterrupted flow of information while exploiting or denying an adversary’s ability to do the same. Operations within the information domain are as important as those conducted on and in the land, sea, air and space domains. Full-spectrum dominance rests upon information superiority as a key enabler.

The Army’s warfighting doctrine, Field Manual (FM) 3-0, *Operations*, underscores the importance of information operations (IO) to successful military operations. Computer network operations provide the foundation from which the Army can achieve its goal of information dominance, and are critical in shaping the battlespace and setting the conditions for success. The commander’s battlespace includes that part of the global information environment that encompasses any information activity affecting his operations.

Full Dimensional Protection will control the battlespace to ensure that U.S. forces can maintain freedom of action during deployment, maneuver and engagement while providing multilayered defenses for forces and facilities at all levels. Adversaries probe U.S. networks continuously for vulnerabilities. The Army Computer Emergency Response Team (ACERT) documented more than 14,600 network security incidents and 98 known intrusions in 2001. The trend indicates these numbers will significantly increase by the end of 2002. There is no doubt that the potential for “cyberwarfare” and attacks on U.S. computer networks are high. Says the vice director of the Defense Information Systems Agency (DISA), Major General James D. Bryan, “I don’t want to sound like an alarmist, but computer network defense is a 24-by-7 constant vigilance operational environment for us. We are engaged every day; we’re attacked every day; and we defend in depth every day.”⁵

A commander must understand the flow of information within his command and how the loss or degradation of his networks influences his ability to conduct operations. Computer Network Defense⁶ is essential to preserving a commander’s freedom of maneuver, and must employ advanced technologies and applications to enhance the defense of Army networks. The Army’s Future Combat Systems (FCS) will have access to the Global Information Grid (GIG) through the Tactical Internet for sharing and dissemination of information and will have organic protection and restoration capabilities.

Shaping operations at any echelon creates and preserves conditions for the success of the decisive operation. Computer Network Attack⁷ capabilities provide the warfighter a nonkinetic option to shape the environment and to seize and retain the initiative. It is another means of delivering “precision fire” to support overall targeting and scheme of maneuver as part of decisive operations. Much like any other precision weapon system, CNA requires a robust intelligence capability to provide the precise information and detection capabilities to target an adversary’s information capabilities without causing unintended or collateral damage. Computer network reconnaissance or exploitation, commonly referred to as CNE,⁸ provides a thorough mapping of the target network, identifies specific requirements for the successful execution of friendly CNA, and in some cases, identifies access routes to an adversary’s system. Currently, each service has invested resources to develop its own unique CNO capabilities. Computer Network Attack supports and augments tactical combat operations, such as suppression of

enemy air defense (SEAD), psychological or military deception operations. CNA also supports defensive information operations by attacking an adversary's computer and telecommunications resources, which they often use to attack or exploit friendly information systems and networks. Using CNA to strengthen our defenses is not a new concept, but one that supports an "active defense." At the operational level, CNA may support forward presence operations, serve as a deterrent, or support contingency operations.

As part of the overall offensive IO campaign, Computer Network Attack may have strategic value as well by demonstrating U.S. resolve to uphold and support certain democratic or human rights, values or issues. CNA also serves to provide a force-projection capability to nations and nongovernmental organizations that have never had it before. As an asymmetric response, CNA allows an adversary to "come ashore" and affect the daily lives of Americans or any deployed force by attacking the home station or intermediate staging base support centers. The proliferation of personal computers, and the skills associated with them, have created millions of potential "information or cyber warriors." Past incidents indicate the cyber threat will continue to increase significantly in the near future. As the probability of a cyber occurrence increases, so does the potential for network damage. From the unsophisticated hacker to the state-sponsored engineer, individuals and countries are investing in advanced technology to attack U.S. information infrastructure in hopes of gaining an economic, political or military advantage.

CNO and Army Transformation

Army operations are increasingly dependent upon high-speed, high-volume information networks to identify targets, create and pass plans, disseminate and share intelligence information, and execute warfare. These information networks have become the linchpin as the Army transforms to the Objective Force. The goal to "acquire and deliver assured access anywhere . . . the Army's part of the Global Grid,"⁹ and to deny the same to an adversary, has become a basic tenet of the Army transformation.

The Defense Science Board Task Force on Defensive Information Operations concluded the GIG is a weapon system and should be treated as such.¹⁰ Currently, the GIG has hundreds of known critical vulnerabilities. With a 20 percent connection growth and 400 percent traffic growth on Department of Defense (DoD) unclassified networks each year, the number of unknown vulnerabilities may well be in the thousands. Protecting U.S. information and information infrastructure presents some unique challenges for today's commanders. Potential adversaries could easily exploit network vulnerabilities if today's network administrators leave them unchecked, possibly allowing for the acquisition of vast amounts of useful information.

The Army's portion of the GIG includes those circuits normally used for record traffic in peacetime, as well as wireless, space-based and tactical networks. As the Army continues to digitize its forces, networked communications to pass data around the battlefield move further forward into the tactical arena. Reachback capabilities, essential for reducing the Objective Force's logistical footprint in an operational theater, provide the foundation for split-based command, control, communications, computer, intelligence, surveillance and reconnaissance (C⁴ISR), personnel and logistics support.

This increased reliance on information systems increases the vulnerability of U.S. forces. Active intervention (e.g., jamming) in a tactical wireless network can deny communication service in a local geographic area. An attack on system-level databases or exploitation of the network control structure can cause failure of the entire network. Critical operating functions provided by reachback capabilities, particularly in the areas of communications, imagery, reconnaissance and warning, will continue to move to space. Space systems have become critical in moving high-volume data at great speed, thus enabling the formation of vast interactive global databases, video conferencing, and the transfer of

large amounts of data (e.g., imagery) important to deployed military forces. Space is fast becoming a primary enabler of the Army's transformation, with CNO and space beginning to converge to the point of interdependence.

As the Army transforms to the Interim and Objective Forces, CNO will undergo a parallel transformation from the current "platform-centric" to a "network-centric" warfare approach. The key feature will be an information superiority-enabled concept of operations that generates increased combat power to achieve shared awareness, increased speed of command, a higher tempo of operations, greater lethality, and increased survivability. In the Objective Force, Computer Network Operations will use a "knowledge-centric" approach to leverage information technologies to provide enhanced situational awareness and the connectivity and interoperability needed to accelerate the warfighter's decisionmaking and execution processes within the information domain. For the Army to achieve and retain information superiority today as well as be prepared for future conflicts, it must continue to develop concepts, doctrine, policies and procedures to institute and integrate CNO at all levels of military plans and operations. The ability to combat the asymmetrical threat in cyberwarfare is dependent upon understanding all the possibilities of current and future information technology and how it can assist in defending U.S. information and information infrastructure. Obtaining a clear picture of all existing U.S. network vulnerabilities, the adversary, and his abilities in acquiring and using cyber resources will allow commanders to accurately gauge and combat the cyber threat against DoD networks.

Army CNO Force Structure

Information is the critical component that enables full and effective functioning of the U.S. military. Both CNO and space control play vital roles in achieving U.S. national objectives and are fundamental elements of the National Military Strategy. As CNO capabilities mature, they become critical to achieving space-control objectives. In 1999, the Department of Defense assigned U.S. Space Command (USSPACECOM) the mission as military lead within DoD for CND and CNA. On 1 October 2002, DoD merged USSPACECOM and USSTRATCOM under one command and, under new Unified Command Plan (UCP) language, assigned the CNO mission to USSTRATCOM.¹¹ This places both space and a critical part of the information operations domain under one combatant commander.

The Army organized its support to these mission areas by identifying U.S. Army Space and Missile Defense Command (SMDC) as the single Army component command for space and CNO. The Commanding General, SMDC executes the Army's space and CNO mission through the planning, coordination, organization, integration, distribution, direction and oversight of Army support to USSTRATCOM. The Commander, Land Information Warfare Activity (LIWA) supports CG, SMDC as his Deputy Commander for CNO. On 13 August 2002, the Secretary of the Army established the U.S. Army Network Enterprise Technology Command (NETCOM)/9th Army Signal Command (ASC), effective 1 October 2002. The Commanding General, NETCOM/9th ASC will be "the single authority assigned to operate, manage, and defend the Army's 'Infostructure' at the enterprise level."

The heart of the Army CND capability is the Army's Computer Emergency Response Team (ACERT) and the Army Network Operations and Security Center (ANOSC). The ACERT provides daily support to NETCOM and the Joint Task Force-Computer Network Operations (JTF-CNO) in their mission to defend DoD's computer and information networks. Each Regional CERT (RCERT) and collocated Theater NOSC (TNOSC) provides a mutually supportive "help-desk" capability to Army users to sort through network outages and anomalies, and identify and react to cyber attacks. The RCERTs and TNOSCs work together to monitor networks and network security devices installed at all Army gateways to the Nonsecure Internet Protocol Router Network (NIPRNET) and on critical classified servers. Together, they are the Army's capability to provide a fully coordinated Common Operational Picture

(COP) of the health of the Army's systems and networks and provide Attack Sensing and Warning support to Army users worldwide in protecting against and responding to cyber attacks.¹² NETCOM/9th Army Signal Command retains responsibility for the defense of the Army's portion of the GIG. The Intelligence and Security Command (INSCOM) is the Army's principal CNA combat developer and organization.

The Space and Missile Defense Command provides the principal interface and facilitates coordination of effort among the Army, USSTRATCOM, and other service components actively working to develop joint doctrine, strategies, plans, and tactics, techniques and procedures (TTP) for CNO. SMDC also works to integrate Army concerns, issues, and projects into USSTRATCOM's Integrated Priority List and assists with the development of other joint operational planning requirements. SMDC also advocates for Army CNO funding within DoD.

Space control provides the Army an offensive and defensive capability that will allow U.S. forces to gain and maintain control of activities conducted in space. This capability prevents an enemy force from gaining an advantage from space systems and space capabilities, and protects U.S. forces' ability to conduct military operations. Effective planning and integration of Computer Network Defense can provide protection to Army space communication capabilities against cyber attacks mounted against any of the infrastructure nodes and databases. Depending on operational considerations, CNA provides a nonlethal means of denying threat satellites certain orbits or portions of orbits, and of minimizing generation of space debris in support of force projection operations or national deterrence options.

Conclusion

While the Information Age has created enormous opportunities, it also created significant vulnerabilities for an Army dependent upon an uninterrupted flow of timely, quality information to support operations. The Army must continue to develop and support CNO by:

- increasing its intelligence capabilities to collect information and provide attack sensing and warning;
- refining the CNO structure to streamline command and control for Army CNO and space operations and support;
- continuing to develop concepts, doctrine, and the tactics, techniques and procedures necessary to conduct CNO;
- making CNO an integral part of the planning process;
- integrating CNO and space with fires and maneuver;
- making CNO and space available to commanders knowledgeable and experienced in their use;
- incorporating CNO and space into training and evaluations, including warfighter exercises and wargames.

Protecting Army information and information systems is a necessity. We cannot afford to ignore it, since in a network-centric force, *everyone* is on the front line.

Endnotes

1. "Protecting the Homeland," Report of the Defense Science Board Task Force on Defensive Information Operations, March 2001, p. ES-2.
2. Richard A. Clarke, "White House Officials Debating Rules For Cyberwarfare," The Washington Post, August 22, 2002.
3. Joint Chiefs of Staff, *Joint Vision 2020*, June 2000, online at <http://www.dtic.mil/jv2020/>.
4. Department of the Army, *The Army Vision*, October 1999, online at <http://www.army.mil/vision/default.htm>.
5. MG James D. Bryan, Vice Director, Defense Information Systems Agency (DISA)/Commander, Joint Task Force for Computer Network Operations (JTF-CNO), "Military Information Technology," Volume 5, Issue 3, 2001.
6. Computer Network Defense (CND) comprises the actions taken to protect, monitor, analyze, detect and respond to unauthorized activity within DoD information systems and computer networks (Joint Publication [JP] 1-02, NATO).
7. Computer Network Attack (CNA) comprises operations to disrupt, deny, degrade or destroy information resident in computers and computer networks, or the computers and networks themselves (JP 1-02).
8. Computer Network Exploitation (CNE) comprises enabling operations and intelligence collection to gather data from target or adversary automated information systems or networks (Department of Defense Directive [DODD] 3600.1, Information Operations [IO]).
9. Robert K. Ackerman, "Electronics Transform the Army," *SIGNAL* Magazine, August 2001.
10. Defense Science Board Task Force Report, p. ES-2.
11. On 1 October 2002, DoD merged USSPACECOM and USSTRATCOM into one command and named it USSTRATCOM.
12. Department of Defense, Department of the Army, Information Technology Fiscal Year (FY) 2002 Amended Budget Estimates, July 2001.