AUSA Background Brief

No. 93
December 2001

An Institute of Land Warfare Publication

Space and Missile Defense Challenges:

Computer Network Operations— An Integral Part of Land Force Operations

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

The Objective Force . . . will leverage joint and interagency reach-back capabilities for . . . information operations while protecting itself against information attacks.

General Eric K. Shinseki, Chief of Staff, Army
Senate Armed Services Committee Testimony
10 July 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. 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 information superiority and full battlespace awareness necessary for full-spectrum dominance. Adversaries understand the importance of operating in the cyber arena. More then 20 nations and a myriad of nongovernmental organizations and individuals are developing computer network attack capabilities.[1] China, Russia, Cuba, Iran, Iraq, Libya and North Korea are developing capabilities to attack military systems. Adversaries will continue to seek and develop asymmetric approaches as a means to counter the Army's superior warfighting capabilities.

CNO and Joint Operations

Both Joint Vision 2020 and the Army Vision 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 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 our forces can maintain freedom of action during deployment, maneuver and engagement** while providing multilayered defenses for our forces and facilities at all levels. Adversaries probe our networks continuously for vulnerabilities. The Army Computer Emergency Response Team (ACERT) documented over 5,500 network security incidents and 64 known intrusions in 2000. The trend indicates these numbers will significantly increase by the end of 2001.

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 Defense (CND)[2] is essential to preserving a commander's freedom of maneuver, and must employ advanced technologies and applications to enhance the defense of Army networks.

***Shaping operations* at any echelon creates and preserves conditions for the success of the decisive operation.** Computer Network Attack (CNA)[3] 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 Attack supports and augments tactical combat operations, such as suppression of enemy air defense (SEAD), and psychological or military deception operations. CNA also supports defensive information operations by attacking an adversary's computer and telecommunications resources used to attack or exploit friendly information systems and networks. 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, CNA may have strategic value as well by demonstrating U.S. resolve to uphold and support certain democratic or human rights, values or issues.

Computer Network Attack provides a force projection capability to nations and nongovernmental organizations that have never had it before. As an asymmetric response, an adversary's CNA allows him to virtually "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 warriors."

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 lynchpin as the Army transforms to the Objective Force. The goal to "acquire and deliver assured access anywhere [in] the Army's part of the Global Grid,"[4] and to deny the same to an adversary, has become a basic tenet of Army Transformation.

The Defense Science Board Task Force on Defensive Information Operations concluded the global information grid (GIG) is a weapon system and is treated as such.[5] 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 are essential for reducing the Objective Force's logistical footprint in an operational theater and provide the foundation for split-based command, control, communications, computer, intelligence, surveillance and reconnaissance (C^4ISR); personnel; and logistics support.

This increased reliance on information systems increases the vulnerability of our 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 needed to accelerate the warfighter's decisionmaking and execution 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.

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 the Department of Defense for CND and CNA. This places both space and a critical part of the information operations domain under one commander.

The Army organized its support to these mission areas by identifying U.S. Army Space Command (ARSPACE) as the single Army component command for space and CNO. The Commanding General, ARSPACE executes the Army's space and CNO mission through the planning, coordination, organization, integration, distribution, direction and oversight of Army support to USSPACECOM. The Commander, Land Information Warfare Activity (LIWA) supports CG, ARSPACE as his deputy commander for CNO.

The heart of the Army's CND capability is the Army Computer Emergency Response Team (ACERT) working in close coordination with the Army Network Operations and Security Center (ANOSC). The ACERT provides daily support to the Joint Task Force-Computer Network Operations (JTF-CNO) in their mission to defend our computer and information networks. Each Regional Computer Emergency Response Team (RCERT) and co-located Theater Network Operations and Security Center (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 intrusion detection systems installed at all Army gateways to the Nonsecure Internet Protocol Router Network (NIPRNET) and on critical 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.[6] The Intelligence and Security Command (INSCOM) is the Army's principal CNA organization as a user and combat developer. The Army Signal Command retains responsibility for the physical configuration all Army computer networks.

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

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.

To support current and future operations, ARSPACE established a Space and Information Operations Element (SIOE) to provide reachback support for Army forces, and to support joint planning and operations. Partnered with ARSPACE, the LIWA assists with full-spectrum information operations planners and subject matter experts in both CND and CNA. ARSPACE also organized support teams able to deploy in direct support of Army forces to assist staffs with the planning, integration and synchronization of space and information operations.

Conclusion

While the Information Age has created enormous opportunities, it has 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.

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. Computer Network Defense (CND): 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, *DoD Dictionary of Military and Associated Terms*).
3. Computer Network Attack (CNA): operations to disrupt, deny, degrade, or destroy information resident in computers and computer networks, or the computers and networks themselves (JP 1-02).
4. Robert K. Ackerman, "Electronics Transform the Army," *SIGNAL* Magazine, August 2001.
5. Defense Science Board Task Force Report, p. ES-2.
6. Department of Defense, Department of the Army, Information Technology Fiscal Year (FY) 2002 Amended Budget Estimates, July 2001.