Order Code RL31787

CRS Report for Congress

Information Operations, Electronic Warfare, and Cyberwar: Capabilities and Related Policy Issues

Updated March 20, 2007

Clay Wilson
Specialist in Technology and National Security
Foreign Affairs, Defense, and Trade Division

GalleryWatch.com
http://www.crsdocuments.com
Penny Hill Press

Prepared for Members and Committees of Congress

Congressional Research Service

Information Operations, Electronic Warfare, and Cyberwar: Capabilities and Related Policy Issues

Summary

This report describes the emerging areas of information operations, electronic warfare, and cyberwar in the context of U.S. national security. It also suggests related policy issues of potential interest to Congress.

For military planners, the control of information is critical to military success, and communications networks and computers are of vital operational importance. The use of technology to both control and disrupt the flow of information has been generally referred to by several names: information warfare, electronic warfare, cyberwar, netwar, and Information Operations (IO). Currently, IO activities are grouped by the Department of Defense (DOD) into five core capabilities: (1) Psychological Operations, (2) Military Deception, (3) Operational Security, (4) Computer Network Operations, and (5) Electronic Warfare.

Current U.S. military doctrine for IO now places increased emphasis on Psychological Operations, Computer Network Operations, and Electronic Warfare, which includes use of non-kinetic electromagnetic pulse (EMP) weapons, and non-lethal weapons for crowd control. However, as high technology is increasingly incorporated into military functions, the boundaries between all five IO core capabilities are becoming blurred.

DOD has noted that military functions involving the electromagnetic spectrum take place in what is now called the cyber domain, similar to air, land, and sea. This cyber domain is the responsibility of the new Air Force Cyber Command and includes cyberwarfare, electronic warfare, and protection of U.S. critical infrastructure networks that support telecommunications systems, utilities, and transportation.

This report will be updated to accommodate significant changes.

Contents

Introduction 1
Background 1

Definitions 2
Information 2
DOD Information Operations 2

DOD Information Operations Core Capabilities 3
Psychological Operations (PSYOP) 3
Military Deception (MILDEC) 4
Operational Security (OPSEC) 4
Computer Network Operations (CNO) 4
Computer Network Defense (CND) 4
Computer Network Exploitation (CNE) 5
Computer Network Attack (CNA) 5
Electronic Warfare (EW) 6
Domination of the Electromagnetic Spectrum 6
Electromagnetic Non-Kinetic Weapons 7

New U.S.A.F. Cyber Command 7

Joint Command Structure for Cyberwarfare 9

DOD and the U.S. Critical Infrastructure 10

Information Operations by Adversaries 10

Law and Proportionality for Information Operations 11

Cyberwarrior Education 12

Policy Issues 13

Current Legislation 14

Information Operations, Electronic Warfare, and Cyberwar: Capabilities and Related Policy Issues

Introduction

Background

Control of information has always been part of military operations, and the U.S. Strategic Command views information operations as a core military competency, with new emphasis on (1) use of electromagnetic energy, (2) cyber operations, and (3) use of psychological operations to manipulate an adversary's perceptions. Department of Defense (DOD) officials now consider cyberspace to be a domain for warfare, similar to air, space, land, and sea.[1]

The DOD views information itself as both a weapon and a target in warfare. In addition, Psychological Operations (PSYOP) provides the ability to rapidly disseminate persuasive information to directly influence the decisionmaking of diverse audiences, and is seen as a means for deterring aggression, and important for undermining the leadership and popular support for terrorist organizations.[2]

However, new technologies for military IO also create new national security policy issues, including (1) consideration of psychological operations used to affect friendly nations or domestic audiences; and (2) possible accusations against the U.S. of war crimes if offensive military computer operations or electronic warfare tools severely disrupt critical civilian computer systems, or the systems of non-combatant nations.

This report describes DOD capabilities for conducting military information operations, and gives an overview of related policy issues. This report will be updated as events warrant.

---

[1] Jason Ma, "Information Operations To Play a Major Role in Deterrence Posture,"*Inside Missile Defense*, Dec. 10, 2003 [http://www.insidedefense.com/secure/defense_docnum.asp?f=defense_2002.ask&docnum=MISSILE-9-25-4]. Todd Lopez, *Air Force Leaders to Discuss new 'Cyber Command'*, Air Force News, Nov 5, 2006, [http://www.8af.acc.af.mil/news/story_print.asp?storyID=123031988]

[2] DOD Information Operations Roadmap, October 30, 2004, p.3. This document was declassified January, 2006, and obtained through FOIA by the National Security Archive at George Washington University. [http://www.gwu.edu/~nsarchiv/NSAEBB/NSAEBB177/info_ops_roadmap.pdf].

Definitions

Information

Information is a resource created from two things: phenomena (data) that are observed, plus the instructions (systems) required to analyze and interpret the data to give it meaning. The value of information is enhanced by technology, such as networks and computer databases, which enables the military to (1) create a higher level of shared awareness, (2) better synchronize command, control, and intelligence, and (3) translate information superiority into combat power.

DOD Information Operations

The current DOD term for military information warfare is "Information Operations" (IO). DOD information operations are actions taken during time of crisis or conflict to affect adversary information, while defending one's own information systems, to achieve or promote specific objectives.[3] The focus of IO is on disrupting or influencing an adversary's decision-making processes.

An IO attack may take many forms, for example: (1) to slow adversary computers, the software may be disrupted by transmitting a virus or other malicious code; (2) to disable sophisticated adversary weapons, the computer circuitry may be overheated with directed high energy pulses; and (3) to misdirect enemy sensors, powerful signals may be broadcast to create false images. Other methods for IO attack may include psychological operations such as initiating TV and radio broadcasts to influence the opinions and actions of a target audience, or seizing control of network communications to disrupt an adversary's unity of command.

Computer Network Defense (CND) is the term used to describe activities that are designed to protect U.S. forces against IO attack from adversaries. Part of CND is information assurance (IA), which requires close attention to procedures for what is traditionally called computer and information security.

DOD places new emphasis on the importance of dominating the entire electromagnetic spectrum with methods for computer network attack and electronic warfare. DOD also emphasizes that because networks are increasingly the operational center of gravity for warfighting, the U.S. military must be prepared to "fight the net".[4] Because the recently declassified source document containing this phrase has some lines blacked out, it is not clear if "...net"means the Internet. If so, then this phrase may be a recognition by DOD that Psychological Operations, including public affairs work and public diplomacy, must be employed in new ways to counter the skillful use of the Internet and the global news media by U.S. adversaries.

---

[3] From the *DOD Dictionary of Military and Associated Terms*, Jan. 2003 [http://www.dtic.mil/doctrine/jel/doddict/data/i/index.html].

[4] DOD Information Operations Roadmap, October 30, 2003, p.6-7. [http://www.gwu.edu/~nsarchiv/NSAEBB/NSAEBB177/info_ops_roadmap.pdf]

DOD Information Operations Core Capabilities

DOD identifies five core capabilities for conduct of information operations; (1) Psychological Operations, (2) Military Deception, (3) Operations Security, (4) Computer Network Operations, and (5) Electronic Warfare. These capabilities are interdependent, and increasingly are integrated to achieve desired effects.

Psychological Operations (PSYOP)

DOD defines PSYOP as planned operations to convey selected information to targeted foreign audiences to influence their emotions, motives, objective reasoning, and ultimately the behavior of foreign governments, organizations, groups, and individuals.[5] For example, during the Operation Iraqi Freedom (OIF), broadcast messages were sent from Air Force EC-130E aircraft, and from Navy ships operating in the Persian Gulf, along with a barrage of e-mail, faxes, and cell phone calls to numerous Iraqi leaders encouraging them to abandon support for Saddam Hussein.

At the same time, the civilian Al Jazeera news network, based in Qatar, beams its messages to well over 35 million viewers in the Middle East, and is considered by many to be a "market competitor" for U.S. PSYOP. Terrorist groups can also use the Internet to quickly place their own messages before an international audience. Some observers have stated that the U.S. will continue to lose ground in the global media wars until it develops a coordinated strategic communications strategy to counter competitive civilian news media, such as Al Jazeera.[6]

Partly in response to this observation, DOD now emphases that PSYOP must be improved and focused against potential adversary decisionmaking, sometimes well in advance of times of conflict. Products created for PSYOP must be based on in-depth knowledge of the audience's decision-making processes. Using this knowledge, the PSYOPS products then must be produced rapidly, and disseminated directly to targeted audiences throughout the area of operations.[7]

DOD policy prohibits the use of PSYOP for targeting American audiences. However, while military PSYOP products are intended for foreign targeted audiences, DOD also acknowledges that the global media may pick up some of these targeted messages, and replay them back to the U.S. domestic audience. Therefore, a sharp distinction between foreign and domestic audiences cannot be maintained.[8]

---

[5] *DOD Dictionary of Military Terms* [http://www.dtic.mil/doctrine/jel/doddict/].

[6] Air Force, *Operation Iraqi Freedom Information Operations Lessons Learned: First Look*, AFC2ISRC/CX, July 23, 2003 [http://www.insidedefense.com/secure/data_extra/pdf3/dplus2004_265.pdf].

[7] DOD Information Operations Roadmap, October 30, 2003, p.6. [http://www.gwu.edu/~nsarchiv/NSAEBB/NSAEBB177/info_ops_roadmap.pdf]

[8] DOD Information Operations Roadmap, October 30, 2003, p.26. [http://www.gwu.edu/~nsarchiv/NSAEBB/NSAEBB177/info_ops_roadmap.pdf]

Military Deception (MILDEC)

Deception guides an enemy into making mistakes by presenting false information, images, or statements. MILDEC is defined as actions executed to deliberately mislead adversary military decision makers with regard to friendly military capabilities, thereby causing the adversary to take (or fail to take) specific actions that will contribute to the success of the friendly military operation.

As an example of deception during Operation Iraqi Freedom (OIF), the U.S. Navy deployed the Tactical Air Launched Decoy system to divert Iraqi air defenses away from real combat aircraft.

Operational Security (OPSEC)

OPSEC is defined as a process of identifying information that is critical to friendly operations and which could enable adversaries to attack operational vulnerabilities. For example, during OIF, U.S. forces were warned to remove certain information from DOD public websites, so that Iraqi forces could not exploit sensitive but unclassified information.

Computer Network Operations (CNO)

CNO includes the capability to: (1) attack and disrupt enemy computer networks; (2) defend our own military information systems; and (3) exploit enemy computer networks through intelligence collection, usually done through use of computer code and computer applications. The Joint Information Operations Warfare Command (JIOWC) and the Joint Functional Component Command for Network Warfare (JFCCNW) are responsible for the evolving mission of Computer Network Attack.[9] The exact capabilities of the JIOWC and JFCCNW are highly classified, and DOD officials have reportedly never admitted to launching a cyber attack against an enemy, however many computer security officials believe the organization can destroy networks and penetrate enemy computers to steal or manipulate data, and take down enemy command-and-control systems. They also believe that the organization consists of personnel from the CIA, National Security Agency, FBI, the four military branches, and civilians and military representatives from allied nations.[10]

Computer Network Defense (CND). CND is defined as defensive measures to protect information, computers, and networks from disruption or destruction. CND includes actions taken to monitor, detect, and respond to unauthorized computer activity. Responses to IO attack against U.S. forces may

---

[9] John Lasker, *U.S. Military's Elite Hacker Crew*, Wired News, April 18, 2005, [http://www.wired.com/news/privacy/0,1848,67223,00.html], U.S. Strategic Command Fact File [http://www.stratcom.mil/fact_sheets/fact_jtf_gno.html] and [http://www.stratcom.mil/fact_sheets/fact_jioc.html].

[10] John Lasker, *U.S. Military's Elite Hacker Crew*, April 18, 2005, Wired News, [http://www.wired.com/news/privacy/0,67223-0.html?tw=wn_story_page_prev2].

include use of passive information assurance tools, such as firewalls or data encryption, or may include more intrusive actions, such as monitoring adversary computers to determine their capabilities before they can attempt an IO attack against U.S. forces.

Some DOD officials believes that CND may lack sufficient policy and legal analysis for guiding appropriate responses to intrusions or attacks on DOD networks. Therefore, DOD has recommended that a legal review be conducted to determine what level of intrusion or data manipulation constitutes an attack. The distinction is necessary in order to clarify whether an action should be called an attack or an intelligence collection operation, and which aggressive actions can be appropriately taken in self-defense. This legal review should also determine if appropriate authorities permit U.S. forces to retaliate through manipulation of unwitting third party computer hosts. And finally, DOD has recommended structuring a legal regime that applies separately to domestic and to foreign sources of computer attack against DOD or the U.S. critical. infrastructure.[11]

Computer Network Exploitation (CNE). CNE is an area of IO that is not yet clearly defined within DOD. Before a crisis develops, DOD seeks to prepare the IO battlespace through intelligence, surveillance, and reconnaissance, and through extensive planning activities. This involves intelligence collection, that in the case of IO, is usually performed through network tools that penetrate adversary systems to gain information about system vulnerabilities, or to make unauthorized copies of important files. Tools used for CNE are similar to those used for computer attack, but configured for intelligence collection rather than system disruption.

Computer Network Attack (CNA). CNA is defined as effects intended to disrupt or destroy information resident in computers and computer networks. As a distinguishing feature, CNA normally relies on a data stream used as a weapon to execute an attack. For example, sending a digital signal stream through a network to instruct a controller to shut off the power flow is CNA, while sending a high voltage surge through the electrical power cable to short out the power supply is considered Electronic Warfare (However, a digital stream of computer code or a pulse of electromagnetic power can both be used to also create false images in adversary computers).

During Operation Iraqi Freedom, U.S. and coalition forces reportedly did not execute any computer network attacks against Iraqi systems. Even though comprehensive IO plans were prepared in advance, DOD officials stated that top-level approval for several CNA missions was not granted until it was too late to carry them out to achieve war objectives.[12] U.S. officials may have rejected launching a planned cyber attack against Iraqi financial computers because Iraq's banking network is connected to a financial communications network also located in Europe. Consequently, according to Pentagon sources, an information operations attack

---

[11] DOD Information Operations Roadmap, October 30, 2003, p52. [http://www.gwu.edu/~nsarchiv/NSAEBB/NSAEBB177/info_ops_roadmap.pdf]

[12] Elaine Grossman, "Officials: Space, Info Targets Largely Cobbled On-The-Fly for Iraq," *Inside the Pentagon*, May 29, 2003.

directed at Iraq might also have brought down banks and ATM machines located in parts of Europe as well. Such global network interconnections, plus close network links between Iraqi military computer systems and the civilian infrastructure, reportedly frustrated attempts by U.S. forces to design a cyber attack that would be limited to military targets only in Iraq.[13]

In a meeting held in January 2003, at the Massachusetts Institute of Technology, White House officials sought input from experts outside government on guidelines for use of cyber-warfare. Officials have stated they are proceeding cautiously, since a cyberattack could have serious cascading effects, perhaps causing major disruption to networked civilian systems.[14] In February 2003, the Bush Administration announced national-level guidance for determining when and how the United States would launch computer network attacks against foreign adversary computer systems. The classified guidance, known as National Security Presidential Directive 16, is intended to clarify circumstances under which a disabling computer attack would be justified, and who has authority to launch such an attack.

Electronic Warfare (EW)

EW is defined by DOD as any military action involving the direction or control of electromagnetic spectrum energy to deceive or attack the enemy. High power electromagnetic energy can be used as a tool to overload or disrupt the electrical circuitry of almost any equipment that uses transistors, micro-circuits, or metal wiring.[15] Directed energy weapons amplify, or disrupt, the power of an electromagnetic field by projecting enough energy to overheat and permanently damage circuitry, or jam, overpower, and misdirect the processing in computerized systems. The Electronic Warfare Division of the Army Asymmetric Warfare Office has responsibility for creating electronic warfare policy, and for supporting development of new electromagnetic spectrum concepts that can be translated into equipment and weapons.

Domination of the Electromagnetic Spectrum. DOD now emphasizes maximum control of the entire electromagnetic spectrum, including the capability to disrupt all current and future communication systems, sensors, and weapons systems. This may include: (1) navigation warfare, including methods for offensive space operations where global positioning satellites may be disrupted; or, (2) methods to control adversary radio systems; and, (3) methods to place false images onto radar systems, block directed energy weapons, and misdirect unmanned aerial vehicles (UAVs) or robots operated by adversaries.[16]

---

[13] Charles Smith, "U.S. Information Warriors Wrestle with New Weapons," *NewsMax.com*, March 13, 2003 [http://www.newsmax.com/archives/articles/2003/3/12/134712.shtml].

[14] Bradley Graham, "Bush Orders Guidelines for Cyber-Warfare," *Washington Post*, February 7, 2003, Section A, p.1.

[15] CRS Report RL32544, *High Altitude Electromagnetic Pulse (EMP) and High Power Microwave (HPM) Devices: Threat Assessments*, by Clay Wilson.

[16] DOD Information Operations Roadmap, October 30, 2003, p.61. [http://www.gwu.edu/~nsarchiv/NSAEBB/NSAEBB177/info_ops_roadmap.pdf]

For example, recent military IO testing examined the capability to secretly enter an enemy computer network and monitor what their radar systems could detect. Further experiments tested the capability to take over enemy computers and manipulate their radar to show false images.[17]

Electromagnetic Non-Kinetic Weapons. Non-kinetic weapons emit directed electromagnetic energy that, in short pulses, may permanently disable enemy computer circuitry. For example, an electromagnetic non-kinetic weapon mounted in an aircraft, or on the ground, might disable an approaching enemy missile by directing a High Power Microwave (HPM) beam that burns out the circuitry, or that sends a false telemetry signal to misdirect the targeting computer.[18] Also, at reduced power, electromagnetic non-kinetic weapons can also be used as a non-lethal method for crowd control.

The Active Denial System (ADS), developed by the Air Force, is a vehicle-mounted nonlethal, counter-personnel directed energy weapon. Currently, most non-lethal weapons for crowd control, such as bean-bag rounds, utilize kinetic energy. However, the ADS projects a focused beam of millimeter energy waves to induce an intolerable burning sensation on an adversary's skin, repelling the individual without causing injury. Proponents say the ADS is safe and effective at ranges between 50 and 1,600 feet. The nonlethal capabilities of the ADS are designed to protect the innocent, minimize fatalities, and limit collateral damage.[19]

The Pentagon reportedly has requested immediate deployment of at least 8 ADS devices to Iraq to assist Marines in guarding posts, countering insurgent snipers and protecting convoys. The ADS system would be the first operationally deployed directed-energy weapon for counter-personnel missions.[20]

New U.S.A.F. Cyber Command

Secretary of the Air Force Michael W. Wynne recently stated that the new mission of the U.S. Air Force is to "fly and fight in air, space, and cyberspace." This means that military action in cyberspace now includes defending against malicious activity on the Internet, and anywhere across the entire electromagnetic spectrum (including the energy spectrum bands for radio, microwaves, infrared, X-ray, and all

---

[17] These programs were called Suter 1 and Suter 2, and were tested during Joint Expeditionary Forces Experiments held at Nellis Air Force Base in 2000 and 2002. David Fulghum, "Sneak Attack," *Aviation Week & Space Technology*, June 28, 2004, p. 34.

[18] David Fulghum, "Sneak Attack," *Aviation Week & Space Technology*, June 28, 2004, p.34.

[19] Active Denial System, Fact Sheet, Air Force Research Lab, Office of Public Affairs, Kirtland Air Force Base, [http://www.de.afrl.af.mil/Factsheets/ActiveDenial.pdf].

[20] Jason Sherman, *Pentagon Considering Sending Non-Lethal Ray Gun to Iraq*, Inside Defense, Mar 2, 2007.

other options for directed energy), where national security is threatened.[21] Secretary Wynne stated that cyberwarfare flows naturally from the Air Force's traditional missions, such as downloading data from platforms in space, and that U.S. capabilities should be expanded to also enable the shut down of enemy electronic networks. Consequently, the 8th Air Force, headquartered at Barksdale Air Force Base, La., has been designated as the operational Cyber Command, responsible for organizing, training, and equipping the Air Force for cyberspace operations.[22] The new Cyber Command will draw on resources from all Air Force commands to gather needed expert capabilities.

Air Force officials, led by the Air Force Chief of Staff Gen. Michael Mosley, met at the Pentagon in a "cyberwarfare-themed summit" during November 2006, to make plans for the new Air Force Cyber Command.[23] General Elder stated that the planning session may require approximately four months of work, and will include an assessment of offensive and defensive cyberwarfare requirements, as well as a review of current capabilities and future needs.[24]

Homeland security reportedly will also be a large part of the Cyber Command's new responsibility, including protection of telecommunications systems, utilities, and transportation. Several issues to be considered may include: (1) what kind of educational skills, technical skills, and training are needed for staff at the Cyber Command; and (2), what kind of career path can be offered to those in the Air Force who want to participate in defending the new cyber domain.

In addition, the Air Force Materiel Command will review the research now ongoing at the 8th Air Force headquarters to identify which work should receive funding as part of the new cyberwarfare function.[25] Some examples of systems or projects that could be affected by the cyber command mission include (1) the Airborne Laser System at Edwards AFB, (2) the Active Denial System at Moody AFB, (3) the Joint Surveillance Target Attack Radar System at Robins AFB, and (4) efforts to protect against damage to computer systems due to electromagnetic pulse attack.

Officials at the 8th Air Force report that as of January 2007, the new U.S.A.F. cyber command has not yet been officially activated, and the final command structure

---

[21] John Bennett and Carlo Munoz, *USAF Sets Up First Cyberspace Command*, Military.com, Nov 4, 2006, [http://www.military.com/features/0,15240,118354,00.html].

[22] Todd Lopez, *8th Air Force to become New Cyber Command,* Air Force Link, Nov 3, 2006, [http://www.af.mil/news/story.asp?storyID=123030505]. Dave Ahearn, *Air Force Forms Cyberspace Unit*, Defense Daily, Nov 3, 2006.

[23] Contact for Dr. Lani Kass, Director of Air Force Cyberspace Task Force, and Special Assistant to General Michael Moseley, is through Maj. Gary Conn, Gary.Conn@pentagon.af.mil, 703-697-3143.

[24] Personal communication with Air Force Public Affairs Office, January 26, 2007.

[25] Head Quarters at Wright Patterson AFB, 937-522-3252, [http://www.wpafb.af.mil/].

has not been determined.[26] Initially, the new organization will operate on an equal footing with other numbered Air Force headquarters. However, eventually the new organization will become a major command that will stand alongside the Air Force Space Command and the Air Combat Command. Precise future command relationships are still being decided in the ongoing planning effort, and more details will be forthcoming.[27]

Joint Command Structure for Cyberwarfare

Currently, the U.S. Strategic Command (USSTRATCOM), which is a unified combatant command for U.S. strategic forces, controls military information operations, space command, strategic warning and intelligence assessments, global strategic operations planning, and also has overall responsibility for Computer Network Operations (CNO).[28]

Beneath USSTRATCOM are several Joint Functional Component Commands (JFCCs): (1) space and global strike integration; (2) intelligence, surveillance and reconnaissance; (3) network warfare; (4) integrated missile defense; and (5) combating weapons of mass destruction.[29]

The JFCC-Network Warfare (JFCC-NW), and the JFCC-Space & Global Strike (JFCC-SGS) have responsibility for overall DOD cyber security. Under the JFCC-NW are the Joint Task Force-Global Network Operations (JTF-GNO) and the Joint information Operations Warfare Center (JIOWC), both of which have direct responsibility for defense against cyber attack.[30] The JTF-GNO defends the DOD Global Information Grid, while the JIOWC assists combatant commands with an integrated approach to information operations. These include operations security, psychological operations, military deception, and electronic warfare. The JIOWC also coordinates network operations and network warfare with the JTF-GNO and with JFCC-NW.

---

[26] Personal communication, Public Affairs Office at the 8th Air Force, which can be reached at 318-456-2145, [http://www.8af.acc.af.mil].

[27] Personal communication with Air Force Public Affairs Office, January 26, 2007.

[28] The Public Affairs Office for the Air Force at the Pentagon can be contacted at 703-571-2776.

[29] United State Strategic Command, July 2006, [http://www.stratcom.mil/organization-fnc_comp.html].

[30] Clark A. Murdock et. al, Beyond Goldwater-Nichols: U.S. Government and Defense Reform for a New Strategic Era, Phase 2 Report, July 2005,Center for Strategic and International Studies, p.128, [http://www.ndu.edu/lIbrary/docs/BeyondGoldwaterNicholsPhase2Report.pdf].

DOD and the U.S. Critical Infrastructure

DOD officials have noted that because 80 percent of U.S. commerce goes through the Internet, DOD systems must develop a capability to adequately protect them.[31] Currently, to assist commercially-owned telecommunications networks, communications satellite systems, and other civilian critical infrastructure systems, DOD contracts with Carnegie Mellon's Software Engineering Institute to operate the Computer Emergency Response Team (CERT-CC), while DHS in partnership with private industry operates a parallel organization called US-CERT. Both organizations monitor trends in malicious code and cyber crime, send out alerts about threats to computer systems, and provide guidance for recovery after an attack.

Information Operations by Adversaries

The low cost of entry (for example, a laptop connected to the Internet), and the ability to operate anonymously, are factors that makes cyberspace attractive to adversaries who know they cannot challenge the United States in a symmetrical contest. Potential adversaries, such as China, Russia, Cuba, Iran, Iraq, Libya, North Korea, and several non-state terrorist groups are reportedly developing capabilities to attack or degrade U.S. civilian and military networks. "Moonlight Maze" and "Titan Rain" are examples of successful attacks against non-classified military systems which DOD officials claim were directed by other governments.[32]

According to the Defense Department's annual report to Congress on China's military prowess, the Chinese military is enhancing its information operations capabilities.[33] The report finds that China is placing specific emphasis on the ability to perform information operations designed to weaken an enemy force's command and control systems.[34]

Terrorist groups also use wireless electronics to detonate roadside bombs (Improvised Explosive Devices). They also use the Internet to transmit financial transactions, and use free Global Positioning System (GPS) signals and commercial

---

[31] John Doyle, *Air Force To Elevate Status Of Cyberspace Command,* Aerospace Daily & Defense Report, Mar 22, 2007.

[32] Elinor Abreu, *Epic cyberattack reveals cracks in U.S. defense*, CNN.com, May 10, 2001, [http://archives.cnn.com/2001/TECH/internet/05/10/3.year.cyberattack.idg/]. Declan McCullagh, *Feds Say Fidel Is Hacker Threat*, WiredNews.com, Feb, 09, 2001, [http://www.wired.com/news/politics/0,1283,41700,00.html]. Staff, *Cyberattack could result in military response*, USAToday, Feb 14, 2002, [http://www.usatoday.com/tech/news/2002/02/14/cyberterrorism.htm].

[33] See the FY2004 Report to Congress on PRC Military Power, [http://www.defenselink.mil/pubs/d20040528PRC.pdf].

[34] John Bennett, "Commission: U.S. Should Push Beijing to up Pressure on North Korea," *Inside the Pentagon*, June 17, 2004.

satellite video and images to direct their ground attacks against U.S. and coalition troops.[35]

Some observers have stated that terrorist groups, through use of the Internet, are now challenging the monopoly over mass communications that both state-owned and commercial media have long exercised. A strategy of the terrorists is to propagate their messages quickly and repeat them until they have saturated cyberspace. Internet messages by terrorist groups have become increasingly sophisticated through use of a cadre of Internet specialists who operate computer servers worldwide. Other observers have also stated that al-Qaeda now relies on a Global Islamic Media Unit to assist with its public outreach efforts.[36]

Law and Proportionality for Information Operations

The new U.S. Cyber Command reportedly will follow the law of Armed Conflict, meaning a response taken after receiving an electronic or cyber attack will be scaled in proportion to the attack received, and distinctions will be maintained between combatants and civilians.[37] However, protection against attack through cyberspace is a new task for the military, and the offensive tools and other capabilities used by DOD to stage retaliatory strikes against enemy systems are highly classified. Experience has shown that a reactive defense is not very effective against increasingly powerful and rapid malicious cyber attacks, or against other malicious activity using the electromagnetic spectrum. A more effective defense against these attacks is to incorporate predictive, active, and pre-emptive measures that allow DOD defenders to prevent, deflect, or minimize the efforts of the attacker.

---

[35] Daniel Helmer, *The Poor Man's FBCB2: R U Ready 4 the 3G Celfone?*, Armor, Nov/Dec 2006, p.7.

[36] Jacquelyn S. Porth, *Terrorists Use Cyberspace as Important Communications Tool*, U.S. Department of State, USInfo.State.Gov, May 5, 2006, [http://usinfo.state.gov/is/Archive/2006/May/08-429418.html].

[37] The Law of Armed Conflict (LOAC) is a part of public international law that regulates the conduct of armed hostilities between nations, and is intended to protect civilians, the wounded, sick, and shipwrecked. LOAC training for U.S. military is a treaty obligation for the United States under provisions of the 1949 Geneva Conventions. Also, under 18 U.S. Code 2441, war crimes committed by or against Americans may violate U.S. criminal law. James Baker, *When Lawyers Advise Presidents in Wartime,* Naval War College Review, Winter 2002, Vol. LV, No. 1. Terry Kiss, ed., Law of Armed Conflict, Air University Library, Maxwell AFB, Jan 2005, [http://www.au.af.mil/au/aul/bibs/loacots.htm]. Josh Rogin, *Air Force to Create Cyber Command*, FCW.COM, Nov 13, 2006, [http://www.fcw.com/article96791-11-13-06-Print&printLayout].

Cyberwarrior Education

As more U.S. military systems become computerized and linked to networks, there is a growing need for qualified Electronic Warfare operators.[38] Each year, DOD conducts a Cyber Defense Exercise, where teams of students from the nation's military academies advance their cyber skills in practice competition where they deliberately hack into test networks, and also protect these test networks against intrusions by other teams. However, DOD must attract, train, and retain skilled information technology professionals beyond those enrolled in the military academies.

In an attempt to solve this problem, the Air Force Research Laboratory (AFRL) Cyber Operations Branch offers a 10-week summer program each year for university students, consisting of intensive studies in cyber security. The Advanced Course in Engineering (ACE) Cyber Security Boot Camp has been held at Rome, NY for the past 4 years, and involves between 40 and 60 student applicants from Air Force and Army pre-commissioning programs, some National Science Foundation Cyber Corps Fellows, and some civilian college students. For 2006, the theme was "Cybercraft", described as a non-kinetic weapon platform that seeks dominance in cyberspace, corresponding to the new mission of the Air Force to 'fly and fight in air, space, and cyberspace', according to program director Dr. Kamal Jabbour. Students study legal and policy issues, cryptography, computer network defense and attack, steganography, and analysis of malicious code. ACE students also spend an average of three days per week in internships at the Air Force Research Laboratory, or with local industry partners, and participate in officer development activities. The faculty for ACE is drawn from Syracuse University, West Point, and Norwich University.

DHS and the National Science Foundation (NSF) have recognized the ACE program as an official internship program for Federal Cyber Service Scholarship for Service (SFS) program. The SFS program seeks to increase the number of skilled students entering the fields of information assurance and cyber security by funding universities to award 2-year scholarships in cyber security. Graduates are then required to work for a federal agency for two years. Recent ACE graduates are now working at the Air Force Office of Special Investigations, the AFRL, and the NSA.

Also, as a result of ACE summer program success with college students, in September 2006, Syracuse University developed a special cyber security course to be offered in 12 high schools in New Your State. Currently, Syracuse University offers 29 introductory cyber security courses in 148 high schools throughout New York, New Jersey, Maine, Massachusetts, and Michigan. High school students who successfully complete the cyber security courses can receive Syracuse college credits in computer science and engineering.

---

[38] Patience Wait, *Army Shores up EM spectrum skills,* Government Computer News, Mar 19, 2007.

Policy Issues

Potential oversight issues for Congress may include the following areas.

Could provocative actions, for example, intelligence gathering by the U.S. military that involves using intrusive cyber or electronic warfare tools to monitor enemy system activity, or copy important data files, be challenged by other nations as a violation of the law of Armed Conflict? Exploratory intrusions by U.S. military computers to gather intelligence may provoke other strong or unexpected responses from some countries or extremist groups that are targeted for monitoring by DOD.

Several questions also may arise when conducting a retaliatory cyber or electronic warfare counterstrike: (1) if the attacker is a civilian, should the attack be considered a law enforcement problem rather than a military matter?; (2) if a U.S. military cyberattack against a foreign government also disables civilian infrastructure, can it be legally justified?; (3) how can the military be certain that a targeted foreign computer system has not been innocently set up to appear as an attacker by another third party attacker?

Some observers have stated that success in future conflicts will depend less on the will of governments, and more on the perceptions of populations, and that perception control will be achieved and opinions shaped by the warring group that best exploits the global media[39]. As a result of the increasingly sophisticated use of networks by terrorist groups and the potentially strong influence of messages carried by the global media, does DOD now view the Internet and the mainstream media as a possible threat to the success of U.S. military missions? How strongly will U.S. military PSYOP be used to manipulate public opinion, or reduce opposition to unpopular decisions in the future?

Another emerging issue may be whether DOD is legislatively authorized to engage in PSYOP that may also affect domestic audiences.[40] DOD Joint Publication 3-13, released February 2006, provides current doctrine for U.S. military Information Operations, and explains the importance of achieving information superiority.[41] However, the DOD Information Operations Roadmap, published October 2003, states that PSYOP messages intended for foreign audiences increasingly are consumed by the U.S. domestic audience, usually because they can be re-broadcast through the global media. The Roadmap document states that, "...the distinction between foreign and domestic audiences becomes more a question of USG (U.S. Government) intent rather than information dissemination practices (by DOD)."[42]

---

[39] Maj. Gen. Robert Scales (Ret), *Clausewitz and World War IV*, Armed Forces Journal, July 2006, p.19.

[40] Psychological Operations are authorized for the military under Title 10, USC, Subtitle A, Part I, Chapter 6, Section 167.

[41] DOD Joint Publication 3-13, Information Operations, Feb 13, 2006, [http://www.dtic.mil/doctrine/jel/new_pubs/jp3_13.pdf].

[42] DOD Information Operations Roadmap, October 30, 2003, p.26. [http://www.gwu.edu/~nsarchiv/NSAEBB/NSAEBB177/info_ops_roadmap.pdf]

This may be interpreted to mean that DOD has no control over who consumes PSYOP messages once they are re-transmitted by commercial media.

Current Legislation

Currently, there are no outstanding bills in the 110th Congress linked to Information Operations or Cyberwarfare.

crsphpgw

GalleryWatch.com
http://www.crsdocuments.com
Penny Hill Press