Order Code RL31787

CRS Report for Congress
Received through the CRS Web

Information Warfare and Cyberwar: Capabilities and Related Policy Issues

Updated July 19, 2004

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

Information Warfare and Cyberwar: Capabilities and Related Policy Issues

Summary

This report describes the emerging areas of information warfare and cyberwar in the context of U.S. national security. It assesses known U.S. capabilities and plans, and suggests related policy issues of potential interest to Congress. This report will be updated to accommodate significant changes.

Military planning is shifting away from the Cold War view that power is derived from platforms, and more toward the view that combat power can be enhanced by communications networks and technologies that control access to, and directly manipulate information. As a result, information itself is now both a tool and a target of warfare.

As concepts emerge, new uses of technology to disrupt the flow of information to affect the ability or willingness of an adversary to fight is referred to by several names: information warfare, cyberwar, and netwar. The U.S. Department of Defense uses the term "Information Operations," and has grouped related activities into five core capabilities: Psychological Operations, Military Deception, Operational Security, Computer Network Operations, and Electronic Warfare. Some weapons used for IO are referred to as "non-kinetic," and include high power microwave (HPM) or directed electromagnetic energy weapons (EMP) that, in short pulses, can overpower and permanently degrade computer circuitry, or in other applications, can cause temporary physical discomfort.

Several public policy issues that Congress may choose to consider include whether the United States should:

- encourage or discourage international arms control for cyberweapons, as other nations increase their cyber capabilities;
- modify U.S. cyber-crime legislation to conform to international agreements that make it easier to track and find cyber attackers;
- engage in covert psychological operations affecting audiences within friendly nations;
- encourage or discourage the U.S. military to rely on the civilian commercial infrastructure to support part of its communications, despite vulnerabilities to threats from possible high-altitude electromagnetic pulse (HEMP) or cyber attack;
- create new regulation to hasten improvements to computer security for the nation's privately-owned critical infrastructure; or
- prepare for possible legal issues should the effects of offensive U.S. military cyberweapons, or electromagnetic pulse weapons spread to accidentally disable critical civilian computer systems, or disrupt systems located in other non-combatant countries.

Contents

Information Warfare and Cyberwar: Capabilities and Related Policy Issues

Introduction

Background

Control of information has always been part of military operations, and new technologies now offer some important strategic advantages. New electronic and computer technologies enable the U.S. military to link remote sensors to decision makers and combat personnel in order to (1) create a higher level of shared awareness, (2) better synchronize command, control, and intelligence, and (3) translate information superiority into combat power. In addition to a nuclear deterrence, the U.S. Strategic Command reportedly now sees electronic warfare used to disable an adversary's computers, psychological warfare used to manipulate an adversary's perception, and other components of information warfare as major tools for deterring attacks in the future.[1]

However, new uses of technology for information warfare also create new national security vulnerabilities and new policy issues, including (1) possible international arms control for cyberweapons; (2) international cooperation for pursuit of cyber terrorists and other cyber attackers; (3) psychological operations affecting friendly nations; (4) possible national security vulnerabilities resulting from military dependence on the civilian computer infrastructure and computer software products; (5) the need to raise the computer security awareness of the civilian community; and (6) possible accusations of war crimes if offensive military cyberweapons severely disrupt critical civilian computer systems, or systems of other non-combatant nations.

Purpose

This report describes Department of Defense capabilities for conducting military information warfare operations, and gives an overview of related policy issues. Topics such as computer crime, disruption of financial organizations, digital piracy of intellectual property, and Internet industrial espionage provide examples of areas where civilian infrastructure vulnerabilities may be targeted by military information warfare operations. These topic areas are numerous, and this report limits discussion to only a few.

---

[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].

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 sensors, computers, networks, and databases.

In previous warfare, adversaries indirectly influenced the information of an adversary (e.g., by dropping dummies from airplanes to simulate attack by live paratroopers or by sending false messages intended for interception), so as to mislead.[2] However, with current digital technology, opponents can now act directly upon the stored bits that comprise the actual information itself.

Information Warfare

The Department of Defense (DOD) technical view of information warfare is that information itself is now a realm, a weapon, and a target. An information-based attack includes any unauthorized attempt to copy data, or directly alter data or instructions. Information warfare involves much more than computers and computer networks. It is comprised of operations directed against information in any form, transmitted over any media, including operations against information content, its supporting systems and software, the physical hardware device that stores the data or instructions, and also human practices and perceptions. [3]

DOD Information Operations

The DOD term for military information warfare is "Information Operations" (IO). IO is conducted during time of crisis or conflict to affect adversary information and information systems while defending one's own information and systems.[4]

IO during a time of conflict, is any attack intended to disrupt or exploit an information system or information flow, regardless of the means. An attack may use information as a weapon to create deception, or influence the psychology of an adversary, or an attack may disrupt the electrical circuits that support an information system. Therefore, IO enables the U.S. military to influence an adversary's will to fight while also protecting our forces and our will.

Examples may include (1) using leaflets or broadcasts to influence opinions and actions of a target audience, (2) creating false appearances of military strength or weakness to mislead an adversary, (3) blocking access to information that might

---

[2] Anthony C. Brown, *Bodyguard of Lies*, N.Y. Quill/William Morrow, 1991.

[3] Dorothy Denning, *Information Warfare and Security*, Addison-Wesley, 1999, pp. 9-19.

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

prove useful to an adversary, (4) sending malicious computer programs to attack and disrupt adversary computer software, and (5) creating directed energy electromagnetic pulses to disrupt or destroy targeted military computer hardware or networks.

Bombing a telephone switch facility, or short-circuiting the telephone switch network, or destroying only the telephone switch facility software, are all examples of information warfare. Other terms such as knowledge-based war, cyberwar, netwar, command and control war, and electronic warfare are sometimes used interchangeably with information warfare.[5]

Information Superiority

The administration has stated that DOD must transform to achieve a fundamentally joint force capable of rapid decision superiority.[6] Decision Superiority is the DOD term used to describe a competitive advantage in the cognitive realm, that is facilitated by Information Superiority. Information Superiority is a DOD term that describes a competitive advantage that enables a military commander to surprise and out maneuver an enemy. Information Superiority supports better coordination of battlefield units, and enables each individual battlefield commander to make better-informed decisions more quickly than an adversary. DOD Information Operations capabilities help achieve Information Superiority leading to Decision Superiority, and also help support information age battlefield concepts related to Network Centric Warfare.[7]

DOD Information Operations Capabilities

DOD has identified five core capabilities for conduct of information operations (IO); (a) Psychological Operations, (b) Military Deception, (c) Operations Security, (d) Computer Network Operations, and (e) Electronic Warfare. These IO capabilities are intended to influence foreign decision makers and protect friendly decision-making, and to affect or defend the electromagnetic spectrum, information systems, and information that supports decision makers, weapon systems, command and control, and automated responses. Other observers have included additional capabilities for IO: Counterintelligence and Public Affairs capabilities as part of Influence Operations; and, Electronic Attack, Electronic Protect, and non-lethal

---

[5] Ronald Fogleman and Sheila Widnall, "Cornerstones of Information Warfare," 2002, Dec. 9, 1995 [http://www.af.mil/lib/corner.html].

[6] For more information, see CRS Report RL32238, *Defense Transformation: Background and Oversight Issues for Congress.*

[7] For more information, see CRS Report RL32411, *Network Centric Warfare: Background and Oversight Issues for Congress.*

suppression of enemy air defenses (SEAD) capabilities as part of Electronic Combat.[8] The five DOD core capabilities for IO are described below.

Psychological Operations (PSYOPS)

PSYOPS is defined by DOD as planned operations to convey selected information and indicators to foreign audiences to influence their emotions, motives, objective reasoning, and ultimately the behavior of foreign governments, organizations, groups, and individuals. The purpose of psychological operations is to induce or reinforce foreign attitudes and behavior favorable to the originator's objectives.[9] For example, during the Operation Iraqi Freedom (OIF), leaflets were dropped carrying the official message, "Any war is not against the Iraqi people, but is to disarm Mr. Hussein and end his government." Similar broadcast messages were sent from Air Force EC-130E aircraft, and from Navy ships operating in the Persian Gulf. U.S. forces also sent a barrage of email, faxes, and cell phone calls to numerous Iraqi leaders encouraging them to abandon support for Saddam Hussein.

However, the Al Jazeera news network, based in Qatar, currently beams its messages to over 35 million viewers in the Middle East, and is considered by many to be a market competitor for U.S. Psyops. 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 Al Jazeera.[10]

Executive Order 13283, signed by President George W. Bush on January 21, 2003, established within the White house the Office of Global Communications (OGC).[11] The Executive Order states that the new office is authorized to send teams of "communicators" to "areas of high global interest and media attention." It is currently studying ways to reach Muslim audiences directly through radio and TV, to counter anti-American sentiments. The new office will not use disinformation, but reportedly will shine a light on disinformation by others.[12]

---

[8] Air Force, *Operation Iraqi Freedom Information Operations Lessons Learned: First Look*, AFC2ISRC/CX, July 23, 2003 [http://www.cadre.maxwell.af.mil/warfarestudies/iwac/Downloads/IW250%20Reading.doc].

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

[10] 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].

[11] "Presidential Documents, Title 3 - The President - Establishing the Office of Global Communications," *Federal Register*, Vol. 68, no. 16, Jan. 24, 2003.

[12] OGC has been up and running since July 2002, working to get the Administration's message out to foreign news media outlets. Tucker Eskew stated that, "(The President) knows that we need to communicate our policies and values to the world with greater clarity and through dialogue with emerging voices around the globe." Scott Lindlaw, "New Office Aims to Bolster U.S. Image," *AP Online*, Feb. 11, 2003.

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, intentions, and operations, thereby causing the adversary to take specific actions (or inactions) that will contribute to the success of the friendly military operation. For example, by dropping dummy figures resembling parachutists from airplanes at night, an enemy might be tricked into moving or rearranging their forces to ward off a false attack.

As an example of deception during OIF, Iraqi forces often hid weapons and munitions inside schools, mosques and private homes. Many tons of military equipment, including airplanes, were also found buried beneath the Iraqi sand. Also, during OIF, the Navy deployed the Tactical Air Launched Decoy system to divert fire from Iraqi air defenses away from real combat aircraft.

Operational Security (OPSEC)

OPSEC is defined as a process of identifying and analyzing information that is critical to friendly operations to; (a) identify which information can be observed by adversary intelligence systems, (b) determine indicators that hostile intelligence systems might piece together to derive critical information in time to be useful to adversaries, and (c) select and execute measures that eliminate or reduce the vulnerability of friendly actions to adversary exploitation. For example, during OIF, US forces were warned to remove certain publicly available information from DOD websites, so that Iraqi forces could not exploit sensitive but unclassified information.

OPSEC is closely related to Information Assurance (IA), which the business community refers to as "computer security". However OPSEC differs from IA because it does not include planning for business recovery after a disaster.

Computer Network Operations (CNO)

Computer Network Operations are comprised of two specific yet complementary mission areas; Computer Network Defense and Computer Network Attack.[13] CNO involves the ability to attack and disrupt enemy computer networks, protect military information systems, and exploit enemy computer networks through intelligence collection. CNO is outlined in DOD Directive 3600.1 "Information Operations," and is composed of methods for attack, defense and exploitation of information.

Computer Network Attack (CNA). CNA is defined as operations to disrupt, deny, degrade, or destroy information resident in computers and computer networks, or the computers and networks themselves. CNA relies on interpreted signals in a data stream to execute an attack, while Electronic Warfare relies more on the power

---

[13] US Strategic Command Fact File [http://www.stratcom.af.mil/factsheetshtml/jtf-cno.htm].

of electromagnetic energy. The following are examples of each type of operation; sending a digital signal stream through a network to a central processing unit that instructs the controller to interrupt the power supply is CNA, while sending a high voltage surge through the electrical power cable to short out the power supply is Electronic Warfare.

Computer Network Defense (CND). CND is defined as defensive measures to protect and defend information, computers, and networks from disruption, denial, degradation, or destruction. It utilizes security measures that seek to keep the enemy from learning about U.S. military capabilities and intentions. CND includes actions taken to protect, monitor, analyze, detect and respond to unauthorized activity within DOD information systems and networks. Defensive information warfare involves measures intended to prevent, detect, and subvert an enemy's direct, or indirect, actions against our information systems. CND focuses on detecting or stopping intrusions, whereas OPSEC focuses on identifying and reducing possible vulnerabilities or exposures that might benefit an intruder.

During OIF there were no reported successful penetrations of DOD systems attributable to Iraqi forces.[14]

Computer Network Exploitation (CNE). CNE is an area of Information Operations that is not yet clearly defined within DOD. Information exploitation involves espionage, that in the case of IO, is usually performed through network tools that penetrate adversary systems to return information or copies of files that singly, or collectively, enable the military to gain an advantage over the adversary. Tools used for CNE are similar to those used for CNA, but configured for different objectives.

While CNA by itself may be considered qualitatively an act of war, it would usually precede a period of careful and covert CNE to determine possible vulnerabilities of an adversary's computers and networks as a first step toward launching a CNA operation. In addition, CND is made more effective if an adversary's technical capabilities are known in advance, or if the origin of suspected probes against U.S. computers can be accurately determined. CNE is also used to acquire this information. Therefore, reconnaissance, probing, and scanning of an adversary's computers and networks may all be used as part of CNA and CND.

Electronic Warfare (EW)

EW is defined as any military action involving the direction or control of electromagnetic spectrum energy to deceive or attack the enemy. EW has been an important component of military air operations since the earliest days of radar, and engineers and scientists have evolved the concepts to now include new stealth

---

[14] 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].

techniques.[15] High power electromagnetic energy can also be used as a tool to overload or disrupt the circuitry of electronic equipment. For example, a nuclear, or specially-designed chemical explosion, can generate a strong electromagnetic pulse. A short energy pulse may not necessarily be directly harmful to humans or physical structures, however, it can overload or destroy nearby electronic devices, such as computers, radios, telephones, and almost anything that uses transistors, circuits, and wiring.

EW can also take the form of a passive activity, such as location, interception, and analysis of enemy radar signals so vulnerabilities can be identified and exploited. As an example of EW, on one occasion during OIF, the Iraqis employed 6 GPS jammers, intended to confuse the targeting systems of U.S. weaponry. However, within 2 nights, all jamming stations were destroyed by combat aircraft, using the jamming signals to help direct weapons onto the Iraqi targets.[16]

Cyberweapons, Non-Kinetic Weapons, and Electronic Warfare

IO activities include (a) attempts to infiltrate networks, (b) attempts to steal or sabotage information, and (c) attempts to paralyze high technology systems. Tools for conducting these operations include cyberweapons, which are computer programs capable of disrupting the data storage or processing logic of enemy computers. Other IO tools used for Electronic Warfare include weapons capable of jamming, overpowering, or degrading enemy communications, telemetry, or circuitry. "Non-kinetic" is a term that is sometimes used to describe the group of non-explosive weapons with the above capabilities. This includes some weapons designed to emit directed electromagnetic energy that, in short pulses, may disable computer circuitry, or in other applications, may cause temporary physical discomfort.

For example, rather than using explosives, a non-kinetic weapon might disable an approaching enemy missile by directing a High Power Microwave (HPM) beam that burns out the circuitry and stops its attack capability, or by sending a false telemetry signal that misdirects the targeting computer.[17] Currently, a reusable directed-energy weapon is being designed for use on the Joint Unmanned Combat Air System, which could remain stealthy and airborne for extended periods while repeatedly focusing energy beams to disable numerous targets. Also, in a different application, a microwave weapon has been tested that can be used for controlling or

---

[15] For more information, see CRS Report RL30841, *Airborne Electronic Warfare: Issues for the 107th Congress*, and CRS Report RL30639, *Electronic Warfare: EA-6B Aircraft Modernization and Related Issues for Congress*.

[16] 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].

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

dispersing crowds without killing people. This weapon reportedly causes a painful burning sensation on the skin, but no long-term damage.[18]

During OIF, many Iraqi command bunkers and suspected chemical-biological weapons bunkers were deeply buried underground and proved difficult to disable using conventional explosives. However, new HPM weapons were reportedly considered for possible use in attacks against these targets because the numerous communications and power lines leading into the underground bunkers offered pathways for conducting powerful surges of electromagnetic energy that could destroy the computer equipment inside.[19]

Cyberweapons include (a) offensive attack tools, such as viruses, Trojan horses, denial-of-service attack tools; (b) "dual use" tools, such as port vulnerability scanners, and network monitoring tools; and, (c) defensive tools, such as encryption and firewalls. Offensive tools are associated with computer network attack (CNA) directed against an enemy's network, while defensive tools are used mainly to protect against attack. Dual-use tools are used either offensively or defensively, depending on the intention of the user. Recent military IO programs tested the capability for U.S. forces to secretly enter an enemy computer network and monitor what their radar systems could detect. Further experiments tested the added capability for U.S. forces to take over the enemy computers and start manipulating their radar to show false images.[20]

During OIF, U.S. and coalition forces reportedly did not carry out comprehensive computer network attacks against Iraqi systems. Even though comprehensive IO plans were prepared in advance, several DOD officials reportedly stated that top-level approval for several computer attack missions was not granted until it was too late to carry them out to help achieve war objectives.[21] U.S. forces reportedly may have rejected launching a planned cyber attack against Iraqi financial computers because Iraq's banking network is connected to a financial communications network located in Europe. According to Pentagon sources, an information warfare attack 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

---

[18] David Ruppe, "Directed-Energy Weapons: Possible U.S. Use Against Iraq Could Threaten International Regimes," *Global Security Newswire*, August 16, 2002 [http://www.globalsecurity.org/org/news/2002/020816-dew.htm] .

[19] Will Dunham, "U.S. May Debut Secret Microwave Weapon versus Iraq," *Reuters*, February 2, 2003 [http://www.globalsecurity.org/org/news/2003/030404-ebomb01.htm].

[20] 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.

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

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.[22]

Cyberweapons are becoming easier to obtain, easier to use, and more powerful. In a 1999 study, the National Institute of Standards and Technology (NIST) found that many newer attack tools, available on the Internet, can now easily penetrate most networks, and many others are effective in penetrating firewalls and attacking Internet routers. Other tools allow attacks to be launched by simply typing the Internet address of a designated target directly into the attack-enabling website.[23]

Current DOD Command Structure for Information Operations

The U.S. Strategic Command (USSTRATCOM), a unified combatant command, is the command and control center for U.S. strategic forces and controls military space operations, computer network operations, information operations, strategic warning and intelligence assessments as well as global strategic operations planning. Within USSTRATCOM, the Joint Information Operations Center (JIOC) has responsibility for managing information warfare activities, including the integration of operations security, psychological operations, military deception, and electronic warfare throughout the planning and execution phases of the operations.[24] Within the JIOC, the Joint Task Force-Global Network Operations (JTF-GNO), coordinates and directs the defense of DOD computer systems and networks, and, when directed, conducts computer network attack in support of combatant commanders' and national objectives.[25]

As the U.S. military increasingly builds up its computer network infrastructure through the Global Information Grid, DOD reportedly wants the command structure to better reflect the importance of computer network operations. The new JTF-GNO handles both network defense and network management. JTF-GNO exercises operational control of the Global Information Grid (GIG) for Network Operations issues which may potentially affect availability, protection, or delivery of information for multiple combatant commands, services, or agencies. JTF-GNO has responsibility to ensure that GIG services are always available to the warfighter. JTF-

---

[22] 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].

[23] WarRoom Research, a private company specializing in information espionage, reported in 1999 that 32 percent of 102 Fortune 500 companies surveyed had an information counter-attack capability. Approximately 30 new network attack tools are created each month, and most are freely available for download from hundreds of hacker-maintained websites by simply typing the phrase "hacking tools" into any Internet search engine. Dorothy Denning, "Reflections on Cyberweapons Controls," *Computer Security Journal*, XVI, 4, Fall, 2000, p.43-53.

[24] "U.S. Strategic Command Facts and Information," March 2004, [http://www.stratcom.mil/factsheetshtml/Joint%20Info%20Operations%20Center.htm].

[25] See USSTRATCOM Fact File [http://www.stratcom.af.mil/factsheetshtml/jtf-cno.htm].

GNO merges with the Global Network Operations and Security Center, the DoD Computer Emergency Response Team, and the Global SATCOM Support Center to for a single entity called the Global NetOps Center (GNC). The GNC is the technical implementation arm of JTF-GNO, and the nerve center for DOD global network operations.[26]

The National Defense Authorization Act for Fiscal Year 2004 (PL108-136) authorizes appropriations for FY2004 military activities. Under this law, the Secretary of Defense is directed to submit to the congressional defense committees and the Permanent Select Committee on Intelligence of the House of Representatives and the Select Committee on Intelligence of the Senate a report on the preparation for and conduct of military operations under Operation Iraqi Freedom from March 19, 2003, to May 1, 2003, including the effectiveness of information operations and a description of technological and any restrictions on the use of psychological operations capabilities. As of the date of this publication, the above report has not yet been made available.

Guidelines for DOD use of Cyberweapons

In February 2003, the Bush administration announced plans to develop national-level guidance for determining when and how the United States would launch computer network attacks against foreign adversary computer systems. The guidance, known as National Security Presidential Directive 16 (classified), was signed in July 2002, and is intended to clarify circumstances under which an attack would be justified, and who has authority to launch a computer attack.

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 cyberweapons. Officials have stated they are proceeding cautiously, since a cyberattack could have serious cascading effects, perhaps causing major disruption to civilian systems in addition to the intended military computer targets.[27]

Policy Issues

Potential oversight issues for Congress include the following:

- possible effects of international arms control for cyberweapons;
- the need for international cooperation for pursuit of cyber terrorists and other cyber attackers;

---

[26] Major Larry Cox, *The Changing Face of Network Operations, Intercom*, Journal of the Air Force C4 Community, February 2004, p. 10, [http://public.afca.af.mil/Intercom/2004/FEB/FEB04_02.pdf].

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

- use of psychological operations that may affect friendly nations;
- possible national security vulnerabilities resulting from military dependence on the civilian computer infrastructure;
- the need to raise the computer security awareness of the civilian population, and;
- possible legal issues resulting from U.S. military use of cyberweapons that may also disable critical civilian computer systems, or computer systems in other countries.

International Arms Control for Cyberweapons

Malicious computer code that attacks information systems may in theory be treated as a weapon of war within the scope of the laws of armed conflict, and attempts are now being made by some international organizations to classify and control malicious computer code.[28] Should the United States adopt a position to encourage or discourage international controls for weapons in cyberspace, as other nations, such as Iraq and China, increase their cyber capabilities?

DOD has not yet developed a policy regarding international controls for cyberweapons, however, the United States remains concerned about future capabilities for foreign nations to develop their own effective capabilities for computer espionage and computer network attack.[29] Officials have reportedly stated that other nations, rather than terrorist groups, pose the biggest threat to U.S. computer networks.[30] For example, the Chinese military is enhancing its information warfare capabilities, according to the Defense Department's annual report to Congress on China's military prowess.[31] The report finds that China is placing

---

[28] In 1998 and 1999, Russia proposed that the First Committee of the U.N. explore an international agreement on the need for arms controls for information warfare weapons. Denning, "Reflections on Cyberweapons Controls," *Computer Security Journal*, XVI, 4, Fall, 2000, p. 43-53. The 2002 Council of Europe's Cybercrime Convention, and the G-8 Government-Industry Conference on High Tech Crime have also sought international agreement on ways to classify and control malicious computer code. Andrew Rathmell, "Controlling Computer and Network Operations," *Information and Security*, vol. 7, 2001, pp. 121-144.

[29] A US Air Force-sponsored workshop held in March 2000 concluded that international efforts to tackle cybercrime and cyberterrorism "could hinder US information warfare capabilities, thus requiring new investments or new research and development to maintain capabilities." USAF Directorate for Nuclear and Counter proliferation and Chemical and Biological Arms Control Institute, *Cyberwarfare: What Role for Arms Control and International Negotiations?* (Washington, D.C., March 20, 2000).

[30] Mickey McCarter, "Computer Offensive," *Military Information Technology*, November 15, 2002 [http://www.mit-kmi.com/print_article.cfm?DocID=51] .

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

specific emphasis on the ability to perform information operations designed to weaken an enemy force's command and control systems.[32]

International Cooperation for Pursuit of Cyber Attackers

An emerging issue is whether the United States should pursue international agreements to harmonize cyber-crime legislation, and also deter cyber-crime through tougher criminal penalties. It is often technically difficult to trace back to the source of a computer attack, because an attacker can hide their location by hopping from one computer system to another, sometimes taking a path that connects networks and computers in many different countries. Pursuit to identify the attacker involves a trace back through networks that may require the cooperation of computer systems administrators or Internet Service Providers in the different nations involved. Sometimes, computer network defense also requires the use of computer espionage to determine whether an adversary has been sending out computer probes in preparation for launching a follow-on attack. In either case, the technical problems of pursuit or detection are made increasingly complex if one or more of the nations involved has a legal policy or political ideology that conflicts with that of the United States.[33]

The Administration has encouraged United States adoption of the Council of Europe Cybercrime Treaty.[34] This Treaty would require participating nations to update their laws to reflect computer crimes such as unauthorized intrusions into networks, the release of worms and viruses, and copyright infringement. The Treaty also includes arrangements for mutual assistance and extradition among participating nations. As of the date of this report, the Treaty has been ratified by Albania, Croatia, Estonia, Hungary, Lithuania and Romania.

The Administration has stated that the Treaty will help deny a safe haven to criminals and terrorists who can cause damage to U.S. interests from abroad using computer systems.[35] However, while some observers say that international cooperation is important for defending against cyber attacks and improving global cybersecurity, others point out that the Treaty also contains a questionable addition that would require nations to imprison anyone guilty of "insulting publicly, through a computer system" certain groups of people based on characteristics such as race or

---

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

[33] In Argentina, a group calling themselves the X-Team, hacked into the website of the Supreme Court of Argentina in April 2002. The trial judge stated that the law in his country covers crime against people, things and animals but not websites. The group on trial was declared not guilty of breaking into the website. Paul Hillbeck, "Argentine Judge Rules in Favor of Computer Hackers," February 5, 2002 [http://www.siliconvalley.com/mld/siliconvalley/news/editorial/3070194.htm].

[34] The Council of Europe is composed of 45 Central and Eastern European countries, with the United States granted non-voting, observer status. For more information, see CRS Report RS21208, *Cybercrime: The Council of Europe Convention*.

[35] Declan McCullagh, "Bush Pushes for Cybercrime Treaty," *CnetNews.com*, November 18, 2003 [http://news.com.com/2102-1028_3-5108854.html?tag=st.util.print].

ethnic origin. The U.S. Department of Justice has stated that such an addition would violate of the First Amendment's guarantee of freedom of expression. The Electronic Privacy Information Center has also objected to the addition, saying that it would "would create invasive investigative techniques while failing to provide meaningful privacy and civil liberties safeguards."[36]

In November 2003, the Administration submitted the Treaty to the U.S. Senate for ratification. On June 17, 2004, the Senate Committee on Foreign Relations held a hearing to discuss the Treaty. As of the date of this report, the Treaty has not yet been ratified by a two thirds vote of the Senate.

Psychological Operations Affecting Friendly Nations

When targeting hostile countries, PSYOPS can include broadcasting from airborne radio and television stations, or dropping leaflets. Psychological operations also include routine public relations work to increase civilian support in friendly nations like Colombia, the Philippines, or Bosnia, whose governments have sometimes relied on American troops.[37]

An apparent issue is whether the Department of Defense is legislatively authorized to engage in covert psychological operations involving friendly nations, and whether any such operations would likely prove to be counterproductive.[38] DOD Directive 3600.1 is the current guide for U.S. military Information Operations.[39] However, in early December 2002 media reports indicated that DOD personnel had drafted what some described as a "secret amendment" to Directive 3600.1, involving covert operations that would influence public opinion and policy makers in friendly and neutral countries. The proposed 2002 amendment reportedly suggested that PSYOPS funds might be used to publish stories favorable to American policies, or hire outside contractors without obvious ties to the Pentagon to organize rallies in support of Administration policies. Press reports suggested that the proposal was designed to counter the influence of organizations that allegedly had developed into breeding grounds for Islamic militancy and anti-Americanism in

---

[36] Declan McCullagh, "Senate Debates Cybercrime Treaty," *CnetNews.com*, June 18, 2004, [http://news.com.com/2102-1028_3-5238865.html?tag=st.util.print] .

[37] Admiral James Ellis, commander of Allied Forces in Southern Europe during Operation Allied Force, contrasted the NATO and Serb media campaigns by observing that "the enemy was much better at this public information and public affairs than we were . . . and far more nimble. The enemy deliberately and criminally killed innocents by the thousands, but no one saw it. . . . We accidentally killed innocents, sometimes by the dozens, and the world watched on the evening news. We were continuously reacting, investigating, and trying to answer 'how could this happen?'" Gary Pounder, "Opportunity Lost: Public Affairs, Information Operations, and the Air War against Serbia," *Aerospace Power Journal*, XIV, 2, 2000, pp. 56-77.

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

[39] DOD Directive 3600.1 was originally created in December 1992, and an unclassified version was published in 1995, which was subsequently revised in October 2001, [http://www.iwar.org.uk/iwar/resources/doctrine/DOD36001.pdf].

certain areas of the Middle East, Asia, and Europe.[40] However, since December 2002, DOD has reportedly stepped back from this proposal, leaving the Department of State and CIA with responsibility for strategic PSYOPS.[41]

The new Office of Global Communications, created in January, 2003 by Executive Order 13283, was established to promote the spread of truthful and accurate messages to others about U.S. policy, and avoid disinformation.[42] The new OGC office replaces an earlier effort, terminated by the administration, to build public support overseas for the war on terrorism.[43] OGC has coordinated themes calling for the disarmament of Saddam Hussein, and the office also coordinated efforts to reveal disinformation and propaganda coming from the Iraqi regime, through distributing publications such as "Apparatus of Lies: Saddam's Disinformation and Propaganda, 1990-2003." Currently, OGC is working with the Department of State to improve worldwide communications about U.S. humanitarian and pro-democracy efforts.

Military Dependence on Satellites and the Civilian Infrastructure

Does increased short-term flexibility outweigh apparent security vulnerabilities while DOD continues to rely on parts of the civilian communications infrastructure? Cyber attacks[44], or attacks by high-altitude[45] or other high-energy electromagnetic

---

[40] Thom Shanker and Eric Schmitt, "Threats and Responses: Fight Against Terrorism; Pentagon May Push Propaganda in Allied Nations," *New York Times*, December 16, 2002, section A, p.1.

[41] Michael Knights, *U.S. Psychological Operations Escalate Against Iraq*, International Strategic Studies Association, February 7, 2003 [http://128.121.186.47/ISSA/reports/Iraq/Feb0703.htm].

[42] For a description of the mission of the new Office of Global Communications, see Scott Lindlaw, "New Office Aims to Bolster U.S. Image," *AP Online*, February 11, 2003.

[43] In February 2002, Defense Secretary Donald Rumsfeld disbanded the Pentagon's Office of Strategic Influence (OSI), ending a previous plan to provide news items, and possibly false ones, to foreign journalists to influence public sentiment abroad. Mr. Rumsfeld stated that the OSI was the target of critical editorial comments speculating that the office could be used to spread disinformation. This criticism damaged the reputation and effectiveness of the office, such that it was thought best to shut it down in February. Scott Nance, "Global Propaganda Office Is Reborn," *Defense Week*, 2003, vol. 24, no 4, and Michael Knights, *U.S. Psychological Operations Escalate Against Iraq*, International Strategic Studies Association, February 7, 2003 [http://128.121.186.47/ISSA/reports/Iraq/Feb0703.htm].

[44] Nine of the 13 main Internet DNS servers that managed the Internet at the time, were targeted by cyber attacks and were temporarily disabled, or halted, in October, 2002. Robert Lemos, "Mystery Attacker Swamps .Info Domain System," *Silicon.com*, December 27, 2002 [http://software.silicon.com/security/0,39024655,11036554,00.htm].

[45] A January 2004 briefing given to the Securities Industry Automation Corporation, by the Congressional Commission to Assess the Threat to the United States from Electromagnetic Pulse Attack, reportedly highlights deficiencies in the U.S. government's readiness to protect against a high-altitude nuclear burst which would emit electromagnetic energy powerful enough to permanently disable many critical infrastructure computers. If the

pulse (EMP) weapons that are directed against civilian computers[46] may slow or disable the Internet, or other parts of the civilian communications infrastructure, and may also reduce the effectiveness of some DOD information warfare capabilities.

The U.S. military typically uses its Non-Classified IP Router Network (NIPRNET) for administrative operations, while its Secret IP Router Network (SIPRNET) allows military staff to access classified databases and conduct secure messaging. Seventy percent of NIPRNET traffic is reportedly directed toward the civilian Internet, while SIPRNET traffic has traditionally been isolated from the civilian Internet.[47] Also, the Defense Information Systems Agency (DISA) reported that up to 84 percent of satellite communications bandwidth provided to the Operation Iraqi Freedom theater was supplied by commercial satellites. DOD has reportedly become the single largest customer for commercial satellite services.[48] Therefore, security for part of DOD communications may depend on the level of security found in civilian computers and software[49], and the global commercial communications infrastructure.

Today's high technology military systems increasingly rely on the constellation of Global Positioning System (GPS) satellites, creating a potential vulnerability for U.S. and allied warfighters should GPS signals be degraded or denied. GPS jamming, or corruption of the telemetry signal, could reduce weapon accuracy, resulting in delays in finding targets, an increase in collateral damage, and, in the worst case, fratricide. However, the technologies needed to create a threat to GPS are within the grasp of virtually any nation, and therefore a significant threat could be fielded quickly and inexpensively.[50] The FY2005 budget estimate for R&D for

---

nuclear burst is delivered higher than 40 kilometers above Chicago, computers as far away as Washington, D.C. and New York could possibly be disabled or degraded by the resulting electromagnetic pulse. Daniel G. Dupont, "Panel Says Society At Great Risk From Electomagnetic Pulse Attack," *Inside the Pentagon*, July 15, 2004, p. 1.

[46] See CRS Report RL32411, *Network Centric Warfare: Background and Oversight Issues for Congress.*

[47] Christopher Dorobek and Diane Frank, "DOD May Pull Key Net from the Internet," December 26, 2002, [http://www.fcw.com/fcw/articles/2002/0826/news-net-08-26-02.asp]. DOD officials are increasingly uncomfortable with having the US military NIPRNET reside on the Internet, according to Keith Fuller, DISA chief engineer for information security. Dan Caternniccia, "Marines Tunnel to SIPRNET: Staff Uses Encryption to Access DOD Network," December 9, 2002 [http://www.fcw.com/fcw/articles/2002/1209/tec-tunnel-12-09-02.asp].

[48] Jefferson Morris, "DISA Chief Outlines Wartime Successes," *Federal Computer Week*, "GAO: DOD Needs New Approach to Buying Bandwidth," *Aerospace Daily*, June 6, 2003 and December 12, 2003.

[49] William Jackson, July 5, 2004, "DOD to exclude high-risk software vendors," *GCN.com*, [http://www.gcn.com/cgi-bin/udt/im.display.printable?client.id=gcn2&story.id=26483].

[50] Maj. West Casper, "GPS Vulnerability Testing: Jamming and Interference," *GPS World*, May 1, 2004 [http://www.gpsworld.com/gpsworld/article/articleDetail.jsp?id=95325].

GPS engineering studies and test and evaluation for upgrades and improvements is $40.568 million.[51]

Need to Raise Computer Security Awareness within U.S. Private Sector

The new National Strategy to Secure Cyberspace[52], published February 2003, states that the private sector now has a crucial role in protecting national security because it largely runs the nation's critical infrastructure.[53] Richard Clarke, former chairman of the CIPB, has also stated that the nation's critical infrastructure is vulnerable because cyber-attackers could possibly use the millions of home and business PCs, that are poorly protected against malicious code, to launch debilitating assaults on the nation's critical infrastructure. The plan urges home and small business computer users to install firewalls and anti-virus software, and calls for a public-private dialogue to devise ways that the government can reduce the burden of security on home users and businesses.

However, some observers in the private sector feel the plan does not do enough to ensure that companies will adopt sound security practices, and question whether regulation is needed to supplement, or replace market forces.[54] For example, the plan has been strongly criticized by the congressionally appointed Advisory Panel to Assess Domestic Response Capabilities for Terrorism Involving Weapons of Mass Destruction, chaired by former Virginia Gov. James S. Gilmore III. In its fourth annual publication, the Gilmore Report indicates that public/private partnerships and market forces are not working to protect national security in cyberspace. The Gilmore Report faults the National Strategy Plan for relying too heavily on persuasion to get the private sector to act, and for not holding managers accountable for improving cybersecurity for the systems they own and operate.[55]

---

[51] Program Element 0603421F covers advanced component development and prototyping for the Global Positioning System. Air Force FY2005 Budget Estimates, RDT&E, Volume II, p. 489.

[52] See the full text for National Strategy to Secure Cyberspace at [http://www.us-cert.gov/reading_room/cyberspace_strategy.pdf].

[53] The plan identifies 24 strategic goals and gives more than 70 recommendations on how various communities can secure their part of cyberspace. The communities are broken down into five levels (the home user, the large enterprise, critical sectors, the nation, and the global community). [http://www.whitehouse.gov/pcipb/]

[54] Brian Krebs, "White House Releases Cybersecurity Plan," *Washingtonpost.com*, February 14, 2003.

[55] *Fourth Annual Report to the President and the Congress of the Advisory Panel to Assess Domestic Response Capabilities for Terrorism Involving Weapons of Mass Destruction* [http://www.rand.org/nsrd/terrpanel/terror4.pdf].

Possible Legal Issues Resulting From Use of High Energy Weapons and Cyberweapons

If offensive information warfare operations are ever employed, a lack of precise control over cyberweapons or high energy weapons might involve the U.S. in violations of international law. The effects of using cyberweapons or electromagnetic pulse weapons, if widespread and severe, could arguably exceed customary rules of military conflict, also known as the laws of war.[56]

The effects from United States use of offensive electromagnetic pulse weapons, high-power microwave weapons, and cyberweapons may be difficult to limit or control. Firing electromagnetic weapons may sometimes be physically dangerous to nearby U.S. forces, if they are not properly shielded against the effects of electromagnetic radiation. For example, possible side effects of prolonged exposure to high power microwaves reportedly may cause equipment operators, or other soldiers nearby to experience symptoms of pain, erratic heartbeat, fatigue, weakness, nose bleeds, headaches, or disorientation.[57] The effects of a directed energy weapon attack against enemy military forces may be widespread enough to also disable nearby critical civilian or medical electronic equipment, such as heart pace-makers, or hospital incubators. Similarly, if a computer attack program accidentally spreads through the Internet, it may severely affect other critical non-military computers, possibly the civilian systems that control electricity, water sanitation, or emergency communications. The effects might spread further to affect critical systems in other non-combatant countries. Also, if hackers are able to subsequently copy and reverse-engineer a military computer attack program, it could be used by terrorists against other countries, or even turned against the civilian computer systems in the United States.[58]

The responsibility for protecting the computer-controlled critical infrastructure of the United States against a cyber attack has fallen to each individual federal agency, and to industry owners of the infrastructure. Some maintain that a much more coordinated approach to nationwide computer security may be needed to protect against threats from information warfare attacks.

---

[56] The laws of war are rules that have evolved to resolve practical problems relating to military conflict, such as restraints to prevent misbehavior or atrocities, and have not been legislated by an overarching central authority. Sometimes the introduction of new technology tends to force changes in the understanding of the laws of war. Gary Anderson and Adam Gifford, "Order Out of Anarchy: The International Law of War," *The Cato Journal*, vol. 15, no. 1, p.25-36. For more information, see CRS Report RL31191, *Terrorism and the Law of War: Trying Terrorists as War Criminals before Military Commissions*.

[57] David Ruppe, "Directed-Energy Weapons: Possible U.S. Use Against Iraq Could Threaten International Regimes," *Global Security Newswire*, August 16, 2002 [http://www.globalsecurity.org/org/news/2002/020816-dew.htm].

[58] For more information, see CRS Electronic Briefing Book, *Terrorism*, page on "War Powers and Terrorism: Domestic Legal Considerations," by Jennifer K. Elsea, at [http://www.congress.gov/brbk/html/ebter126.html].

Current Legislation

H.R. 4200, which authorizes appropriations for FY2005 for DOD military activities, was introduced in the House on April 22, 2004. The bill was amended by the House Committee on Armed Services on May 14, 2004, and reported in House Report 109-491. A supplemental report was filed on May 20, 2004, as House Report 108-491, Part II. On June 23, the Senate required an amendment, and on June 24, requested a conference to resolve differences.