Order Code RL31787

Report for Congress
Received through the CRS Web

Information Warfare and Cyberwar: Capabilities and Related Policy Issues

March 14, 2003

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, suggests related policy issues of potential interest to Congress, and tracks relevant current legislation. Additional reports are planned for specific information warfare issues. 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.

An important objective of using technology is to control the flow of information, and through deception or blockage, reduce the ability or willingness of an adversary to fight. As concepts emerge, this new use of technology is referred to by several names; information warfare, cyberwar, and netwar.

The U.S. Department of Defense uses the term "Information Operations" to describe their information warfare activities. DOD has identified five capabilities for conducting military information operations; Psychological Operations, Military Deception, Operational Security, Computer Network Operations, and Electronic Warfare. This report briefly defines each capability and describes the technologies that are used.

Information warfare has raised several public policy issues that congress may choose to consider, including whether the United States should:

- encourage or discourage international arms control for cyberweapons, as other nations increase their cyber capabilities.
- pursue international agreements to harmonize cyber-crime legislation to make it easier to track and find cyber attackers.
- engage in covert psychological operations affecting audiences within friendly nations.
- encourage the U.S. military to rely on the civilian Internet infrastructure to support its communications, despite demonstrated Internet vulnerabilities.
- create new regulation to hasten improvements to computer security for the nation's privately-owned critical infrastructure.
- or, prepare for possible legal issues should U.S. military cyberweapons or electromagnetic pulse energy weapons accidentally disable critical civilian computer systems, or computer 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. The use of new technologies now offers important strategic advantages. New electronic and computer technologies enable the U.S. military to link remote sensors to decision makers and combat personnel to (1) create a higher level of shared awareness, (2) better synchronize command, control, and intelligence, (3) respond faster than their adversaries, and (4) translate information superiority into combat power.

However, new uses of technology also create new national security vulnerabilities and new policy issues. Several policy issues that Congress may ultimately consider include: (1) 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 provides definitions of Department of Defense capabilities for conducting military information warfare, along with an overview of related policy issues. Future CRS reports will discuss information warfare technologies in greater depth, and will examine related national security policy issues more closely.

Although closely linked to problems associated with military information warfare, such topics as computer crime, digital piracy, Internet industrial espionage, and other computer network attacks not directly associated with national security, are not the focus of this overview.

Definitions

Information warfare uses technology both offensively and defensively, and also to gain intelligence about the plans and capabilities of opponents. However, a dependence on technology also invites new national security vulnerabilities and

raises new policy issues. The first requirement for a better understanding of the many uses of new technology for information warfare is a definition of terms.

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: for example, by dropping dummies from airplanes to simulate attack by live paratroopers; or by sending false messages intended for interception, so as to mislead.[1] 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. [2]

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. [3]

Therefore, information warfare, or military 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. 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 theat might prove useful to an adversary, (4) sending malicious computer programs to attack and disrupt adversary computer

---

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

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

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

software, and (5) creating high 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.[4]

Information Superiority

Information Superiority is a DOD term that describes a competitive advantage in the information realm that enables a military commander to surprise and out maneuver an enemy. It supports better coordination of battlefield units, and enables each individual battlefield commander to make better-informed decisions more quickly than an adversary. Decision Superiority is the DOD term used to describe a competitive advantage in the cognitive realm. Decision Superiority is facilitated by Information Superiority.[5] DOD capabilities for IO help achieve the objectives of Information Superiority and Decision Superiority.

DOD Information Operations Capabilities

DOD has identified five core capabilities for conduct of information operations; (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.

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.[6] For example, during the 1991 Gulf War, leaflets and broadcasts were used in a campaign to reassure Iraqi soldiers that they would be treated well if they

---

[4] Ronald Fogleman and Shiela Widnall, *Cornerstones of Information Warfare,* 2002, December 9, 1995, [http://www.af.mil/lib/corner.html]

[5] "Joint Vison 2020" is a DOD guide that presents a vision of future warfare that is enabled by the competitive advantages of Information Superiority and Decision Superiority. Arthur Money, *Report on Network Centric Warfare*, 2001, h[ttp://www.dodccrp.org/NCW/NCW_report/report/ncw_sense.pdf]

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

surrendered, depicting them as brave men who had been led astray by an “evil” Saddam.[7]

Executive Order 13283, signed by President George W. Bush on January 21, 2003, established within the White house the Office of Global Communications (OGC), headed by Deputy Assistant to the President for Global Communications, Tucker Eskew.[8] 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 instead will shine a light on others' disinformation, according to Eskew.[9]

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.

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, OPSEC may recommend removal of certain publicly available information from DOD web sites, as political crises develop.

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.

---

[7] Dorothy Denning, *Information Warfare and Security*, Addison-Wesley, 1999, p.7.

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

[9] OGC has been up and running since July 2002, working to get the American 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, February 11, 2003.

Computer Network Operations (CNO)

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. CNO may be subdivided into Computer Network Attack (CNA), Computer Network Defense (CND), and Computer Network Exploitation (CNE) operations.

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. Electronic Warfare (EW) can be used against a computer, but it is not computer network attack. CNA relies on the data stream to execute the attack while EW relies on the electromagnetic spectrum. Examples of these two different operations are the following; sending a digital signal through the computer network to a central processing unit that instructs the controller to short out the power supply is CNA, while sending a high voltage surge through the electrical power cable to short out the power supply is EW.

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.

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 use of electromagnetic energy to control the electromagnetic spectrum to attack the enemy. The high power electromagnetic energy can 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. The generated pulse is not directly harmful to humans or structures, however, it can overload or destroy nearby electronic devices — 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. 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 techniques.[10]

Cyberweapons and Cyberwarfare

Computer Network Operations (a.k.a., cyberwarfare) is the component of information operations that treats computers and digital networks as a battlefield. Potential cyberwarfare operations include (a) attempts to infiltrate networks, (b) attempts to steal or sabotage information, and (c) attempts to paralyze high technology systems. Cyberweapons are computer programs (code modules) used as tools to enable these operations.

Cyberweapons are tools that may be placed into 3 categories;

- offensive attack tools, such as viruses, Trojan horses, denial-of-service attack tools, and other malicious code;
- defensive tools, such as encryption and firewalls; and
- "dual use" tools, such as port vulnerability scanners, and network monitoring tools.

Offensive tools are used mainly to cause harm, 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.

Offensive cyberweapons can also be used defensively, as for an information counter-attack. Launching a counter-attack against an intruder is risky, though, because of the possibility of damaging the computers or networks of an innocent third party. However, if attackers are made aware that a potential target organization has an effective information counter-attack capability, then offensive cyberweapons also may serve as a deterrent to information attack.

---

[10] For more on Electronic Warfare, see CRS Report RL30841 and CRS Report RL30639.

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 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 Web site.[11]

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. Within JIOC, the Joint Task Force-Computer Network Operations (JTF-CNO), has responsibility to (a) coordinate the defense of DOD computer systems and networks; and (b) coordinate and conduct computer network attack in support of other combatant commanders and national objectives.

The JIOC also supports the integration of operations security, psychological operations, military deception, and electronic warfare throughout the planning and execution phases of the operations. The JIOC is comprised of personnel from all four military services, the civil service, and three allied nations.[12]

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, 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. There is speculation by some that the Pentagon is considering the use of possible offensive computer

---

[11] 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 Web sites 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.

[12] U.S. Strategic Command Facts and Information, February 10, 2003, [http://www.stratcom.mil/factsheetshtml/Information%20Operations.htm].

operations against Iraq, if war is initiated to halt their chemical, biological and weapons development programs.

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.[13]

Policy Issues

Several policy issues that Congress may choose to consider include:

- international arms control for cyberweapons;
- international cooperation for pursuit of cyber terrorists and other cyber attackers;
- psychological operations affecting 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 the confidentiality, integrity, or availability of information systems may in theory be treated as a weapon of war, and within the scope of arms control or the laws of armed conflict. Attempts are being made by international organizations to classify and control malicious computer code.[14] DOD has not yet developed a policy regarding international controls for

---

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

[14] In 1998 and 1999, Russia proposed that the First Committee of the UN 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.

(continued...)

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..[15] The issue is whether the United States should 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.

International Cooperation for Pursuit of Cyber Attackers

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 (CND) also requires the use of computer espionage (CNE) to determine whether an adversary has been sending out computer probes in preparation for launching a follow-on attack (CNA). 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.[16] An emerging issue is whether the United States should pursue international agreements to harmonize cyber-crime legislation for CND and CNE, and also deter CNA through tougher criminal penalties.

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. Management of media-relations during crisis is also transforming the military public-affairs officer into an information warrior.

---

[14] (...continued)
121-144, [http://www.isn.ethz.ch/onlinepubli/publihouse/infosecurity/volume_7/c1/C1_index.htm].

[15] 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).

[16] In Argentina, a group calling themselves the X-Team, hacked into the web site of the Supreme Court in April 2002. The trial judge stated that the law in his country covers crime against people, things and animals but not web sites. The group on trial was declared not guilty of breaking into the web site. Paul Hillbeck, *Argentine judge rules in favor of computer hackers*, 2003, February 5, 2002, http://www.siliconvalley.com/mld/siliconvalley/news/editorial/3070194.htm.

Instantaneous news reports, particularly television images, now offer an effective way to influence and transform public opinion.[17]

DOD Directive 3600.1 is the current guide for U.S. military Information Operations.[18] However, in 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 certain areas of the Middle East, Asia, and Europe.[19] No further information is available on the status of this proposal.

This reported proposal seems to be at variance with the stated mission and methods of the new Office of Global Communications, established on January 24, 2003 by Executive Order 13283. The OGC is directed to promote the spread of truthful and accurate messages to others about U.S. policy, and avoid disinformation.[20] OGC has coordinated themes calling for the disarmament of Saddam Hussein. The office is also coordinating 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.

The new OGC office replaces an earlier effort by the administration to build public support overseas for the war on terrorism. In February 2002, the Pentagon opened, and then quickly shut down, the Office of Strategic Influence (OSI), after it

---

[17] 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, p. 56-77
[http://www.airpower.maxwell.af.mil/airchronicles/apj/apj00/ sum00/sum00.html]

[18] DOD Directive 3600.1 was created December 9, 1996.

[19] 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.

[20] 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.

was proposed internally to use the Internet and other media to spread false information.[21]

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.[22]

Military Dependence on the Civilian Critical Infrastructure

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. A large percentage of less-secure NIPRNET traffic is routed through the civilian Internet, while SIPRNET traffic has traditionally been isolated from the civilian Internet.

In August 1999, the Defense Information Systems Agency (DISA) sought to increase security for NIPRNET by implementing policy changes to reduce the number of unofficial connections to the Internet. However, according to a December 2000 report from the DOD inspector general, that policy failed to reduce the number of security problems. The report was critical of the efforts and concluded that NIPRNET's security policy was never incorporated into overall DOD policy. The report also noted that the DISA policy "lacked visibility" because it did not clearly define the process for connecting services to the Internet, nor did it require regular status reports on the progress made in securing the NIPRNET/Internet connections.[23]

Recently, DOD has reported that 47 military sites are scheduled in 2003 to start transmitting encrypted classified SIPRNET messages through the NIPRNET. This use of encrypted traffic through the less-secure NIPRNET enables military sites to reach operational status for transmitting classified information within a shorter time frame. However, security of communications through the NIPRNET depends partly on the level of security found in the civilian computer systems that control the national and global communications infrastructure.[24] Attacks directed against

---

[21] 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.

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

[23] Christopher Dorobek and Diane Frank, *DOD May Pull Key Net From the Internet*, FCW.com, December 26, 2002, [http://www.fcw.com/fcw/articles/2002/0826/news-net-08-26-02.asp].

[24] Seventy percent of NIPRNET traffic is directed toward the civilian Internet. Christopher Dorobek and Diane Frank, *DOD may pull key net from the Internet, 2002, December 26,*

(continued...)

civilian computers may slow or disable the Internet, or parts of the civilian communications infrastructure, and also increase risk to NIPRNET.[25]

The Defense Department began in February 2003 to block access to selected Internet communications ports that link the Internet to NIPRNET. This is a policy change designed to improve protection for sensitive online information, defense officials say. Communications ports enable certain Web applications to transmit information over the Internet, and are commonly referred to by a number. One of the ports slated for closure is port 156, which is used to communicate with the Microsoft SQL server. In January 2003, an Internet worm exploited a known vulnerability in the Microsoft SQL server software package. A handful of DOD sites were not patched to protect against the worm and were briefly taken off line for repair.

However, the new policy will allow several other NIPRNET communications ports to remain unblocked, including those used for mail transfer and for Web page browsing.[26] The issue for military communications using NIPRNET is whether increased short-term flexibility outweighs apparent vulnerabilities for national security while DOD continues to rely on parts of the civilian Internet communications infrastructure.

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

The new National Strategy to Secure Cyberspace, delivered as a draft in September 2002, by the Critical Infrastructure Protection Board (CIPB), states that the private sector now has a crucial role in protecting national security because it largely runs the nation's critical infrastructure [27]. However, the September plan has been 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 report, the

---

[24] (...continued)
2002, [http://www.fcw.com/fcw/articles/2002/0826/news-net-08-26-02.asp]. Dan Caternniccia, *Marines tunnel to SIPRNET: Staff uses encryption to access DOD network*, 2002, December 9, 2002, December 9, [http://www.fcw.com/fcw/articles/2002/1209/tec-tunnel-12-09-02.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. Christopher Dorobek and Diane Frank, *DOD may pull key net from the Internet*, FCW.com, December 26, 2002, [http://www.fcw.com/fcw/articles/2002/0826/news-net-08-26-02.asp].

[25] Nine of 13 main Internet DNS servers were attacked and temporarily disabled in October, 2002. Robert Lemos, *Mystery attacker swamps .info domain system*, Silicon.com, Dec 27, 2002, [http://www.silicon.com].

[26] Anne Plummer, *DOD To Begin Closing Gateways Between Internet And Military Network*, Inside the Pentagon, February 13, 2002, p. 2.

[27] 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/]

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.[28]

In February 2003, the White House released a scaled-back cybersecurity strategy outlining steps that the government, industry and citizens should take to protect computer systems from online attacks. The plan does not indicate a need for regulation, and instead urges home and small business computer users to install firewall 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 scaled-back plan does not do enough to ensure that companies will adopt sound security practices.[29] Richard Clarke, former chairman of the CIPB, has also stated that the nation's critical infrastructure is vulnerable because cyber-attacks could possibly use the resources of millions of home and business PCs to launch debilitating assaults on the nation's infrastructure

The issue is whether regulation should be considered as a tool to supplement, or replace, market forces to encourage the private sector to improve its computer security.

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

The effects of offensive electromagnetic pulse weapons and cyberweapons may be difficult to limit or control. The effects of a high energy weapon may be widespread enough to also disable nearby critical civilian or medical electronic equipment, such as pace-makers, or hospital incubators. Or, the possibility exists that if a computer attack program is targeted at enemy military computer systems, the malicious code might accidentally spread through the Internet to severely affect other critical non-military computers, possibly civilian systems that control electricity, water sanitation, or communications. The effects might spread further to also shut down critical systems in other non-combatant countries. 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.

The effects of using cyberweapons or electromagnetic pulse weapons, if widespread and severe, could arguably exceed customary rules of military conflict,

---

[28] "The Gilmore Report". Gilmore, 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, 2002, [http://www.rand.org/nsrd/terrpanel/terror4.pdf].

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

also known as the laws of war.[30] The issue is whether lack of precise control over cyberweapons or high energy weapons might involve the U.S. in violations of international law, should offensive information warfare operations ever be employed.

Current Legislative Proposals

In the absence of a central clearing house, responsibility for protecting the national security of the computer controlled infrastructure has fallen to each individual federal agency, and to industry owners of the infrastructure. Some maintain that a much more coordinated approach to computer security may be needed to protect against threats from information warfare attacks, whether launched by a hostile nation or by terrorist groups.

Legislative proposals introduced thus far in the 108th Congress that are related to national security and information warfare policy issues include:

- H.R. 48: This bill establishes in the International Broadcasting Bureau the Office of Global Internet Freedom to develop and implement a comprehensive global strategy to combat state-sponsored and state-directed Internet jamming and persecution of those who use the Internet.

- S. 6 and S. 22: A bill to create a grants program to support homeland security activities of States, local governments, and Indian tribes public safety officers.

- S. 87: This bill, also known as the Homeland Security Block Grant Act of 2003, is intended to improve cyber and infrastructure security by giving federal block grant assistance to state, local and community planning organizations.

- S. 187: This bill, known as the National Cyber Security Leadership Act of 2003, proposes that civilian government Chief Information Officers for each federal agency must identify significant computer security vulnerabilities, establish performance goals to eliminate those vulnerabilities, test for new vulnerabilities regularly, and report agency security status to the Office of Management and Budget.

---

[30] 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. The United States is party to various limiting treaties. For example, innocent civilians are protected during war under the Convention on Prohibitions or Restrictions on the Use of Certain Conventional Weapons Which May Be Deemed to be Excessively Injurious or to have Indiscriminate Effects. 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.

A bill known as the Cybersecurity Research and Education Act of 2002 (S.1901) was introduced in the 107th Congress. This earlier bill would have awarded: (1) graduate fellowships for doctoral studies and research in cybersecurity; (2) grants to institutions of higher education to enable faculty members who are teaching cybersecurity subjects to spend a sabbatical working at the National Security Agency, the Department of Defense, the National Institute of Standards and Technology, a research laboratory supported by the Department of Energy, or a qualified institution; and (3) grants to qualified institutions for activities related to acquiring cybersecurity infrastructure. The bill was referred to the Senate Committee on Health, Education, Labor, and Pensions on January 28, 2002, and no further action was taken.

In 2002, the Cyber Security Research and Development Act (PL107-305) was enacted to support research and education programs at the National Science Foundation and the National Institute of Standards and Technology to improve federal and private sector computer security. Also, in 2002, the Federal Information Security Management Act of 2002 (PL107-347) was enacted to improve security for civilian agency information systems.