International and Operational Law Department
The Judge Advocate General's School
Charlottesville, Virginia

INFORMATION OPERATIONS

LIEUTENANT COLONEL JORDAN
U.S. Marine Corps

REFERENCES

1. 50 U.S.C. § 402 (1996)[*hereinafter* The National Security Act of 1947].
2. 10 U.S.C. § 161-168 (1996) Department of Defense Reorganization Act of 1986, Pub. L. No. 99-433 (1985)[*hereinafter* Goldwater-Nichols].
3. Executive Order 12684
4. Executive Order 13010
5. Presidential Decision Directive 62, *Combating Terrorism*, 22 May 1998
6. Presidential Decision Directive 63, *Critical Infrastructure Protection*, 22 May 1998
7. Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts (Protocol I), *opened for signature* 12 Dec. 1977, U.N.Doc. A/32.144, *reprinted in* 16 I.L.M. 1391, U.S. DEP'T OF ARMY, PAM 27-1-1, PROTOCOLS TO THE GENEVA CONVENTIONS OF 12 AUGUST 1949 (1 Sept. 1979).
8. U.S. DEP'T OF DEFENSE, DIR. S-3600.1 INFORMATION OPERATIONS (U) (9 Dec. 1996).
9. U.S. DEP'T OF DEFENSE, OFFICE OF GENERAL COUNSEL, PAPER, *AN ASSESSMENT OF INTERNATIONAL ISSUES IN INFORMATION OPERATIONS*
10. THE JOINT CHIEFS OF STAFF, JOINT PUB. 5-0, DOCTRINE FOR PLANNING JOINT OPERATIONS (13 April 1995).
11. CHAIRMAN, JOINT CHIEFS OF STAFF INSTR. 5810.01, IMPLEMENTATION OF THE DOD LAW OF WAR PROGRAM (12 Aug. 1996).
12. CHAIRMAN, JOINT CHIEFS OF STAFF INSTR. 3210.01A, JOINT INFORMATION OPERATIONS POLICY ( ).
13. CHAIRMAN, JOINT CHIEFS OF STAFF INSTR. 6510.01B, DEFENSIVE INFORMATION OPERATIONS IMPLEMENTATION (22 Aug. 1997).
14. THE JOINT CHIEFS OF STAFF, JOINT PUB. 0-2, UNIFIED ACTION ARMED FORCES (UNAAF) (24 Feb. 1995).
15. THE JOINT CHIEFS OF STAFF, JOINT PUB. 2-01,JOINT INTELLIGENCE SUPPORT TO MILITARY OPERATIONS (20 Nov. 1996).
16. THE JOINT CHIEFS OF STAFF, JOINT PUB. 3-13, JOINT DOCTRINE FOR INFORMATION OPERATIONS (9 OCTOBER 1998).
17. THE JOINT CHIEFS OF STAFF, JOINT PUB. 3-13.1, JOINT DOCTRINE FOR COMMAND AND CONTROL WARFARE (C2W) (7 Feb. 1996).
18. THE JOINT CHIEFS OF STAFF, JOINT PUB. 3-53, DOCTRINE FOR JOINT PSYCHOLOGICAL OPERATIONS (10 July 1996).
19. THE JOINT CHIEFS OF STAFF, JOINT PUB. 3-54, JOINT DOCTRINE FOR OPERATIONS SECURITY (27 Jan. 1996).
20. THE JOINT CHIEFS OF STAFF, JOINT PUB. 5-03.1, JOINT OPERATIONS PLANNING AND EXECUTION SYSTEM VOL I: PLANNING POLICIES AND PROCEDURES (4 Aug. 1993).
21. THE JOINT CHIEFS OF STAFF, JOINT PUB. 5-03.2, JOINT OPERATIONS PLANNING AND EXECUTION SYSTEM VOL II: OPLAN FORMATS AND GUIDANCE (10 March 1992).
22. THE JOINT CHIEFS OF STAFF, CHAIRMAN JOINT CHIEFS OF STAFF MANUAL 3500.05, JOINT TASK FORCE HEADQUARTERS MASTER TRAINING PLAN (15 Apr. 1997).
23. U.S. DEP'T OF ARMY, FIELD MANUAL 100-6, INFORMATION OPERATIONS (27 Aug. 1996).

I. "KEY TERRAIN"

A. Understand the evolving role for Information Operations considerations as an integral part of the operational planning and review process.

B. Introduce the doctrinal definitions and operational concepts in the area of Information Operations.

C. Be familiar with the relevant international and domestic legal considerations inherent in the practice of Information Operations.

D. Have a functional awareness of the issues affecting your installation.

E. Be alert for currently recommended changes in the UCMJ, as well as the organizational structures charged with conducting Information Operations.

II. INFORMATION OPERATIONS – BACKGROUND

A. Introduction. "Computers and computer-dependent systems permeate everyone's daily life. From local, state, and federal government decision-makers to warfighters, businessmen, lawyers, doctors, bankers, and individuals—everyone relies upon information and information systems that involve the acquisition, transmission, storage, or transformation of information. . . . Anyone with a computer has access to instantaneous worldwide communications and a wealth of resources on the internet. Instead of human watch standers, computerized sensing and control devices now monitor transportation, oil, gas, electrical, and water treatment systems throughout our Nation. Satellites serve as the backbone of our telecommunication systems and our economic well-being. The Global positioning System (GPS) guides virtually all of the commercial aircraft in the world."[1]

[1] W.G. SHARP, CRTITICAL INFRASTRUCTURE PROTECTION: *A NEW ERA OF NATIONAL SECURITY*, THE FEDERALIST SOCIETY INTERNATIONAL AND NATIONAL SECURITY LAW NEWS, Vol.2, at 1 (Summer 1998).

1. "The Department of Defense is heavily dependent upon timely and accurate information and is keenly focused on information operations and information assurance. . . . Over 95% of Department of Defense telecommunications travel over commercial systems, and the interdependence of our civilian infrastructure and national security grows dramatically on a daily basis. In a few short decades, the global networking of computers via the internet will very likely be viewed as the one invention that had the greatest impact on human civilization—and perhaps the greatest challenge to our national security.[2]

2. "All of these computers and computer-dependent systems are vulnerable to physical and electronic ["cyber"] attack—from the computers on which individuals store and process classified information, privileged attorney-client information, or proprietary data, to our nationwide telecommunication and banking systems. Indeed the year 2000 {"Y2K"] problem demonstrates that we are even vulnerable to our own misfeasance and poor planning. A single non-nuclear, electromagnetic pulse can destroy or degrade circuit boards and chips, or erase all electronic media on Wall Street, in the Pentagon, or your local bank. The loss of a single satellite can terminate service for over 90% of the 45 million pagers in the United States, as well as interrupt thousands of cable television stations and credit card transactions. GPS signals can be spoofed or degraded, or used as part of highly accurate targeting systems. Advanced computer technology can help build nuclear weapons. Internet and computer crime is so simple that two teenagers in Cloverdale, California with a mentor in Israel can break into sensitive national security systems at the Department of Defense. Information warfare experts can use global television to selectively influence political and economic decisions or produce epileptic-like spasms in viewers. Cyber warfare of the 21st century could significantly impact the daily lives of every man, woman, and child in America."[3]

[2] *Id.*
[3] *Id.*

B. **The Information Age and Information Technology**: **Revolutions in Military and Business Affairs**. Successful military commanders have always depended on the best quality and quantity information to make effective decisions. For thousands of years, the means to transmit and use information remained essentially unchanged. However, the advent of electronics-based communications over the last 150 years has dramatically increased the variety, volume, accessibility, and speed of transmitting and using information. The telegraph, telephone, radio, and television have greatly changed the nature and pace of warfare. Since World War II, advances in digital electronic data processing and the speed and transmission methods of telecommunications have been applied widely and with dramatic success as force multipliers in the information systems that support military organizations and functions. Information systems include organizations, components, and the entire infrastructure that act upon information—including people.[4]

1. Nations, corporations, and individuals each seek to increase and protect their own store of information while trying to limit and penetrate the adversary's. Since around 1970, there have been extraordinary improvements in the technical means of collecting, storing, analyzing, and transmitting information.[5]

2. There is a technological revolution sweeping through information systems and their integration into our daily lives leading to the term "Information Age." Information-related technologies concentrate data, vastly increase the rate at which we process and transmit data, and intimately couple the results into virtually every aspect of our lives. The Information Age is also transforming all military operations by providing commanders with information unprecedented in quantity and quality. The commander with the advantage in observing the battlespace, analyzing events, and distributing information possesses a powerful, if not decisive, lever over the adversary.[6]

---

[4] Chairman of the Joint Chiefs of Staff (CJCSI) brochure, *Information Operations: A Strategy for Peace, The Decisive Edge in War*, March 1999, (*hereinafter*, CJCSI brochure*, Information Operations*).

[5] Dep't of the Air Force brochure, *Cornerstones of Information Warfare*

[6] *Id.*

3. We must distinguish between *information age warfare and information operations*. Information age warfare uses information age technologies as tools to better perform combat operations. For example, cruise missiles exploit information age technologies to put a bomb on target. Ultimately, information age warfare will impact all combat operations. In contrast, information operations, view information itself as a separate realm, potent weapon, and lucrative target. Information, is technology dependent. Information age technology is turning a theoretical possibility into fact: directly manipulating the adversary's information.[7]

4. As reliance upon electronic information systems grows, their value is matched by their significance as targets and as weapons. The opposing information systems must be attacked; our information systems must be protected. Attacking adversary information and information systems while defending one's own information and information systems is referred to as Information Operations (IO).[8]

5. Our reliance on technology makes protecting critical US infrastructure against hostile IO a paramount mission. Concurrently, developing US capabilities for IO in peacetime engagement activities, smaller scale contingencies, and major theater war is critical. The capability to penetrate, manipulate, and deny an adversary's battlespace awareness is of utmost importance. IO must orient not just on the technology, but on the most crucial factor in all aspects of warfare—the human element. The ultimate targets of IO are the will and ability of decision makers, leaders, and commanders to observe, interpret, reason, and make and implement sound decisions.[9]

6. To achieve the greatest effect, all types of military operations at every level of war must include IO. In the hands of a commander, IO are a valuable instrument in every national security situation, including peace, pre-crisis, conflict and combat, and return to stability and peace.[10]

---

[7] *See generally, Id.*
[8] CJCSI brohcure, *Information Operations*.
[9] *Id.*
[10] *Id.*

C. Information Technology: Simultaneously Enhancing and Threatening US Economic Potential. Along with the tremendous economic potential offered by use of the internet, reliance on computers and computer-dependent systems produces significant national security vulnerabilities. The Information Age marks the end of the physical sanctuary that the United States has enjoyed for two hundred years. Now, the low cost of developing the tools to operate in the electronic environment has decreased the threshold of what it takes to be an active and capable player on the global scene.[11]

1. Our military power and national economy are increasingly reliant upon interdependent critical infrastructures—the physical and information systems essential to the operations of the economy and the government. They include telecommunications, energy, banking and finance, transportation, water systems and emergency services. It has long been the policy of the United States to assure the continuity and viability of these critical infrastructures. But advances in information technology and competitive pressure to improve efficiency and productivity have created new vulnerabilities to both physical and information attacks as those infrastructures have become increasingly automated and interlinked. If we do not implement adequate protective measures, attacks on our critical infrastructures and information systems by nations, groups or individuals might be capable of significantly harming our military power and economy.

2. On 15 September 1993, President Clinton established the "United States Advisory Council on the National Information Infrastructure" by **Executive Order 12864**. This Advisory Council was tasked to advise the Secretary of Commerce on a national strategy and other matters related to the development of the National Information Infrastructure (NII). The Council's reports included, "A Nation of Opportunity: Realizing the Promise of the Information Superhighway" and "A Framework for Global Electronic Commerce" concerning the Administration's strategy for the development of global electronic commerce. These reports recognized that as our nation recognizes the enormous economic potential of the world-wide web, we also increase our vulnerabilities.[12]

---

[11] American Bar Association, National Security Law Report, Vol. 20, No. 2, May 1998, summarizing comments of Professor Daniel T. Kuehl, Professor at the National Defense University's School for Information Warfare and Strategy, made during the ABA Standing Committee on Law and National Security's Sixth Annual Conference Reviewing the Field of National Security Law.

[12] *See generally*, SHARP, CRTITICAL INFRASTRUCTURE PROTECTION: *A NEW ERA OF NATIONAL SECURITY*.

3. The US is enhancing its ability to defend against hostile information operations, which could in the future take the form of a full-scale, strategic information attack against our critical national infrastructures, government and economy—as well as attacks directed against our military forces. As other countries develop their capability to conduct offensive information operations, we must ensure that our national and defense infrastructures are well protected and that we can quickly recognize, defend against and respond decisively to an information attack.[13]

B. Identifying National Security Vulnerabilities. Recognizing the vulnerabilities created by US dependence upon information technology, on 15 July 1996, President Clinton promulgated **Executive Order 13010**, establishing the "President's Commission on Critical Infrastructure Protection" (CIP). EO 13010 declared that certain "national infrastructures are so vital that their incapacity or destruction [by physical or cyber attack] would have a debilitating impact on the defense or economic security of the United States." EO 13010 listed eight categories of critical infrastructures: telecommunications; electrical power systems; gas and oil storage and transportation; banking and finance; transportation; water supply systems; emergency services (including medical, police, fire, and rescue); and continuity of government. Recognizing that many of these infrastructures are owned and operated by the private sector, the EO noted that, "it is essential that the government and private sector work together to develop a strategy for protecting them and assuring their continued operation."[14]

1. The President's Commission determined that widespread capabilities to exploit US infrastructure vulnerabilities exist and are growing at an alarming rate and for which we have little defense. The Commission identified potential threats, including insiders, recreational and institutional computer hackers, organized criminals, industrial competitors, terrorists, and states.[15]

[13] A National Security Strategy for a New Century, The White House, October 1998.
[14] *See*, SHARP, CRTITICAL INFRASTRUCTURE PROTECTION: *A NEW ERA OF NATIONAL SECURITY*
[15] *See, id.*.

2. The President's Commission made seven findings: information sharing is the most immediate need; responsibility is shared among owners and operators and the government; infrastructure protection requires integrated capabilities of diverse agencies, and special means for coordinating federal response to ensure these capabilities are melded together effectively; the challenge is one of adapting to a changing culture; the federal government has important roles in the new infrastructure protection alliance with industry and state and local governments; **the existing legal regime is imperfectly attuned to deal with cyber threats**; research and development are not presently adequate to support infrastructure protection.[16]

3. The President's Commission adopted recommendations for a national strategy to deal with infrastructure protection. These recommendations included strengthening the existing international and domestic legal regimes for federal response to and deterrence of cyber threats.[17]

C. Defending U.S. Critical Infrastructure and Information Systems:

[16] *See, id*.
[17] *See, id.*

1. **The 1998 National Security Strategy[18] (NSS).** The 1998 NSS recognizes that the U.S. faces diverse threats requiring integrated approaches to defend the nation, shape the international environment, respond to crises and prepare for an uncertain future. The NSS declares that "[t]hreats to the national information infrastructure, ranging from cyber-crime to a strategic information attack on the United States via the global information network, present a dangerous new threat to our national security. We must also guard against threats to our critical national infrastructures—such as electrical power and transportation—which could increasingly take the form of a cyber attack in addition to physical attack or sabotage, and could originate from terrorist or criminal groups as well as hostile states."[19] The NSS further provides that "[o]ur military power and national economy are increasingly reliant upon interdependent critical infrastructures—the physical; and information systems essential to the operations of the economy and government. . . . [A]dvances in information technology and competitive pressures to improve efficiency and productivity have created new vulnerabilities to both physical and information attacks as those infrastructures have become increasingly automated and interlinked. If we do not implement adequate protective measures, attacks on our critical infrastructures and information systems by nations, groups or individuals might be capable of significantly harming our military power and economy."[20]

[18] www.whitehouse.gov/WH/EOP/NSC/html/documents/nssrpref.html
[19] A National Security Strategy for a New Century, The White House, October 1998.
[20] *Id.*

2. **The 1997 National Military Strategy (NMS).**[21] The 1997 NMS listed Information Operations as a key capability which the US military must provide in order to give the national leadership a range of viable options for promoting and protecting US interests in peacetime, crisis, and war. According to the NMS, Information Operations are an integral component of modern military operations because "[s]uccess in any operation depends on our ability to quickly and accurately integrate critical information and deny the same to an adversary. We must attain information superiority through the conduct of both offensive and defensive information operations. Information operations are, however, more than discrete offensive and defensive actions; they are also the collection and provision of that information to the warfighters. Superiority in these areas will enable commanders to contend with information threats to their forces, including attacks which may originate from outside their area of operations. It also limits an adversary's freedom of action by disabling his critical information systems. We are developing joint doctrine for offensive and defensive information operations that assigns appropriate responsibilities to all agencies and commands for assuring committed forces gain and maintain information superiority. This emerging joint doctrine must fully integrate interagency participation allowing us to leverage all existing information systems."[22]

3. **Presidential Decision Directive (PDD) 62, *Combating Terrorism* and Presidential Decision Directive 63, *Critical Infrastructure Protection***. To enhance US ability to protect critical infrastructures, on 22 May 1998, President Clinton promulgated two Presidential Decision Directives to build the interagency framework and coordinate our critical infrastructure defense programs.

   a. **PDD 62** focuses on the growing threat of all unconventional attacks against the United States such as terrorist acts, use of weapons of mass destruction (WMD), assaults on critical infrastructures, and cyber attacks.

   b. **PDD 63** calls for immediate action and national effort between government and industry to assure continuity and viability of our critical infrastructures. PDD 63 makes it US policy to take all necessary measures to swiftly eliminate any significant vulnerability to physical or information attacks on critical US infrastructures, particularly our information systems.

[21] www.dtic.mil/jcs/core/nms.html
[22] The 1997 National Military Strategy of the United States

D. Information Operations in Current US Military Operational Policy, Strategy and Doctrine.

1. **Department of Defense Directive (DODD) S-3600.1**, "Information Operations," and **Chairman of the Joint Chiefs of Staff Instruction (CJCSI) 3210.01A**, "Joint Information Operations Policy," outline general and specific information operations (IO) policy for Department of Defense (DOD) components and delineate specific responsibilities. **CJCSI 6510.01B**, "Defensive Information Operations Implementation," provides specific policy concerning defensive IO.[23]

2. **IO apply across all phases of an operation, throughout the range of military operations, and at every level of war.** Information warfare (IW) is conducted during time of crisis (including war) to achieve or promote specific objectives over a specific adversary. Defensive IO activities are conducted on a continuous basis and are an inherent part of force deployment, employment, and redeployment across the range of military activities.[24]

3. **IO may involve complex legal and policy issues** requiring careful review and national-level coordination and approval. IO planners must understand the **legal limitations** that may be placed on IO across the range of military operations. IO planners at all levels should consider the following broad areas: (1) **Domestic and international criminal and civil laws** affecting national security, privacy, and information exchange. (2) **International treaties and agreements** and customary international law, as applied to IO. (3) Structure and relationships among US intelligence organizations and general interagency relationships, including nongovernmental organizations.[25]

4. **IO focus on the vulnerabilities and opportunities** presented by the increasing dependence of the United States and its adversaries or potential adversaries on information and information systems.[26]

---

[23] THE JOINT CHIEFS OF STAFF, JOINT PUB 3-13, JOINT DOCTRINE FOR INFORMATION OPERATIONS, 9 Oct 1998 (*hereinafter*, Joint Pub 3-13).
[24] *Id.*
[25] *Id.*
[26] *Id*

5. IO contribute to the **integration of aspects** of the military element of national power with all other elements of national power to achieve objectives. IO can support the overall USG strategic engagement policy throughout the range of military operations. The effectiveness of **deterrence, power projection**, and **other strategic concepts** is greatly affected by the ability of the United States to influence the perceptions and decision making of others. In times of crisis, **IO can help deter adversaries from initiating actions** detrimental to the interests of the United States or its allies and/or coalition partners. . . . **IO can make an important contribution to defusing crises**; reducing periods of confrontation and enhancing the impact of informational, diplomatic, economic, and military efforts; and forestalling or eliminating the need to employ forces in a combat situation. Thus IO . . . **require close coordination among numerous elements of the USG**, to include the Department of Defense. Command, control, communications, and computers (C4) and intelligence provide crucial support to IO.[27]

6. **Information Warfare (IW) can be waged in crisis or conflict** within and beyond the traditional battlespace. IW may be conducted to shape the battlespace and prepare the way for future operations to accomplish US objectives.[28]

7. **CJCSI 3210.01A** sets forth specific US IO policy, including the following:

   a. **Offensive IO** will be employed to achieve mission objectives when deemed appropriate.[29]

   b. **Information, information systems, and information-based processes** (such as Command and control (C2)) used by US military forces will be protected relative to the value of the information they contain and the risks associated with their compromise or loss of access.[30]

---

[27] *Id.*
[28] *Id.*
[29] Chairman of the Joint Chiefs of Staff Instruction 3210.0A, *Joint Information Operations Policy* (*hereinafter*, CJCSI 3210.0A), *quoted in* Joint Pub 3-13.
[30] *Id*.

c. **Intelligence requirements** in support of IO will be articulated with sufficient specificity and timeliness to the appropriate intelligence production center or other intelligence organizations to meet the IO demand.[31]

d. **Technology** that affects an adversary's information and information systems and protects and defends friendly information and information systems will be pursued at every opportunity to ensure the greatest return on investment.[32]

e. **Joint and Service school curricula** will ensure personnel are educated in the concepts of IO, to include an appreciation of the vulnerabilities inherent in information systems and the opportunities found in adversary systems.[33]

f. **Combatant commanders** will incorporate offensive and defensive IO into deliberate and crisis action planning to accomplish their assigned missions.[34]

g. The growth in **IO-related technology and capabilities and associated legal issues makes it critical for commanders at all levels of command to involve their staff judge advocates in development of IO policy and conduct of IO.**[35]

8. **DODD S-3600.1, CJCSI 3210.01A**, and **CJCSI 6510.01B** assign specific unclassified responsibilities for IO within DOD. Among those responsibilities are:

a. **Chairman of the Joint Chiefs of Staff**:

(1) Serves as the principal military advisor to the Secretary of Defense on IO matters.

[31] *Id.*
[32] *Id.*
[33] *Id.*
[34] *Id.*
[35] *Id.*

(2) Establishes doctrine to facilitate the integration of IO concepts into joint warfare.

(1) Ensures plans and operations include and are consistent with IO policy, strategy, and doctrine.

b. **Combatant Commanders**:

(1). Plan, exercise, and conduct IO in support of national goals and objectives as directed by the Joint Strategic Capabilities Plan (JSCP).

(2). Integrate capabilities into deliberate and crisis action planing to conduct IO in accordance with appropriate policy and doctrine to accomplish their Unified Command Plan (UCP) assigned missions.

c. **Chiefs of the Services and Commander in Chief, US Special Operations Command**:

(1) Conduct research, development, testing and evaluation, and procurement of capabilities that meet validated Service and joint IO requirements.

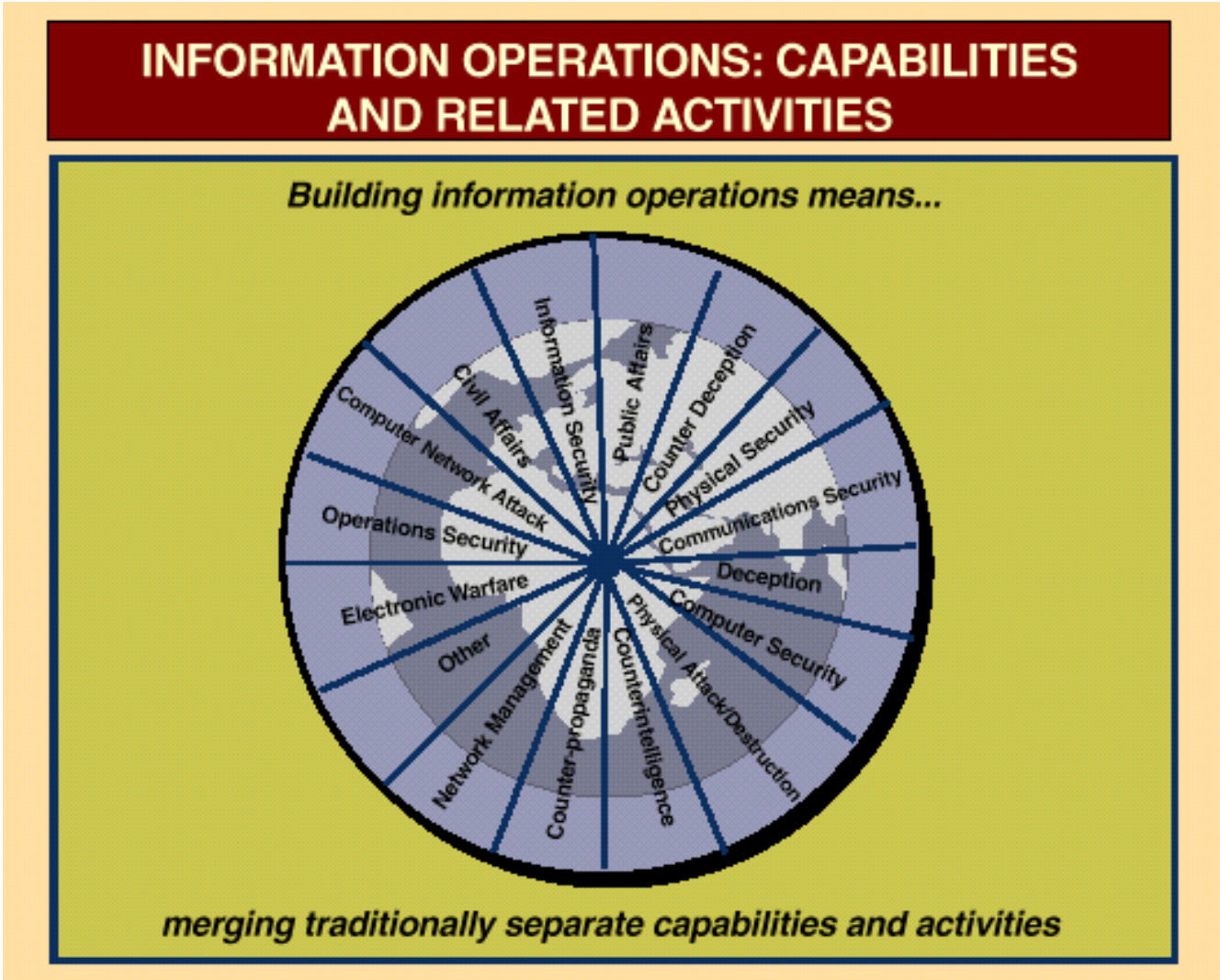
(2) Incorporate IO into Service school curricula and into appropriate training and education activities.

(3) Organize forces with capabilities to conduct IO. Train forces to conduct IO. Ensure Services' forces and planning capabilities effectively support the combatant commanders through the appropriate Service component commanders.

d. **All DOD Elements**: Adopt a risk management approach to the protection of their information, information systems, and information-based processes based on potential vulnerability to IO.

IV. BASELINE DEFINITIONS AND CONCEPTS
(drawn from Joint Pub 3-13)

A. "**Information Operations**" **are actions taken to affect adversary information, and information systems, while defending one's own information and information systems**. IO require the close, continuous integration of offensive and defensive capabilities and activities, as well as effective design, integration, and interaction of Command and control (C2) with intelligence support. IO are conducted through the integration of many capabilities and related activities. **Major IO capabilities** to conduct IO include, but are not limited to, **operations security** (OPSEC), **psychological operations** (PSYOP), **military deception**, **electronic warfare** (EW), and **physical attack** and/or **destruction**, and could include **Computer Network Attack** (CNA). **IO-related activities** include, but are not limited to, **public affairs** (PA) and **civil affairs** (CA) activities.



1. At the grand strategy level, nations seek to acquire, and protect information in support of their objectives. This exploitation and protection can occur in the economic, political, or military arenas. Knowledge of the adversary's information is a means to enhance our own capabilities, degrade or counteract enemy capabilities, and protect our own assets, including our own information.[36]

2. There are two major subdivisions within IO: **offensive IO** and **defensive IO**.

B. "Offensive IO" involve the integrated use of assigned and supporting capabilities and activities, mutually supported by intelligence, to affect adversary decision-makers and achieve or promote specific objectives. These assigned and supporting capabilities and activities include, but are not limited to, OPSEC, military deception, PSYOP, EW, physical attack and/or destruction, and special information operations (SIO), and could include CNA.

1. **Offensive IO principles** include the following:

a. The human decision making processes are the ultimate target for offensive IO. Offensive IO involve the integration and orchestration of varied capabilities and activities into a coherent, seamless plan to achieve specific objectives.

b. Offensive IO objectives must be clearly established, support overall national and military objectives, and include potential spectrum of IO objectives ranges from peace to war.

c. Selection and employment of specific offensive capabilities against an adversary must be appropriate to the situation and consistent with US objectives. These actions must be permissible under the law of armed conflict, consistent with applicable domestic and international law, and in accordance with applicable rules of engagement.

d. In order to efficiently attack adversary information and information systems, it is necessary to be able to do the following:

(1) Understand the adversary's or potential adversary's perspective and how it may be influenced by IO.

[36] Dep't of the Air Force brochure, *Cornerstones of Information Warfare*

(2) Establish IO objectives.

(3) Identify information systems value, use, flow of information, and vulnerabilities.

(4) Identify targets that can help achieve IO objectives.

(5) Determine the target set.

(6) Determine the most effective capabilities for affecting the vulnerable portion of the targeted information or information systems.

(7) Predict the consequences of employing specific capabilities with a predetermined level of confidence.

(8). Integrate, coordinate, and implement IO.

(9) Obtain necessary approval to employ IO.

(10) Evaluate the outcome of specific IO to the predetermined level of confidence.

2. **Offensive IO Capabilities**. When employed as an integrating strategy, IO weave together related capabilities and activities toward satisfying a stated objective. Offensive IO applies perception management actions such as PSYOP, OPSEC, and military deception, and may apply attack options such as EW and physical attack/destruction to produce a synergistic effect against the elements of an adversary's information systems.

a. **OPSEC** contributes to offensive IO by slowing the adversary's decision cycle and providing opportunity for easier and quicker attainment of friendly objectives. OPSEC denies the adversary critical information about friendly capabilities and information needed for effective and timely decision making, leaving the adversary vulnerable to other offensive capabilities.

b. **PSYOP** are actions to convey selected information and indicators to foreign audiences. They are designed to influence emotions, motives, reasoning, and ultimately, the behavior of foreign governments, organizations, groups, and individuals.

c. **Military Deception** targets adversary decision makers through effects on their intelligence collection, analysis, and dissemination systems.

d. **EW**. There are three major subdivisions of EW. They are **electronic attack** (EA), **electronic protection** (EP), and **electronic warfare** support (ES). All three contribute to both offensive and defensive IO.

(1) **EA** is any military action involving the use of electromagnetic and directed energy to control the electromagnetic spectrum or to attack the enemy. EA involves actions taken to attack the adversary with the intent of degrading, neutralizing, or destroying adversary combat capability to prevent or reduce an adversary's effective use of the electromagnetic spectrum.

(2) **EP** involves such actions as self-protection jamming and emission control taken to protect friendly use of the electronic spectrum by minimizing the effects of friendly or adversary employment of EW that degrade, neutralize, or destroy friendly combat capability.

(3) ES contributes to the Joint Force's situational awareness by detecting, identifying, and locating sources of intentional or unintentional radiated electromagenetic energy for the purpose of immediate threat recognition.

e. **Physical attack/destruction** refers to the use of "hard kill" weapons against designated targets as an element of an integrated IO effort.

f. **CNA.** See item D below.

C. "**Defensive IO"** integrate and coordinate policies and procedures, operations, personnel, and technology to protect and defend information and information systems. Defensive IO are conducted and assisted through **information assurance** (IA), **OPSEC**, **physical security**, **counterdeception**, **counterpropaganda**, **counterintelligence** (CI), **EW**, and **Special Information Operations** (SIO). Defensive IO ensure timely, accurate, and relevant information access while denying adversaries the opportunity to exploit friendly information systems for their own purposes. Offensive IO can support defensive IO.

1. Defensive IO integrate and coordinate protection and defense of information and information systems.

2. Defensive IO must be integrated with offensive IO to provide a timely response against identified and potential threats to friendly information and information systems.

3. **Defensive IO capabilities.**

   a. **OPSEC** is a process of identifying critical information and subsequently analyzing friendly actions attendant to military operations and other activities to identify those actions that can be observed by adversary intelligence systems; determine indicators adversary intelligence systems might obtain that could be interpreted or pieced together to derive critical information in time to be useful; and select and execute measures

   b. **EW**. EA, EP, and ES are examples of EW capabilities contributing to protection and defense of information and information systems.

   c. **Counterdeception** supports defensive IO by negating, neutralizing, or diminishing the effects of—or gaining advantages from—a foreign deception operation.

   d. **Counter-propaganda Operations.** Activities identifying adversary propaganda contribute to situational awareness and serve to expose adversary attempts to influence friendly populations and military forces.

   e. **CI** activites contribute to defensive IO by providing information and conducting activities to protect and defend friendly information systems against espionage, sabotage, or terrorist activities.

D. "Computer Network Attack" is defined as operations to disrupt, deny, degrade, or destroy information resident in computers and computer networks or the computers and networks themselves.

E. "Information" is defined as facts, data, or instructions in any medium or form. It is the meaning a human assigns to data by means of the known conventions used in their representation.

F. "Information assurance" is defined as IO that protect and defend information systems by ensuring their availability, integrity, authentication, confidentiality, and nonrepudiation. This includes providing for restoration of information systems by incorporating protection, detection, and reaction capabilities.

G. "Information-based processes" are processes that collect, analyze, and disseminate information using any medium or form. These processes may be stand-alone processes or sub-processes which, taken together, comprise a larger system or systems. Information-based processes are included in all systems and components thereof that require facts, data, or instructions in any medium or form to perform designated functions or provide anticipated services. For purposes of IO, examples range from strategic reconnaissance systems, to a key adversary decision-maker, to a local traffic control point in an austere overseas joint operations area (JOA).

H. "Information environment" is the aggregate of individuals, organizations, or systems that collect, process, or disseminate information, including the information itself.

I. "Information superiority" is the capability to collect, process, and disseminate an uninterrupted flow of information while exploiting or denying an adversary's ability to do the same.

J. "Information system" is the entire infrastructure, organization, personnel, and components that collect, process, store, transmit, display, disseminate, and act on information. The information system also includes the information-based processes.

K. "Information warfare" (IW) is information operations conducted during time of crisis or conflict to achieve or promote specific objectives over a specific adversary or adversaries.

1. IW consists of targeting the enemy's information and information systems, while protecting our own, with the intent of degrading his will or capability to fight. IW may involve actions to deny, exploit, corrupt, or destroy the enemy's information and its functions; protecting ourselves against those actions; and exploiting our own information systems.

2. IW is any attack against an information system, regardless of the means. Bombing a telephone switching facility is IW. So is, destroying the switching facility's software.

3. IW is any action to protect our information or information systems, regardless of the means. Hardening and defending the switching facility against air or ground attack is IW. So is using an anti-virus program to protect the facility's software.

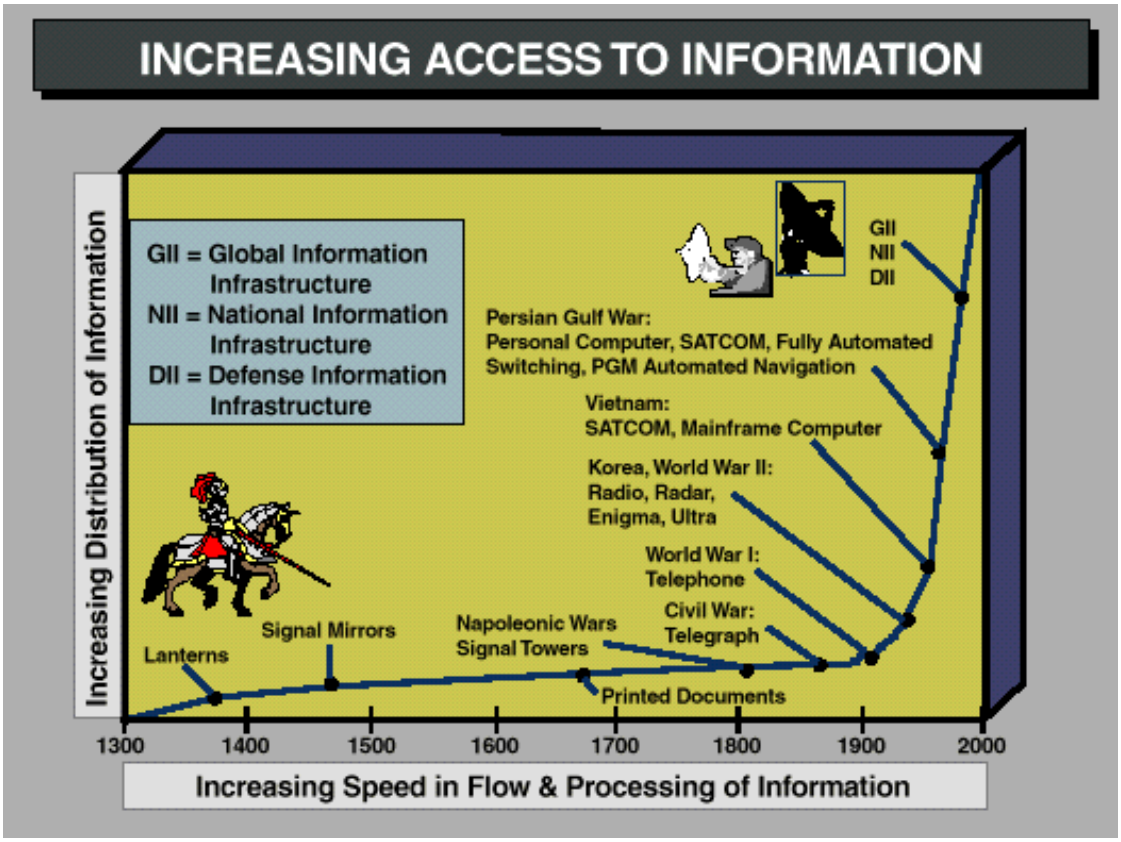
4. IW is a method of warfare to achieve objectives, rather than an objective in itself, in precisely the same manner that air or ground warfare are methods of warfare to achieve objectives. The means of conducting IW are varied and range from kinetic attack (e.g., iron bombs on target) through Computer Network Attack (CNA). We may use IW as a method to conduct strategic attack and interdiction, just as we may use air or ground warfare to conduct strategic attack and interdiction.

L. "Special information operations" are IO that, by their sensitive nature and due to their potential affect or impact, security requirements, or risk to the national security of the US, require a special review and approval process.

III. FUNDAMENTALS OF INFORMATION OPERATIONS
(drawn from Joint Pub 3-13)

A. General.

1. **Increasingly complex information systems** are being integrated into traditional warfighting disciplines such as mobility; logistics; and command, control communications, computers, and intelligence (C4I). Many of these systems are designed and employed **with inherent vulnerabilities** that are, in many cases, the unavoidable consequences of enhanced functionality, interoperability, efficiency, and convenience to users. The **broad access** to, and use of, these information systems enhances warfighting. However, **these useful capabilities induce dependence, and that dependence creates vulnerabilities**. These information systems are a **double edged sword**—on one edge representing areas that warfighting components must protect, while on the other edge creating new opportunities that can be exploited against adversaries or used to promote common interests.



2. **IO capitalize on the growing sophistication, connectivity, and reliance on information technology**. IO target information or information systems in order to affect the information-based process, whether human or automated. Such information dependent processes range from NCA-level decision making to the automated control of key commercial infrastructures such as land and space-based telecommunications and electric power.

3. Many different **capabilities and activities must be integrated** to achieve a coherent IO strategy. **Intelligence and communications support** are critical to conducting offensive and defensive IO. The thoughtful design and correct operation of information systems are fundamental to the successful conduct of IO. Moreover, to be successful, **IO must be integrated with other operations** (air, land, sea, space, and special) and contribute to national and military objectives.

4. IO support the national military strategy but **require support, coordination, and participation by other USG departments and agencies** as well as commercial industry. Although much of DOD information flows depend on commercial infrastructures, in many cases the protection of these infrastructures falls outside the authority and responsibility of DOD.

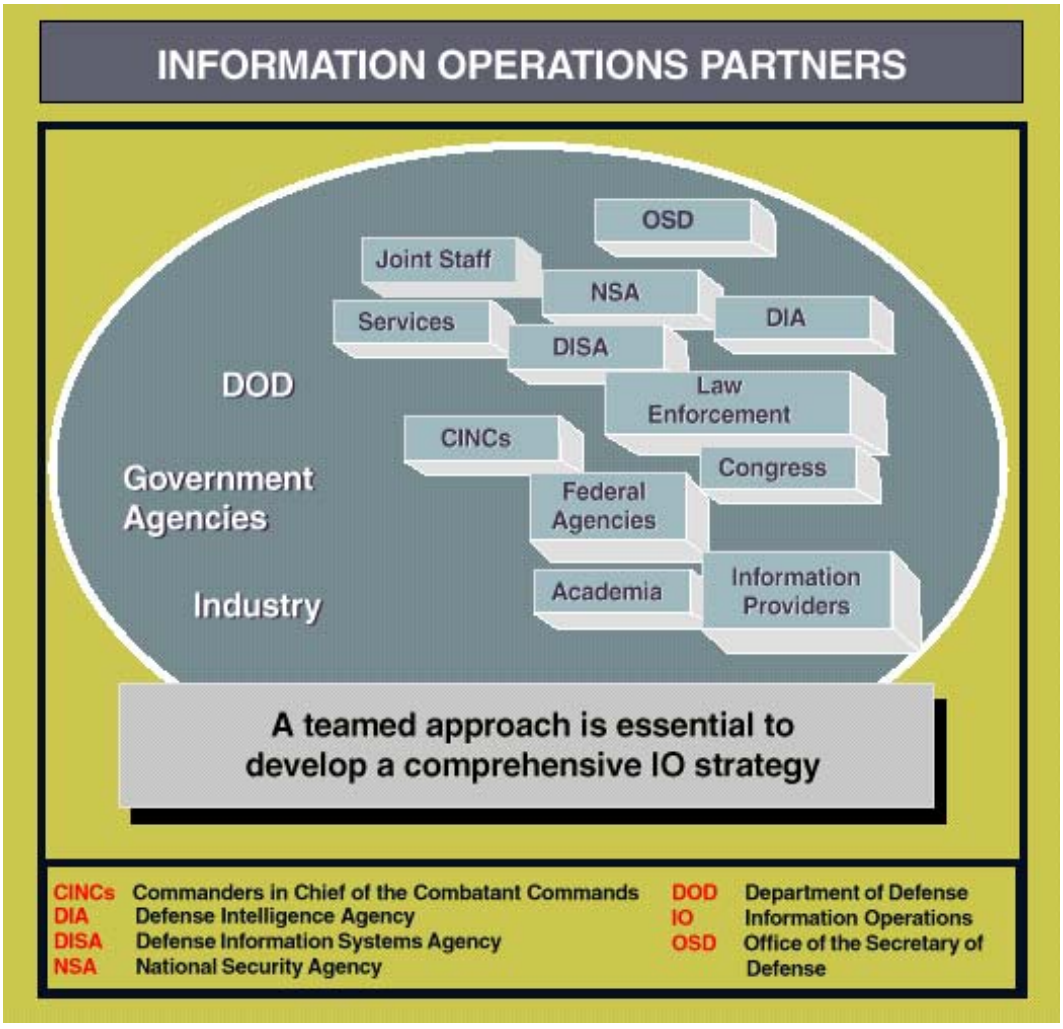
5. Several **fundamental legal considerations** must be taken into account during all aspects of IO planning and execution. The staff judge advocate should be an integral part of the planning and execution of such operations. Legal considerations include, but are not limited to, an assessment of the following:

    a. The different legal limitations that may be placed on IO in peacetime, crisis, and conflict (to include war). Legal analysis of intended wartime targets requires traditional Law of War analysis.

    b. The legal aspects of transitioning from defensive to concurrent offensive operations.

    c. Special protection for international civil aviation, international banking, and cultural or historical property.

d. Actions that are expressly prohibited by international law or convention. Examples include, but are not limited to: (1) Destruction resulting from space-based attack (Convention on International Liability for Damage Caused by Space Objects); (2) Violation of a country's neutrality by an attack launched from a neutral nation (Hague Convention V); and (3) PSYOP broadcasts from the sea, which may constitute unauthorized broadcasting (UN Convention on the Law of the Sea).



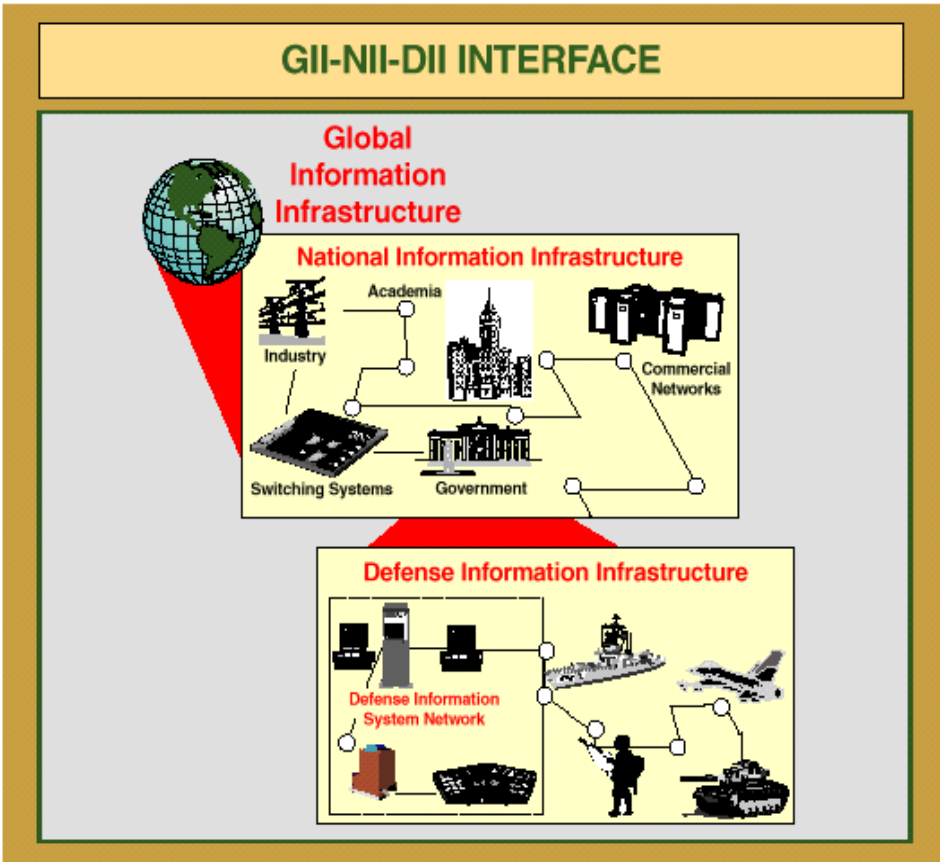
B. Information Environment.

1. The growth of information systems and technologies offer **continuing potential for exploiting the power of information in joint warfighting**. **Open and interconnected systems are coalescing into a rapidly expanding global information infrastructure (GII)** that includes the US national information infrastructure (NII) and the defense information infrastructure (DII).

2. **The GII is the worldwide interconnection of communications networks, computers, databases, and consumer electronics** that make vast amounts of information available to users. It encompasses a wide range of equipment, including cameras, scanners, keyboards, facsimile machines, computers, switches, compact disks, video and audio tape, cable, wire, satellites and satellite ground stations, fiber-optic transmission lines, networks of all types, televisions, monitors, printers, and much more. The GII includes more than just the physical facilities used to store, process, and display information. The personnel who make decisions and handle the transmitted information constitute a critical component of the GII.

3. The **NII** is similar in nature and purpose to the GII but relates in scope only to a **national information environment**, which includes all government and civilian infrastructures.

4. **The DII is embedded within and deeply integrated into the NII**. Their seamless relationship makes distinguishing between them difficult. The DII is the shared or interconnected system of computers, communications, data applications, security, people, training, and other support structures serving DOD local, national, and worldwide information needs. The DII connects DOD mission support, C2, and intelligence computers through voice, telecommunications, imagery, video, and other multimedia services. It provides information processing and services to subscribers over the Defense Information Systems network. It includes C2, strategic, tactical, intelligence, and commercial systems to transmit DOD information.



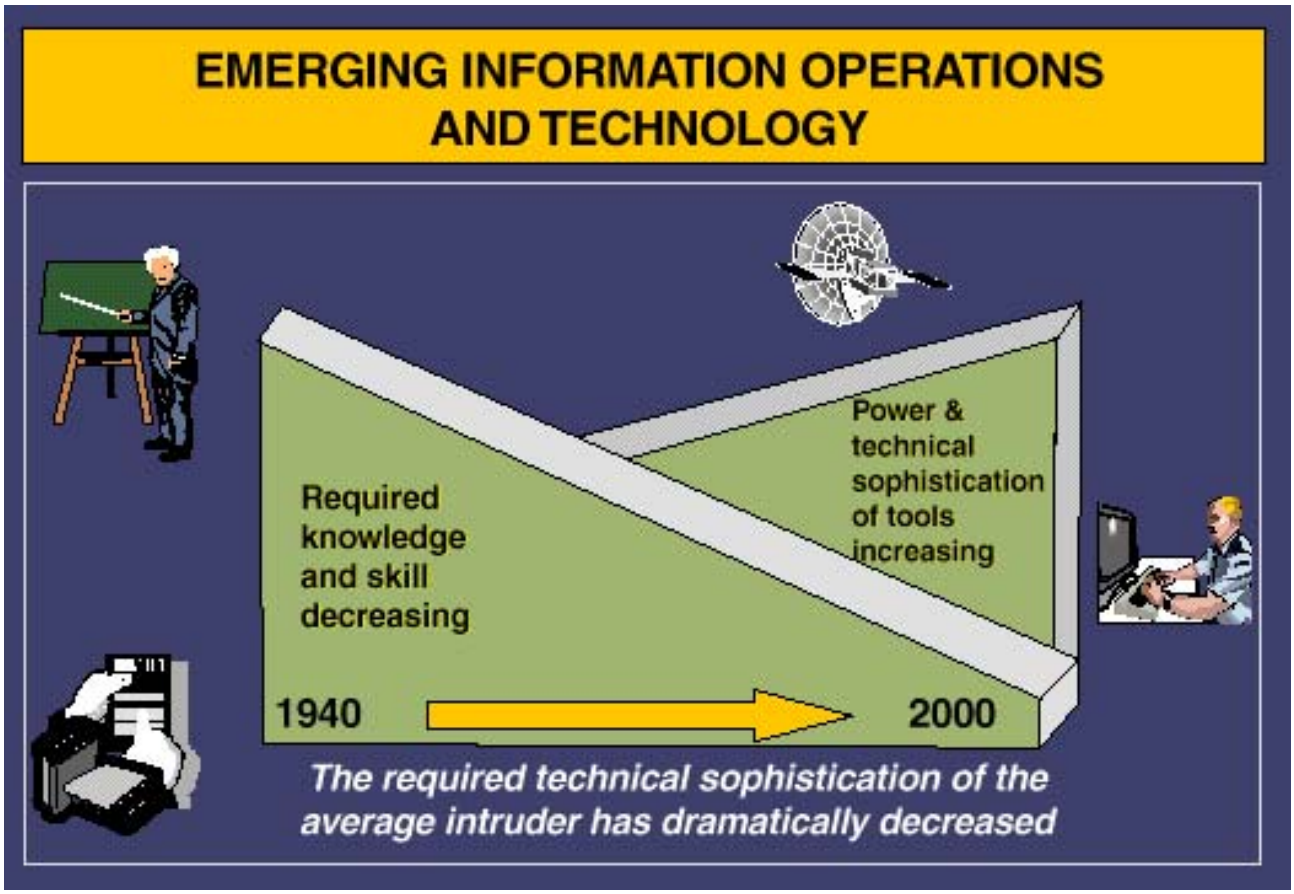
C. Reachback Dependencies.

1. Military planners at all levels of command should understand the nature, complexities, and dependencies of the GII, NII, and DII.

2. The successful conduct of operations requires **access to information available outside the operational area**. Information infrastructures no longer parallel traditional command lines, and warfighters need **frequent, instant, and reliable access to information** at locations in the continental United States as well as in theater. For example, mobility and sustainment of forces are highly dependent on commercial infrastructures that include international telecommunications, the public switched network, commercial satellites and ground stations, transportation systems, and electric power grids. Joint forces require secure video teleconferencing, database connectivity, direct downlink, and broadcast/receive capabilities for reachback access to intelligence, logistics, and other essential support data.

3. Providing capabilities to support crises and contingency operations requires the **expansion of our information infrastructure beyond the established peacetime information environment**. Joint forces must have assurance that this expanded infrastructure can attain the level of protection required to assure mission success.

4. **US dependence on information and information systems**, and the resultant vulnerabilities this entails, **exposes the United States to a wide range of threats**. These threats include, but are not limited to, computer hackers, criminals, vandals, terrorists, and nation states, and have brought focus and compelling relevance to our vulnerabilities to emerging technologies. The dramatically increased power and availability of computers and their telecommunications connections and computer applications have set in motion revolutionary capabilities that will enhance and support all aspects of military operations.



D. IO Target Set. IO targets are determined by the Joint Force Commander's objectives and operations concepts and are largely influenced by in-depth intelligence analysis. The Joint Force must determine the vulnerabilities and critical elements of friendly and adversary information, information-based processes, and information systems.

1. **Early identification of critical elements** with respect to specific IO targets is essential for successful offensive and defensive IO. Understanding the nature of the threat will help defend and protect against adversary IO.

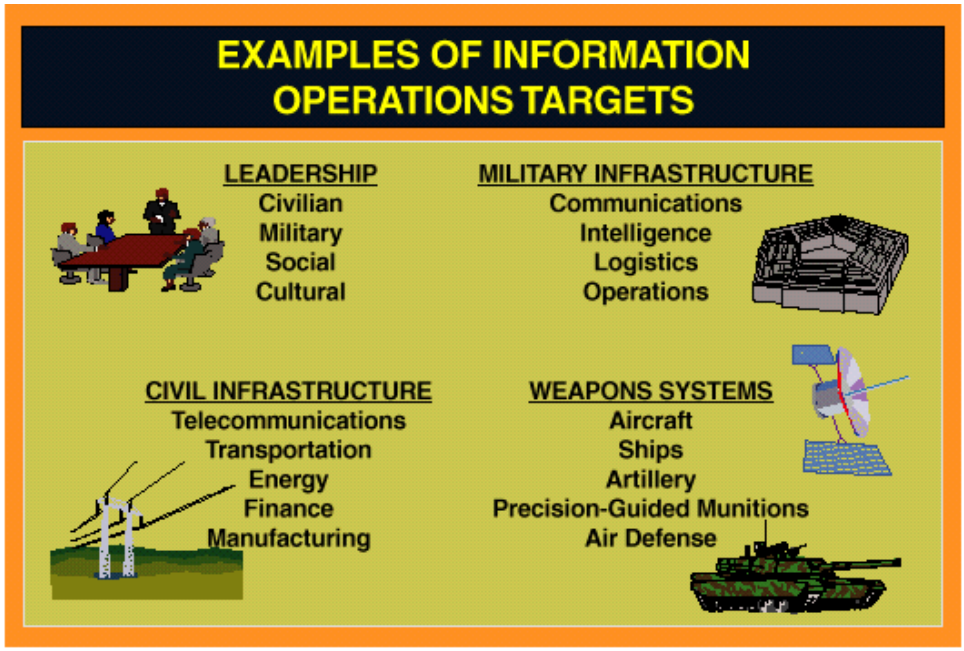
   a. **Offensive IO may target only a key element** of a specific critical adversary target set and attain great success.

   b. Conversely, understanding the nature of the threat will help defend and protect against adversary IO. An IO threat should be defined in terms of a specific adversary's intent, capability, and opportunity to adversely influence the elements of the friendly information environment critical to achieving objectives.

   c. An **IO threat** is an adversary that is organized, resourced, and politically sponsored/motivated to affect decision-makers. Hackers, criminals and organized crime, insiders, industrial and economic espionage, and, in some cases, terrorism constitute a general threat to the protected information environment. This general threat requires monitoring for indications of a specific IO threat and subsequently may require additional defensive IO measures.

2. **Command and control (C2) remains a substantial target for IO**. Commercial communications systems linked to friendly and adversary C2 systems offer unique challenges to offensive targeting and defensive protection.

3. **Examples of key areas of warfare support** comprising potential offensive target sets and requiring protection include, but are not limited to, **logistics, intelligence**, and **non-C2 communications systems**. Friendly commercial infrastructures also may be targeted by an adversary's offensive capabilities, just as friendly offensive capabilities may target an adversary's commercial infrastructures.



E. Special Operations Forces Support to IO. The unique capabilities of SOF enable the Joint Forces Commander to access, alter, degrade, delay, disrupt, deny, or destroy adversary information systems throughout the range of military operations and all levels of war.

F. Activities Related to IO. The following activities relate to and support the conduct of IO.

1. **Public Affairs (PA)**. **PA seek a timely flow of information** to both external and internal audiences. PA programs contribute to information assurance by disseminating factual information. Factual information dissemination counters adversary deception and propaganda. Coordination of PA and IO plans is required to ensure that PA initiatives support the commander's overall objectives, consistent with the DOD principles of information. PA and IO efforts will be integrated consistent with policy or statutory limitation and security.

2. The **news media** and **other information networks'** increasing availability to society's leadership, population, and infrastructure can have significant impact on national will, political direction, and national security objectives and policy.

3. **Civil Affairs (CA)**. **CA activities are an important contributor to IO** because of their ability to interface with key organizations and individuals in the information environment. CA activities can support and assist the achievement of IO objectives by coordinating with, influencing, developing, or controlling indigenous infrastructures in foreign operational areas.

G. Intelligence Support. **Intelligence support is critical to the planning, execution, and assessment of IO**.

1. The conduct of IO requires unique and detailed intelligence never before asked of intelligence collection agencies and activities. Intelligence preparation of the battlespace (IPB) is vital to successful IO. Support from non-DOD and non-US sources may also be required.

2. IO products must support IO planning, execution, and assessment; provide analysis of a potential adversary's IO capabilities and intentions; and help support the indications and warning (I & W) process.

H. IO as an Enabler to Combatant Commanders.

1. Rapidly advancing information-based technologies and an increasingly competitive global environment have thrust information into the center stage in society, government, and warfare in the 21st century. Information and information-based technologies are pervasive and impact every facet of warfighting from planning, deployment and sustainment, post-conflict, and redeployment process to the plethora of forces and weapons systems employed by Joint Forces.

2. All forms of national power, to include military operations in particular, are dependent on many simultaneous and integrated activities that, in turn, depend on information systems. This is especially true of those activities associated with critical C2 processes. Some of these activities include conducting strategic deployment, sustaining theater forces, ensuring force protection—both in garrison and in forward-deployed areas, preserving theater strategic C2, and developing strategic and theater intelligence.

3. Information itself is a strategic resource vital to national security. This reality extends to warfighters at all levels. Increasingly complex information systems are being integrated into traditional disciplines such as mobility, logistics, and C4I.

4. If carefully conceived, coordinated, and executed, IO will make an important contribution to combatant commanders' efforts to defuse crises and return to peace, reduce periods of confrontation, enhance the impact of other elements of national power, and forestall or eliminate the need to employ forces in combat situations. Simultaneously, IO also must prepare the battlespace for conflict and should enhance the ability of all components to conduct successful combat operations.

OUTLINE OF INTERNATIONAL LEGAL ISSUES IN INFORMATION OPERATIONS (drawn from DOD General Counsel paper, *An Assessment of International legal Issues in Information Operations, except as otherwise footnoted*)

We can make some educated guesses as to how the international legal system will respond to information operations, but the direction that response actually ends up taking may depend a great deal on the nature of the events that draw the nations' attention to the issue. If information operations techniques are seen as just another new technology that does not greatly threaten the nations' interests, no dramatic legal developments may occur. If they are seen as a revolutionary threat to the security of nations and the welfare of their citizens, it will be much more likely that efforts will be made to restrict or prohibit information operations by legal means.[37]

I. INTRODUCTION

A. Sources and Application of International Law.

1. Sovereign states are legally equal and independent actors in the world community; and assume legal obligations only by affirmatively acting.

2. States may be legally bound by:

   a. Treaties/International agreements (whether bilateral or multilateral);

   b. Customary international law, which consists of practices that have been so widely followed by the community of nations, with the understanding that compliance is mandatory, that they are considered to be legally binding.

   c. International institutions (like the United Nations) created by treaty and invested with legislative authority to create binding legal obligations.

[37] U.S. DEP'T OF DEFENSE, OFFICE OF GENERAL COUNSEL, PAPER, *AN ASSESSMENT OF INTERNATIONAL ISSUES IN INFORMATION OPERATIONS*

3. Voluntary compliance is the primary mechanism that makes Int'l Law effective. Enforcement mechanisms in International law include:

   a. Threat of sanctions.

      (1) UN Security Council is invested with coercive authority to maintain or restore International peace and security.

      (2) Possibility of international litigation before the International Court of Justice and other judicial tribunals also exists.

   b. Self-help enforcement mechanisms, including:

      (1) The right to use force in individual and collective self-defense; and

      (2) The right (in some circumstances) to repudiate treaty obligations violated by another party.

   c. An aggrieved nation's withdrawal from voluntary relationships involving diplomatic representation and most kinds of commerce.

   d. Public complaint to exact diplomatic costs against offending nations.

4. International legal obligations and international enforcement mechanisms apply to sovereign states and generally do not apply to individual persons except where a nation enforces certain principles of international law through its domestic criminal law, or in a very limited class of serious offenses (war crimes, genocide, crimes against humanity, and crimes against peace) that nations have agreed may be tried and punished by international criminal tribunals.

B. Essentials of Treaty Law.

1. Under US domestic law important distinctions exist between Treaties and Executive Agreements. The distinction primarily involves issues of Constitutional authority within the US government, but is of little importance internationally.

2. Treaty obligations are binding on their parties, but international law recognizes certain circumstances in which a nation can regard a treaty obligation as suspended, modified, or terminated.

   a. Generally, unless the terms of the agreement establish a right of unilateral withdrawal, a nation may not unilaterally repudiate or withdraw from a treaty unless it has a basis for doing so that is recognized under international law.

   b. A fundamental change of circumstances may justify a party to regard its treaty obligations as suspended or terminated.

      (1) Initiation of armed conflict may constitute such a change.

         [a] Some international agreements specifically provide that they will remain in effect during armed conflict between the parties, such as law of war treaties and the UN Charter.

         [b] Most treaties are silent on the issue.

         [c] Issues further complicated when the relevant treaty is multilateral rather than bilateral.

         [d] Where parties to a multilateral agreement are engaged in armed conflict, the treaty may be suspended as between the belligerents, but remain in effect among belligerents and other parties.

c. US is party to a variety of bilateral and multilateral agreements containing obligations that may affect information operations.

(1) SJA must determine which agreements are likely to remain in effect during hostilities.

(2) Test for continuing effect:

[a] Does specific treaty language address effect of hostilities? If not,

[b] Is treaty's object and purpose compatible with a state of armed hostilities between the parties?

C. New Legal Challenges presented by Information Operations.

1. Application of international law to some traditional military activities now associated with "information operations" and "information warfare" is reasonably well settled. These include **physical attack on information systems by kinetic means**, **psychological operations**, **military deception**, and **jamming radar** and **radio signals**. Similarly, existing legal principles may well apply to use of **electromagnetic pulse** (EMP) **weapons** and **directed energy weapons** such as lasers, microwave devices, and high-energy radio frequency (HERF) guns. On the other hand, it may not be as easy to apply existing international legal principles to a form of information attack doctrinally referred to as **computer network attack (CNA).** CNA operations employ electronic means to gain access to, disrupt, degrade, or destroy information resident in computer networks, or the computers and networks themselves (i.e., "hacking" or "cyber attack." of another nation's computer systems).

2. Global communications are almost seamlessly interconnected and virtually instantaneous, making distance and geographical boundaries essentially irrelevant to CNA.

a. Equipment necessary for CNA is readily available and inexpensive, and access to many computer systems can be obtained through the Internet.

b. Result: many information systems are subject to CNA anywhere and anytime.

[1] Actor may be a foreign state, an agent of a foreign state, an agent of a non-governmental entity or group, or an individual acting for purely private purposes.

[2] Major implications:

[A] **Attribution** of attack to a foreign state and **characterization** of intent and motive underlying attack may be very difficult.

[B] Attacker may not be physically present at situs of attack.

[C] Means of attack, except in form of anonymous and invisible radio waves or electrons, may not be tangibly present.

3. All of this significantly complicates application of traditional international law principles which developed in response to territorial invasions and attacks by troops, aircraft, vehicles, vessels and kinetic weapons that the victim could see and touch, and whose sponsor was usually readily apparent.

4. For purposes of addressing how existing international legal principles may apply to information operations, the following analysis initially assumes away issues of attribution and characterization, but will return to them later.

II. THE LAW OF WAR

A. Essentials of the Law of War (LOW).

1. LOW applies during international armed conflict.

   a. LOW comprised of treaties & customary international law.

   b. US is party to 16 LOW treaties, annexes and protocols and several are pending Senate advice and consent to ratification.

2. **General Principles of the LOW** include:

   a. **Distinction of combatants from noncombatants**:

      (1) Combatants must distinguish themselves from noncombatants and may not use noncombatants or civilian property to shield themselves from attack.

      (2) Combatant immunity: combatants may not be punished for combatant acts consistent with the LOW.

      (3) Persons committing combatant acts without authorization are subject to prosecution.

   b. **Military necessity**:

      (1) Enemy combatants are declared hostile and they, their equipment and stores may be attacked at will.

      (2) Civilians and civilian property making a direct contribution to the war effort may be attacked, along with objects whose damage or destruction would produce a significant military advantage because of their location, purpose, or use.

(3) Noncombatants and civilian objects making no direct contribution to the war effort and whose damage or destruction would produce no significant military advantage, are immune from deliberate attack.

c. **Proportionality**.

(1) Collateral injury and damage to noncombatants and civilian property is not unlawful.

[a] Forseeable collateral damage must not be disproportionate in relation to the direct and concrete military advantage anticipated from the attack.

[b] Attacker has a responsibility to take reasonable steps to determine what collateral damage may result from a contemplated attack.

[c] Commander ordering attack must make proportionality judgment.

[d] Enemy failure of duty to separate troops/equipment from noncombatants and civilian property may affect calculus.

(2) "Military advantage" refers to an attack considered as a whole, in the full context of the war strategy, rather than merely the tactical gains anticipated from an isolated attack or particular parts of a specific attack.

d. **Superfluous injury**. Nations have agreed to ban certain weapons because they cause superfluous injury. Included among these are "dum-dum" bullets, projectiles filled with glass or nondetectable fragments, poisoned weapons, and laser weapons specifically deigned to cause permanent blindness to unenhanced vision.

e. **Indiscriminate weapons**. Nations have agreed to ban certain weapons because they cannot be directed with any precision against combatants. Included among these are bacteriological weapons and poison gas.

f. **Perfidy**.

(1) LOW provides visual and electronic symbols to identify persons and property protected from attack.

[a] Among these are prisoners of war (POW), POW camps, the wounded and sick, and medical personnel, vehicles, aircraft, and vessels.

[b] Any misuse of protected symbols to immunize a lawful military target from attack constitutes the war crime of **perfidy**. Known misuse of symbols may lead combatants to disregard them.

(2) It is unlawful to feign surrender, illness, or death to gain an advantage in combat, as well as to broadcast a false report of a cease-fire or armistice.

g. **Neutrality**.

(1) Traditionally, nations not engaged in armed conflict may declare themselves neutral and are entitled to immunity from belligerent attack, so long as they do not assist a belligerent.

(2) Neutral nations unable or unwilling to prevent a belligerent from use of the neutral's territory in a manner that gives it a military advantage to that belligerent may be subject to attack by an opposing belligerent.

(3) Considerable support exists for argument that neutrality has no application during a conflict in which force is employed pursuant to UN Security Council Chapter VII mandate.

B. Application of LOW to Information Operations.

It is not clear what information operation techniques will be considered to be "weapons," or what kinds of information operations may be considered to constitute armed conflict. **However, if the deliberate actions of one belligerent cause injury, death, damage, and destruction to the military forces, citizens, and property of another belligerent, those action are likely to be judged by applying traditional LOW principles. *DOD GC adopts a "results test."**

1. **Distinction of combatants from noncombatants**.

(a) Conduct of Computer network attack (CNA) launched far from its target makes it of no practical significance whether "combatants" distinguish themselves from noncombatants.

(b) **However**, LOW requires lawful combatants distinguish themselves from noncombatants by wear of a uniform, be trained in LOW, and serve under effective discipline, and responsible command.

(1) Thus, combatant information operations during international armed conflict must be conducted only by uniformed members of the armed forces.

(2) Combatant acts (including CNA) by non-military forces therefore are a violation of LOW.

[A] Individuals conducting such acts may be subject to criminal prosecution by the enemy or an international war crimes tribunal.

[B] Long-distance and anonymous nature of CNA may make detection and prosecution unlikely.

2. **Military necessity.**

(a) Both military and civilian infrastructures are vulnerable to CNA.

(b) During armed conflict, virtually all military infrastructures are lawful targets, but purely civilian infrastructures may not be attacked unless their location, use, or purpose makes an effective contribution to the enemy's war effort and their damage, destruction, or neutralization offers a definite military advantage to the attacker.

[1] Stock exchanges, banking systems, universities, and similar civilian infrastructures may not be attacked simply because a belligerent has the ability to do so.

[2] In long, protracted conflicts, damage to enemy's economy and research and development capabilities may well undermine its war effort, but in short and limited conflict it may be difficult to articulate any expected military advantage from attacking economic targets.

(c) Targeting analysis must be conducted for CNA just as it has traditionally been conducted for attacks using traditional kinetic weapons.

3. **Proportionality**.

(a) Attacks upon "dual-use" infrastructures (those used for both military and civilian purposes) require that commanders make reasonable efforts to discover forseeable collateral damage. Commanders must consider whether system contemplated for attack is essential to public health and safety.

(b) Proportionality principle operates in the same way whether an attack is conducted using traditional kinetic weapons or in the form of CNA.

(c) LOW places much responsibility for collateral damage upon a defending force that fails to separate military targets from noncombatants and civilian property.

[1] Military forces using civilian infrastructure for military purposes (or vice-versa) may make such infrastructure a lawful military target.

[2] Such use may be unavoidable, as when military traffic must move on civilian highways and railroads or military use of civilian communications systems.

[3] Where a choice exists, military systems should be kept separate from infrastructures used for essential civilian purposes.

(d) Military command and control (C2) systems are lawful targets. Civilian media generally are not, but circumstances may make them so. (Exp. Rwanda and Somalia, where civilian broadcast urged civilian population to commit acts of violence against members of other tribes, or against UN-authorized forces, respectively).

[1] Civilian media broadcasts directly interfering with mission accomplishment may present grounds for use of minimum necessary force to shut them down.

[2] The international community has yet to authoritatively determine lawfulness of use of force for psychological operations purposes, such as shutting down civilian media broadcasts for the sole purpose of undermining civilian population morale.

4. **Superfluous injury**.

(a) To date, no known information operations weapon or device exists that has potential for causing superfluous injury.

(b) However, all new weapons and weapon systems must be reviewed for compliance with domestic and international law, including the LOW, in accordance with DOD Directives and service implementing regulations.

5. **Indiscriminate weapons**.

(a) The LOW prohibition upon indiscriminate weapons may apply to IO techniques such as malicious logic, as when malicious logic launched against a military information system spreads to other information systems used by noncombatants to provide essential services, or by neutral or friendly nations.

(b) This LOW principle might be violated indirectly if the consequences of CNA was to release dangerous forces, such as opening floodgates of a dam, causing an oil refinery in a populated area to explode in flames, or causing release of radioactivity.

6. **Perfidy**.

(a) Combatant vessel or aircraft broadcast of agreed identification signals for medical vessel or aircraft constitutes a war crime.

(b) "*Morphing*" techniques used to create an image of the enemy's chief of state, etc. informing troops that an armistice or cease-fire agreement exists, if false, constitutes a war crime.

7. **Neutrality**.

(a) A belligerent nation has a right to demand that a neutral nation prevent belligerents from using its information systems that generate information, rather than merely relay communications.

[1] For example, belligerents may demand that neutrals not provide satellite imagery of that belligerent's forces, real-time weather information, precision navigation services, or other kinds of intelligence-producing systems such as intelligence and hydrophonic systems.

[2] If neutral is unable or unwilling to do so, other belligerent(s) may have limited right of self-defense to take necessary and proportionate action against neutral, (e.g., jamming) to prevent such use by the enemy.

(b) A limited exception exists for **communications relay systems**.

[1] Articles 8 and 9 of 1907 *Hague Convention respecting Rights and Duties of Neutral Powers and Persons in Case of War on Land* (US is a party) provides that "A neutral Power is not called upon to forbid or restrict the use on behalf of belligerents of telegraph or telephone cables or of wireless telegraph apparatus belonging to it or to Companies or private individuals," so long as such facilities are provided equally to both belligerents.

(c) **International consortia** present special problems.

[1] Where an international communications system is developed by a military alliance, such as NATO, few neutrality issues are likely to arise.

[2] Other international consortia provide satellite communications and weather data used for both civilian and military purposes and are comprised by membership that virtually guarantees not all members of the consortium will be allies in future conflicts. Current examples include" INTELSAT, INMARSAT, ARABSAT, EUTELSAT, and EUMETSAT.

[3] Consortia have attempted to deal with this possibility by limiting system uses during armed conflict. **Example:** INMARSAT agreement provides that its mobile communications service may be used "exclusively for peaceful purposes." However, INMARSAT nations have determined that this language permits use by UN Security Council authorized forces, even while engaged in armed conflict.

C. **Assessment**. Novel features of information operation exist and will require expansion and interpretation of established principles of the LOW. Nevertheless, the outcome of this process by extrapolation appears reasonably predictable. The LOW is probably the single area of international law in which current legal obligations can be applied with the greatest confidence to information operations.

III. INTERNATIONAL LAW GOVERNING THE USE OF FORCE AMONG NATIONS IN "PEACETIME."

This section focuses on the application of international law principles outside the context of international armed conflict and where no UN Security Council Chapter VII mandate exists, that is, during peacetime, including during the conduct of military operations other than war.

This section explores the manner in which international law on the use of force among nations is likely to apply to peacetime computer intrusions.

A. International Law Concerning the Use of Force among Nations.

1. "**Act of war**." An act of war is a violation of another nation's rights under international law so egregious that the victim would be justified in declaring war.

   (a) Declarations of war have fallen into disuse, and the *act of war* concept plays little role in the modern international legal system.

   (b) In any event, significant sanctions follow from much less serious violations of another nation's rights that would not traditionally be regarded as *acts of war*.

2. **UN Charter Article 2(4)** requires that UN member states "refrain in their international relations from the **threat or use of force** against the territorial integrity or political independence of any state, or in any other manner inconsistent with the purposes of the United Nations."

3. States may lawfully employ armed force in two circumstances.

   (a) **UN Security Council (UNSC) authorization under Chapter VII**. Articles 39, 41 and 42 of Chapter VII of the UN Charter provide that the UNSC may authorize use of coercive measures, including military force, to maintain or restore international peace and security, where it determines a threat to the peace exists, or a breach of the peace, or act of aggression has occurred.

[1] There is no requirement that a "threat to the peace" take the form of an armed attack, a use of force, or any other condition specified in the Charter. The UNSC has plenary authority to conclude that virtually any conduct or situation constitutes such, in response to which it can authorize remedial action of a coercive nature.

[2] The UNSC could determine that a CNA constituted a "threat to the peace."

[A] It seems unlikely that UNSC would take action on an isolated case of state-sponsored computer intrusion producing little or no damage.

[B] But, a CNA causing widespread damage, economic disruption, and loss of life might well precipitate UNSC action. Debate in such case might center upon the offender's intent and the **consequences** of the offending action, rather than upon the means employed.

(b) **Individual or collective self-defense**. Article 51 provides that "Nothing in the present Charter shall impair the inherent right of individual or collective self-defense if an **armed attack** occurs against a member of the United Nations, until the Security Council has taken measures necessary to maintain international peace and security."

[1] Article 51's language seems to limit its effect to attacks and invasions using traditional weapons and forces.

[2] Article 51, however, did not create right of self-defense; rather, it recognized a preexisting and inherent right that is broader in some respects than Article 51's language. "Inherent right of . . . self-defense" refers to right as it existed at customary international law, which included doctrines of "**anticipatory self-defense**" and "**self-defense in neutral territory**."

[A] **Anticipatory self-defense** permits a nation to strike the first blow if it has good reason to conclude that it is about to be attacked. **CJCSI 3121.01** (Standing Rules of Engagement for US Forces) implement this doctrine in their authorization of the use of force in response to an adversary's demonstration of "**hostile intent.**"

[i] State activities that convey hostile intent constitute a threat to use force, and a state which is the object of that hostile intent has the right to use necessary and proportional force to respond in anticipatory self-defense."[38]

[B] **Defense of nationals** is the right of a state to use force to neutralize a continuing threat located in the territory of a neutral state, but not acting on its behalf, when the neutral state is unable or unwilling to execute its responsibility to prevent the use of its territory as a base or sanctuary for attacks on another nation.

[3] **Acts of self-defense must satisfy the tests of necessity and proportionality, but need not use the same means as the provocation, nor be conducted against a similar type of target.** Further, past US actions in Libya in 1986, Iraq in 1993 and in Afghanistan and Sudan in 1998, seem to suggest that self-defense actions need not be contemporaneous with the provocation, particularly if the attacker is responding to a continuing course of conduct. The latter point is, however, subject to significant international debate and seemingly inconsistent with the traditional customary international law principle requiring that the necessity for self-defense action be "instant, overwhelming, and leaving no choice of means, nor moment for deliberation."

[38] SHARP, CRITICAL INFRASTRUCTURE PROTECTION: *A NEW ERA OF NATIONAL SECURITY* at 95.

4. "While the phrase 'use of force' is commonly understood to include a military attack of one state by the organized military of another state, i.e., an *armed attack*, some coercive state activities that fall short of an armed attack may also cross the thresholds of Article 2. The phrase 'use of force also applies to all agencies and agents of a state government, such as the organized military, militia, security forces, police forces, intelligence personnel, mercenaries, and other surrogate forces of volunteers."[39]

   (a) "The Article 2(4) prohibition on the use of force also covers physical force of a non-military nature committed by any state agency. . . . [U]narmed, non-military physical force may produce the effects of an armed attack prompting the right of self-defense laid down in Article 51."[40]

   (b) "Any destructive state activity intentionally caused within the sovereign territory of another state is an unlawful use of force."[41]

   (c) "A state never loses its right to use force in self-defense in response to a use of force within the meaning of Article 2(4), however, the right of self-defense under customary international law may not always justify an armed response."[42]

5. "The best way . . . to accurately predict what may be considered a use of force and an armed attack within the meaning of Articles 2(4) and 51 is by studying state practice. In addition to traditional, universally accepted examples such as an armed cross-border invasion, an armed attack may occur when a use of force or an activity not traditionally considered an armed attack is used in such a manner that it becomes tantamount in effect to an armed attack."[43]

B. Acts Not amounting to a Use of Force.

[39] *Id* at 82.
[40] *Id* at 101.
[41] *Id.*
[42] *Id* at 143.
[43] *Id* at 115.

1. "Violations of international law are not *per se* a use of force and the unlawfulness of those violations follows from international norms other than [UN Charter] Article 2(4)."[44]

2. In its 1949 decision in the Corfu Channel Case, the ICJ ruled that the intrusion of British warships into Albanian territorial waters, which it found without justification under international law, constituted a violation of Albania's sovereignty. The result seems to be recognition of a general international law of trespass, although the remedy may be limited to a declaratory judgment that the victim's rights have been violated.

3. The Permanent Court of International Justice, in its 1928 Chorzow Factory decision, declared that reparations were due to any nation whose rights under international law were violated by another nation. This concept is often referred to as the Doctrine of State Responsibility.

4. International law generally recognizes the right of a nation whose rights under international law have been violated, to take **countermeasures** against the offending state, in circumstances where neither the provocation nor the response involves the use of armed force. Example: In 1978 an arbitral tribunal ruled appropriate the US suspension of French commercial flights into Los Angeles after France suspended US flights into Paris.

   (a) The Doctrine of countermeasures distinguishes between those that would otherwise be violations of treaty obligations or of general principles of international law and **retorsions -** actions which may be unfriendly or even damaging, but which do not violate any international obligation.

   (b) The use of countermeasures is subject to the requirements of necessity and proportionality.

   (c) Examples of countermeasures accepted as lawful include: suspension of diplomatic relations, trade and communications embargoes, cutting off foreign aid, blocking assets belonging to the other nation, and prohibiting travel to or from the other nation.

5. A trend in international law is to provide a remedy for every violation of a nation's rights under international law.

---

[44] *Id* at 97.

(a) Some remedies are in the nature of self-help, such as armed self-defense, the interruption of commercial or diplomatic relations, or public protest.

(b) Other remedies may be sought from international institutions, such as an imposition of coercive measures by the international tribunal.

(c) Victim nation must choose the most effective available sanction.

(d) Nations contemplating actions that may violate rights of another nation under international law must attempt to accurately predict what sanctions such action may provoke.

C. Application of International Law to Computer Network Attacks.

1. How these principles of international law will be applied to CNA by the international community is unclear. Much will depend on how nations and international institutions react to the particular circumstances in which the issues are raised for the first time.

2. It seems likely that the international community will be more interested in the **consequences** of a CNA than in the means used.

   (a) Principles of international law **may** be seen to place "far-reaching restrictions on a state's activities in CyberSpace that 'attack' the critical infrastructure of another state and cause destructive effects. A state can cause significant property and economic damage, as well as human fatalities, in another state by utilizing the Internet to cause

      [1] flooding by opening the flood gates of a dam,
      [2] train wrecks by switching tracks for oncoming trains,
      [3] plane crashes by shutting down or manipulating air traffic control systems,
      [4] large chemical explosions and fires by readjusting the mix of volatile chemicals at an industrial complex,
      [5] a run on banks or a massive economic crisis by crashing stock exchanges,

and any number of other examples that are limited only by the imagination of the state actors. . . The effect can be the same, if not more severe, as if the destruction was caused by conventional kinetic means of warfare."[45]

(b) State activities in CyberSpace that constitute a use of force within the meaning of Article 2(4) may be conducted by any state agent—not just the military."[46]

(c) "[A]ny state activity in CyberSpace that intentionally cause any destructive effect within the sovereign territory of another state are an unlawful use of force."[47]

(d) "*Any* computer network attack that intentionally causes *any* destructive effect within the sovereign territory of another state is an unlawful use of force within the meaning of Article 2(4) that **may** produce the effects of an armed attack prompting the right of self-defense."[48]

3. If a CNA results in widespread civilian deaths and property damage, it **may** well be that the international community would not challenge the victim nation if it concluded that it was the victim of an armed attack, or an equivalent of an armed attack. Even if the systems attacked were unclassified military logistics systems, an attack upon such systems might seriously threaten a nation's security.

4. If a particular CNA is considered an armed attack or its equivalent, it would seem to follow that the victim nation would be entitled to respond in self-defense by CNA or by conventional military means to respond in self-defense.

(a) A state might respond in self-defense to disable the equipment and personnel used to mount the offending attack.

(b) In some circumstances it may be impossible or inappropriate to attack the specific means used, where for example, the personnel and equipment cannot reliably be identified, or an attack would not be effective, or an effective attack might result in disproportionate collateral damage.

[45] *Id* at 101-102.
[46] *Id* at 143.
[47] *Id* at 102.
[48] *Id* at 140.

(c) In such cases, any legitimate military target could be attacked, as long as the purpose of the attack is to dissuade the enemy from further attacks or to degrade the enemy's ability to undertake them (i.e., not in "retaliation" or reprisal).

(d) A nation considering such action must make its best judgment on how world opinion, or the UNSC or ICJ is likely to apply self-defense doctrine to electronic (CNA) attacks.

5. It seems beyond doubt that any unauthorized intrusion into a nation's computer systems would justify that nation in taking self-help action to expel the intruder and to secure the system against reentry.

6. Though the issue has yet to be addressed in the international community, unauthorized electronic intrusion may be regarded as a violation of the victim's sovereignty, or even as equivalent to a physical trespass into that nation's territory. Such intrusions create vulnerability, since the intruder had access to information and may have corrupted data or degraded the system.

7. As a minimum, a victim nation of an unauthorized computer intrusion has the right to protest such actions if it can reliably characterize the act as intentional and attribute it to agents of another nation.

D. An "Active Defense" against Computer Network Attacks.

The initial discussion assumes knowledge of the computer attacker's identity and confidence in US ability to characterize his intent.

1. Persistent unauthorized foreign intrusions into a nation's computer systems **may** indicate a continuing danger that requires coercive measures to stop the intruder's pattern of conduct.

2. Similarly, a single foreign electronic attack causing significant damage to a system critical to national security or data stored in it, or where an intruder's conduct or the context of the activity clearly manifest malicious intent, may justify a nation in taking self-defense action.

(a) A victim nation may be justified in launching a computer attack in self-defense, intended to disable the equipment used by the intruder.

(b) A responsive CNA, as a measure in self-defense against foreign CNA, minimizes issues of proportionality relative to the application of traditional military force (e.g., launching a cruise missile at the building housing the offending system).

(1) Any response to foreign CNA is likely to be analyzed under traditional self-defense criteria of necessity and proportionality.

(2) Any legitimate military target may be attacked in self-defense, if it is impractical to focus an attack on the equipment used in the provocation.

[a] However, the ability to demonstrate a nexus between the provocation and the responsive action is important in the court of world opinion, as well as under the international law principles of self-defense.

[b] The next most attractive target may be the offending nation's communications systems or military intelligence chain of command.

The above legal analysis may change if the identity and location on intruder is uncertain, or if his intent is unclear.

3. **Attribution problems**. Identification of a CNA originator has often been a difficult problem, especially when the intruder has used a number of intermediate relay points, when he has used an anonymous bulletin board whose function is to strip away all information about the origin of messages it relays, or when he has used a device that generates false origin information.

(a) However, progress has been made in this area and reliable identification of the computer that originated a message may soon be routinely available.

(b) Locating an originating computer does not entirely resolve attribution problems, since a computer may have been used by an unauthorized user, or by an authorized user for an unauthorized purpose.

(c) Thus, the US must act cautiously in implementing "active defense" systems for government computers. Nevertheless, circumstances may arise in which the urgency of protecting critical information systems may warrant adoption of a properly deigned "active defense."

4. **Characterization problems**. Characterization of an intruder's intentions may be difficult. However, factors such as persistence, sophistication of methods used, targeting of especially sensitive systems, and actual damage done may persuasively indicate both the intruder's intentions and the dangers to the system in a manner that would justify an "active defense."

5. **State-sponsored actor problems.** A determination that a CNA was originated from a foreign country is only a partial solution to the attribution problem, since the attack may or may not have been state-sponsored.

(a) **State-sponsored attacks** may generate the right of self-defense, while attacks that cannot be shown to be state-sponsored generally do not.

(b) **State sponsorship** might be persuasively established by signals or human intelligence, the location of the offending computer within a state-controlled facility, or public statements by officials. It might also be inferred from the state of relationships between the countries, the prior involvement of the suspect state CNA, the nature of the systems attacked, the nature and the sophistication of the methods and equipment used.

(c) **Non-State-sponsored CNA**. When individuals carry out malicious acts for private purposes against the interests of one state from the territory of a second state, the aggrieved state does not generally have the right to use force in self-defense against either the second state itself or the offending individual.

(a) A state in which a responsive attack was conducted (if it became aware of it) could argue that its sovereignty and territorial integrity had been violated.

(b) The general expectation in international law is that a nation whose interests are damaged by the private conduct of an individual who acts within the territory of another state will notify the government of that nation and request its cooperation in stopping the offending conduct.

(c) Only if the requested nation is unable or unwilling to prevent recurrence does the doctrine of self-defense permit the injured nation to act in self-defense inside the territory of another nation.

[1] At some point, providing safe refuge for those who conduct attacks against another nation becomes complicity in those attacks.

[2] At a minimum, the offended nation is authorized to attack its tormentors, the terrorists.

[3] As complicity shades into the kinds of active support that are commonly called "state sponsorship," military and leadership targets of the host state may themselves become lawful targets for acts of self-defense.

[4] Attacks on insurgents or on terrorists and other criminals using a neutral nation's territory as a refuge may also be justified when the neutral state is unable to satisfy its obligations.

6. The international law of self-defense would not generally justify acts of "active defense" across international boundaries unless the provocation could be attributed to an agent of the nation concerned, or until the sanctuary nation had been put on notice and given the opportunity to put a stop to such private conduct in its territory and has failed to do so, or the circumstances demonstrate that such a request would be futile.

(a) Nevertheless, the National Command Authorities (NCA) might decide to take self-defense action by attacking a computer system in a foreign nation and take the risk of having to apologize or pay compensation to the offended government.

(b) In making this decision, the NCA might consider the danger presented to US national security from continuing attacks, whether immediate action is necessary, how much the sanctuary government is likely to object, and how the world community is likely to respond.

7. Use of a nation's public communications networks as a conduit for an electronic attack would not be a violation of its sovereignty.

(a) No established principle of international law prohibits routing a destructive message through a nation's communications networks.

(b) Even during an international armed conflict international law does not require a neutral nation to restrict the use of public communications networks by belligerents.

(c) A transited state would have grounds to complain if the attacking state obtained unauthorized entry into its computer systems as part of the path to the target computer.

[1] A transited state would be even more offended if malicious logic directed against a target computer had harmful effects against its own equipment, operating systems, or data.

[2] The launching state must consider the possibility of collateral damage to transited systems as part of its targeting analysis.

8. It may be possible to specify certain information systems that are vital to national security—both government systems and key civilian infrastructure systems.

(a) This process should serve both to give such systems high priority for security measures and to identify a class of systems any attack on which would immediately raise the issue of whether an active defense should be employed.

(b) This would not eliminate consideration of using active defense against attacks on systems not on such a "vital systems" list where the circumstances justify action.

9. It would be useful to create a process for determining when the response to a computer intrusion should shift from the customary law enforcement and counter-intelligence modes to a national defense mode.

10. A variety of treaty obligations, discussed below, must be considered before adopting an "active defense" against foreign CNA. Additionally, a variety of domestic legal concerns may impact information operations.

E. **Assessment**. It is far from clear the extent to which the world community will regard CNA as "armed attacks" or "uses of force," and how the doctrine of self-defense will be applied to CNA. The most likely result is an acceptance that a nation subjected to a state-sponsored CNA can lawfully respond in kid, and that in some circumstances it may be justified in using conventional military means in self-defense. Unless nations decide to negotiate a treaty addressing CAN, international law in this area will develop through the actions of nations and through the positions the nations adopt publicly as events unfold. US officials must be aware of the implications of their own actions and statements in this formative period.

IV. SPACE LAW

A. Introduction.

1. International law regulating activities in outer space is important to information operations because space segments are critical to so many information systems.

   (a). The exclusive functions of both military and civilian satellites are to gather and relay information. These systems perform such functions as communications relay, imagery collection, missile warning, navigation, weather forecasting, and signals intelligence.

   (b). In the conduct of information operations, there will be strong imperatives to interfere with the adversary's space-based information systems, and to defend one's own.

2. One approach to attacking space systems is by targeting their ground stations. Another approach is to jam or "spoof" their communications links. Such actions are subject to the normal international law principles governing other terrestrial activity.

3. Sometimes, however, it may be more effective to attack the satellite or satellites that form the space segment of the system. Activities in space are subject both to general principles of international law and to a number of treaty obligations that apply specifically to space activities.

B. Space Law Treaties.

1. Four treaties, taken together, provide the foundations of existing space law.
   (a) *The Treaty on Principles Governing the Activities of States in the Exploration of Outer Space, including the Moon and Other Celestial Bodies* (the Outer Space Treaty, 1967).
   (b) *The Agreement on the Rescue of Astronauts, Return of Astronauts, and the return of Objects launched into Outer Space* (the Rescue and Return Agreement, 1968).
   (c) *The Convention on International Liability for Damages Caused by Space Objects* (the Liability Convention, 1972).
   (d) *The Convention on the Registration of Objects Launched into Outer Space* (the Registration Convention, 1975).

2. These treaties establish the following principles, now generally regarded as constituting customary international law.

   (a) Space is free for exploration and use by all nations. It is not subject to national appropriation by claim of sovereignty, use, occupation, or any other means.

   (b) Activities in space shall be conducted with due regard for the interests of other states.

   (c) States that launch space objects are liable for any damage they may do in space, in the air, or on the surface of the Earth.

      (1) A "fault" standard is applied where damage is done to other items in space.

      (2) An absolute liability standard is applied where damage is done on the surface of the Earth or to aircraft in flight.

   (d) Space activities are subject to general principles of international law, including the UN Charter.

3. The international legal regime regulating the use of force among nations during peacetime (discussed in Part III) applies fully to activities in outer space.

(a) States are obligated not to use force in their relations with each other unless they are acting in self-defense or when authorized by the UN Security Council.

(b) As with other forms of information operations, however, the issue remains what actions by or against objects in space will be considered uses of force.

(1) The world community would likely regard as uses of force, the destruction of a satellite by a missile or laser, or the taking control by one nation of another nation's satellites by electronic means, thereby causing the satellite to fall out of orbit (if this could be proven).

(2) The world community might consider lesser kinds of interference as not constituting a use of force, as where one nation by electronic means were to suspend the operations of another nation's satellite for a brief period, after which it returned it to service undamaged. This might, however, be considered a breach of the launching nation's sovereign rights.

4. During international armed conflict, the law of war would apply unless it was trumped by the principle of noninterference with space systems.

(a) Resolution of this issue depends on whether the four space treaties are considered to apply during armed conflict.

(1) None of the space treaties contains any specific provision indicating whether the parties intended that the agreement apply in wartime.

(2) A strong argument exists that the principle of noninterference established by these agreements is inconsistent with a state of hostilities, at least where the systems concerned are of such high military value that there is a strong military imperative for the adversary to be free to interfere with them, even to the extent of destroying the satellites in the system.

(b) It seems most likely that these agreements will be considered to be suspended between belligerents for the duration of any armed conflict, at least to the extent necessary for the conduct of the conflict.

(c) If the principle of noninterference is regarded as suspended for the period of the conflict, it also seems likely that the liability provisions in these agreements would also be suspended, at least between the parties. This would not, however, excuse belligerents from liability to neutral nations if their actions caused damage to their citizens or property.

C. **Specific Prohibitions of Military Activities in Space**.

1. Existing treaty restrictions on military operations in space are very limited and are included in the space treaties previously listed and in various arms control agreements.

2. The **Outer Space Treaty** provides that parties will not "place in orbit around the Earth any objects carrying nuclear weapons or any other kinds of weapons of mass destruction, install such weapons on celestial bodies [i.e., the moon, planets, and asteroids], or station such weapons in outer space in any other manner."

(a) The OST also prohibits the establishment of military bases, the testing of weapons, and the conduct of military maneuvers on the moon or other celestial bodies.

(b) The OST permits these activities in orbit around the Earth, and in other places in outer space.

(c) The OST does not prohibit establishment of military space stations or operating other satellites with offensive or defensive capabilities.

3. The *Treaty Banning Nuclear Weapons Tests in the Atmosphere, in Outer Space and Under Water* (the Limited Test Ban Treaty, 1963) prohibits all nuclear explosions in outer space.

   (a) Parties may not lawfully explode a nuclear device in outer space in order to disable an adversary's satellites by means of the **electromagnetic pulse** (EMP) generated by a nuclear explosion, or by its own effects.

   (b) A nation operating its own satellites are unlikely to take such action since its satellites (unless hardened against blast/EMP effects) would be subject to the same effects as its adversary.

4. The *Treaty on the Limitation of Anti-ballistic Missile Systems* (the ABM Treaty, 1972) provides that no party may "develop, test or deploy space-based ABM systems or components."

5. Under a 1997 theater missile defense (TMD) agreement not yet ratified by the Senate, the US and Russia agreed not to place in space theater missile defense interceptor missiles "or space-based components based on other physical principles, whether or not part of a system, that are capable of substituting for such interceptor missiles."

6. A number of arms control agreements provide that no party will interfere with the others' "national technical means of verification." Translated, this means no interference with the orbiting imaging systems used to monitor the strategic arms of another party.

7. Read together, these agreements permit the development, testing, and deployment of anti-satellite and satellite-defense systems unless they involve either the stationing or testing of nuclear devices in outer space or the orbiting of systems that also have ABM or ATM capabilities.

   (a) Anti-satellite and satellite defense system use id subject only to:

      (1) The general principles of international law relating to the use of force;

(2) The principle of non-interference with the space systems of other nations in peacetime, subject to the right to use force in self-defense and when authorized by the UN Security Council;

(3) The law of war during international armed conflicts; and

(4) Obligations under relevant arms-control agreements not to interfere with other parties' national technical means of verification.

(b) This leaves a very broad range of permissible "space-control" systems of operations.

8. In non-nuclear conflict, the Parties might very well determine that the treaty prohibitions against placing nuclear weapons in orbit, against exploding nuclear devices in outer space, and against placing ABM components and ATM interceptors in orbit remain consistent with a state of limited armed conflict.

(a) Those obligations may well serve to avoid escalation of the conflict to the nuclear level.

(b) The parties' conclusions as to the obligation not to interfere with other parties' national technical means of verification will probably depend to a great extent on the circumstances of the conflict.

D. **Domestic Law and Policy**.

1. A federal statute, 18 USC 1367, makes it a felony to intentionally or maliciously interfere with a communications or weather satellite, or to obstruct or hinder any satellite transmission.

2. US domestic policy on developing space control capabilities has been inconsistent.

(a) Following US Air Force development and testing of an anti-satellite missile in the 1980s, Congress decreed that no appropriated funds were to be used to test any weapon against an object in orbit.

(b) Later, following US Army testing of lasers as anti-satellite weapons, Congress prohibited the use of appropriated funds to illuminate any object in orbit with a laser.

(c) In the FY 98 DOD Authorization Act, Congress authorized funds for development of a Kinetic Energy Anti-Satellite Missile, which President Clinton vetoed with his short-lived line item veto authority.

(d) In the FY 99 DOD Authorization Act Congress authorized funds for space control projects and urged expenditure of the FY 98 funds restored following the Supreme Court's ruling that the line item veto was unconstitutional.

3. The US has not arrived at a consensus on the fundamental policy issues concerning space control. It seems likely that development of such systems will continue.

E. International Efforts to Control "Weaponization of Space."

1. Growing international support exists for a treaty banning weapons in space.

2. In December 1998, the UN General Assembly approved a resolution by a vote of 165-0-4 entitled "Prevention of an arms race in outer space." This resolution calls for reestablishment of a Conference on Disarmament (CD) Ad Hoc Committee on the prevention of an Arms race in Outer Space that existed in prior years.

F. Assessment.

1. No legal prohibition exists against developing and using space control weapons, whether employed in orbit, from an aircraft in flight, or from the Earth's surface.

2. Placing nuclear weapons in orbit and detonating a nuclear explosion in outer space are prohibited

3. The use of space control systems in peacetime would be subject to both the general principles of international law and to treaty obligations not to interfere with other nations' space systems and national technical means of verification.

4. These obligations would probably be suspended during international armed conflict, during which the parties' conduct would be governed primarily by the LOW.

5. US domestic policy on space control is unsetteled.

V. COMMUNICATIONS LAW

A. International Communications Law.

1. International communications law consists primarily of a number of bilateral and multilateral communications treaties.

(a) The *International Telecommunications Convention of 1982 (ITC)* (the Nairobi Convention) is the most significant.

[1] The ITC is the latest of a series of multilateral agreements which establish the International Telecomunication Union (ITU) (a specialized agency of the UN).

[2] These agreements invest the ITU with the authority to formulate telegraph and telephone regulations, which become binding legal obligations upon formal acceptance by ITU member nations.

[3] These agreements establish mutual legal obligations among parties, several of which are directly relevant to information operations.

(b) **ITC Article 35** provides that all radio "stations, whatever their purpose, must be established and operated in such a manner as not to cause harmful interference to the radio services or communications of other Members or of recognized private operating agencies, which carry on radio service, and which operate in accordance with the provisions of the Radio Regulations."

(1) **Annex 2 to the ITC** defines "harmful interference" as "interference which endangers the functioning of a radio navigation service or of other safety services or seriously degrades, obstructs or repeatedly interrupts a radio communication service operating in accordance with the Radio Regulations."

(2) This provision would appear to restrict information operations techniques that involve the use of radio broadcasting, for example, jamming or "spoofing" of a radio navigation service.

(c) **However**, **ITC Article 38** provides a specific exemption for military transmissions: "members retain their entire freedom with regard to military radio installations of their army, naval and air forces."

(1) Article 38 further provides: "Nevertheless, these installations must, so far as possible, observe . . . the measures to be taken to prevent harmful interference, and the provisions of the Administrative Regulations concerning the types of emission and the frequencies to be used, according to the nature of the service performed by such installations."

(2) This provision indicates that military installations do not have carte blanche to interfere with civilian communications, but the phrase "so far as possible," read together with the specific exemption for military radio installations, provides considerable room for military forces' information operations.

(d) The ITC permits member nations to interfere with international communications in certain circumstances:

(1) Article 19 allows members to "stop the transmission of any private telegram which may appear dangerous to the security of the State or contrary to their laws, to public order or to decency, provided that they immediately notify the office of origin of the stoppage of any such telegram or part thereof, except when such notification may appear dangerous to the security of the state."

(2) Article 19 also permits members to "cut off any private telecommunications which may appear dangerous to the security of the State or contrary to its laws, to public order or to decency."

(3) Article 20 reserves the right of members "to suspend the international telecommunications service for an indefinite time, either generally or only for certain relations and/or certain kinds of correspondence, outgoing, incoming or in transit, provided that it immediately notifies such action to each of the other members through the medium of the Secretary-General."

(e) It seems clear that ITC provisions apply primarily in peacetime. The treaty does not specifically state whether it applies during armed conflict.

(1) Ample precedent exists, however, in which nations have demonstrated conclusively that they regard international communications conventions as suspended between belligerents engaged in armed conflicts.

(2) Many parties to the ITC and other multilateral communications conventions will be neutrals in armed conflicts.

(3) Most ITC obligations will be considered suspended between the belligerents, but will remain in effect between each belligerent and the neutral parties, as well as among the neutral parties.

(f) The US has negotiated a number of bilateral communications agreements with nations where US military forces are stationed. Potential exists for such agreements to restrict or facilitate US military information operations.

B. Domestic Communications Law

ITC obligates each member nation to suppress acts by individuals or groups within its territory that interfere with the communications of other members.

(1) **47 USC § 502** implements this treaty obligation. It provides, "Any person who willfully and knowingly violates any rule, regulation, restriction, or condition . . . made or imposed by any international radio or wire communications treaty or convention, or regulation annexed thereto, to which the United States is or may hereafter become a party, shall, in addition to any other penalties provided by law, be punished, upon conviction thereof, by a fine of not more than $500 for each and every day during which such offense occurs."

(2) Department of justice, Office of Legal Counsel issued a written opinion providing in effect that 47 USC § 502 does not apply to actions of the US military executing instructions of the President acting within his constitutional powers to conduct foreign policy and to serve as Commander-in-Chief.

C. Assessment.

1. Neither international nor domestic communications law presents any significant barrier to US military information operations.

2. International Communications law contains no direct and specific prohibition against the conduct of information operations by military forces, even in peacetime.

3. Established state practice evidences that nations regard telecommunications treaties as suspended among belligerents during international armed conflict.

4. Domestic communications laws do not prohibit properly authorized military information operations.

VI. IMPLICATIONS OF OTHER TREATIES

The US is party to literally thousands of multilateral and bilateral international agreements. The US State Department compiles a list of all such agreements entitled *Treaties in Force.* Based on sheer numbers alone, it seems likely that some of these agreements will affect particular information operations activities. This section attempts only to highlight certain kinds of "typical" agreements that are likely to contain obligations relevant to the conduct of information operations.

A. Mutual Legal Assistance Agreements.

Mutual legal assistance agreements obligate parties to gather and provide evidence located in its territory concerning litigation or criminal prosecutions that occur within the jurisdiction of another party requesting such assistance. The US is party to several dozen legal assistance agreements.

B. Extradition Agreements.

Extradition agreements obligate parties in certain circumstances to deliver persons accused of crime to the other party for criminal prosecution. The US is party to more than 100 bilateral extradition treaties.

C. The United Nations Convention on the Law of the Sea (UNCLOS).

1. US is a signatory, but not a party. The treaty is before the Senate for advice and consent.

2. Many provisions of this treaty are considered to express customary international law.

3. **UNCLOS Article 19** obligates vessels exercising the right of innocent passage through a nations' territorial sea not to engage in activities "prejudicial to the peace, good order, or security of the coastal State." Prejudicial activities listed in Article 19 include:
   (a) "-any threat or use of force against the sovereignty, territorial integrity or political independence of the coastal State, or in any other manner in violation of the principles of international embodied in the Charter of the United Nations

(b) -any act aimed at collecting information to the prejudice of the defence or security of the coastal State

(c) -any act of propaganda aimed at affecting the defence or security of the coastal State

(d) -any act aimed at interfering with any systems of communication or any other facilities or installations of the coastal State."

4. **UNCLOS Article 109** provides that all "States shall co-operate in the suppression of unauthorized broadcasting from the high seas" and defines unauthorized broadcasting as "the transmission of sound radio or television broadcasts from a ship or installation on the high seas intended for reception by the general public contrary to international regulations."

(a) "International regulations" refers primarily to the Nairobi Convention and the ITU's radio Regulations discussed in section V above.

5. UNCLOS Article 113 requires parties to adopt domestic criminal legislation punishing willful or culpably negligent damage to submarine cables belonging to other parties by ships or persons under their jurisdiction.

6. These UNCLOS provisions have the potential to affect only a narrow category of information operations, but must be considered at least during peacetime, to those to which they do apply.

7. State practice conclusively establishes that Article 19's regime governing innocent passage through territorial seas will be suspended between belligerents. Likewise Article 113's protections for submarine cables would be considered as suspended between belligerents.

D. Treaties on Civil Aviation.

1. The US is **party** to a number of treaties concerning civil aviation, the most significant of which is the 1944 *Convention on International Civil Aviation* (the Chicago Convention).

2. The **Chicago Convention** establishes the International Civil Aviation Organization (ICAO) and provides a basic legal framework for international civil aviation.

(a) Chicago Convention does not directly apply to state aircraft, except for the obligation stated in Article 3(d).

(b) **Article 3(d)** provides: 'The contracting States undertake, when issuing regulations for their state aircraft, that they will have due regard for the safety of navigation of civil aircraft."

(c) **Article 28** provides that each party will provide navigation and communications services as agreed upon through ICAO procedures.

(d) **Article 37** provides that parties will comply with "international standards and recommended practices and procedures" on a variety of subjects including communications systems and air navigation aids.

3. The ICAO Council has adopted 18 technical Annexes to the Chicago Convention.

(a) **Annex 10**, Aeronautical Telecommunications, contains agreed provisions on aeronautical communications, navigation and surveillance. While military aircraft are not directly bound by these provisions, their obligation of "due regard" for the safety of civil aircraft generally includes an obligation not to interfere with these systems.

4. Chicago Convention **Article 89** addresses the Convention's application during armed conflict, providing, "In case of war, the provisions of this Convention shall not affect the freedom of action of any of the contracting States, whether as belligerents or as neutrals. The same principle shall apply in the case of any contracting State which declares a state of national emergency and notifies the fact to the Council."

(a) Many Convention provisions are inconsistent with a state of armed conflict, including the principle that aircraft not engaged in scheduled airline service have the right of free passage into or through the airspace of parties. These provisions would be considered suspended between the belligerents.

(b) However, other Convention provisions are not incompatible with a state of armed conflict and their obligations should not be considered as suspended. For example, Parties' obligations to carry out combatant activities with due regard for the safety of civil aviation.

F. Treaties on Diplomatic Relations.

1961 ***Vienna Convention on Diplomatic Relations.*** US is a party to this treaty which establishes obligations concerning the treatment of diplomatic personnel and premises.

1. Among the protections afforded a party's diplomatic mission in the territory of another state are the right to inviolability of:

   (a) **Article 2**: the premises of the mission;

   (b) **Article 24**: its "archives and documents";

   (c) **Article 30**: the private residences, papers, correspondence, and property cf diplomatic agents; and

   (d) **Article 27**: diplomatic communications. The treaty further provides that the mission may communicate with its government and other missions and consulates of its government by "all appropriate means, including diplomatic couriers and messages in code or cipher. However, the mission may install and use a wireless transmitter only with the consent of the receiving State."

2. The treaty imposes certain duties on diplomatic missions.

   (a) **Article 41** provides that mission personnel must respect the laws and regulations of the receiving State, that they may not interfere in the receiving state's internal affairs, and that the "premises of the mission must not be used in any manner incompatible with the functions of the mission as laid down in the present Convention or by other rules of general international law or by any special agreements in force between the sending and receiving States."

   (b) **Article 45** provides that the duties of the receiving state continue in force even in the case of armed conflict between the parties, or if diplomatic relations are broken off between them, even though the staff of the mission is recalled.

3. Any information operations activity involving diplomatic premises, persons, archives, documents, or communications, either as an instrument or as a target of the operation, must take into account these international legal obligations.

F. Treaties of Friendship, Commerce, and Navigation.

1. These bilateral agreements provide reciprocal arrangements for tourism, trade and transportation between parties.

2. Most FCN agreements contain no specific provisions on telecommunications and constitute the archetype agreement likely regarded as suspended during armed conflict.

G. Status of Forces and Stationing Agreements.

When military forces of one nation are present in the territory of another with its consent, the countries customarily execute written agreements establishing the rights and obligations of the parties concerning the visiting parties.

1. **Stationing agreements** establish the host nation's consent to foreign troop's presence, including agreements on numbers, equipment, permissible activities and facilities for their use.

2. **Status of forces agreements (SOFAs)** address the allocation of various kinds of legal jurisdiction over the visiting forces.

(a) US is a party to 103 SOFAs, most following the general pattern of the 1951 *Agreement Between the Parties to the North Atlantic Treaty Regarding the Status of Their Forces* (NATO SOFA).

(b) SOFAs are necessary because of an overlap of legal jurisdiction exercised by the **sending** and **receiving states**. The receiving state has jurisdiction over persons and activities within its territory, while the sending state has both the right and duty to exercise control over its armed forces.

(c) SOFAs allocate criminal and civil court jurisdiction between the two states and exempt the visiting force from certain taxes, customs fees and procedures, immigration formalities, and most host nation licensing and inspection requirements.

(d) SOFAs typically contain administrative claims procedures established for personal injuries and property damage caused by the visiting force.

(e) SOFAs contain provisions requiring visiting force members "respect" host nation laws.

3. SOFAs and stationing agreements contain provisions that must be taken into account if US military forces intend to engage in information operations while present in the territory of the receiving state. US forces must determine whether such agreements require host nation notification or consent.

(a) Such agreements frequently require that the US notify the host nation of any significant change in capabilities or uses of installations made available for US use.

(b) **Stationing agreements** often provide that US forces may install and use various communications equipment, but that such equipment must not interfere with host nation communications systems and must be in accordance with host nation laws and regulations. If equipment is to be used for information operations, US forces must determine whether contemplated activities are consistent with these obligations.

(1) Stationing agreements often authorize or obligate the visiting force to use the receiving state's military and civilian communications systems.

(2) US forces must consider the possibility that offensive information operations through host nation communications systems (if even permissible) may subject the host nation to countermeasures and acts of self-defense in peacetime, and may make them legitimate military targets during an armed conflict.

4. If a host nation discovers that its territory and facilities have been used without its knowledge as a base for US information operations of a nature that may tend to involve it against its will in a conflict or dispute, US diplomatic and military relations with the host nation are likely to suffer.

(a) While as a practical matter, CNA are difficult to identify, trace, and attribute, it will not always be impossible to do so.

(c) Accordingly, decisions to engage in information operations from its territory without the host nation's knowledge and consent, must be made at senior policy levels.

VII. FOREIGN DOMESTIC LAWS

A. Introduction.

1. Foreign domestic laws, like US criminal statutes addressing computer-related offenses, space activities, communications, and the protection of classified information, may have important implications for US forces' conduct of information operations.

2. The state of domestic laws dealing with high-tech misconduct varies enormously from country to country. This has important implications for US information operations because:

   (a) The state of a nation's domestic criminal law directly impacts the assistance that the nation's public officials can provide in suppressing certain behavior by persons operating in its territory; and

   (b) The state of the nation's domestic criminal law may have a significant effect on US information operations conducted in the nation's territory or involving communications through the nation's communications systems.

B. Cooperation in Investigations and Prosecutions.

1. Law enforcement officials may not prosecute an individual for conduct that is not defined as a crime in the applicable state.

2. Similarly, in most constitutional governments, law enforcement officials may conduct criminal investigations unless the alleged conduct constitutes a crime.

3. Domestic laws of some nations may permit the use of devices specifically designed to frustrate attempts to trace Internet communications to their source.

   (a) Devices such as anonymous remailers, strip of all information about the originator of a message, and make it possible for a computer "hacker" located anywhere— even in the US – to avoid identification by routing a message through the device.

(b) In this way, weaknesses in domestic law of one state may provide impunity to hackers everywhere. The weakest link therefore threatens law enforcement even in countries with robust and sophisticated laws.

C. Effect of Foreign Domestic Law on US Information Operators' Actions.

1. US forces must determine whether local laws prohibit contemplated information operations activities. These prohibitions are important because:

(a) Individuals who order or execute prohibited activities might be subject to prosecution in a host nation criminal court; and

(b) Commanders might feel obligated on a policy basis to refrain from issuing such an order.

2. US military members who order or execute acts in the course of their official duties overseas, that are a crime under host nation law, may be subject to prosecution in that nation's criminal courts.

(a) Under many US SOFAs, official acts fall within the primary jurisdiction of the sending state (US), but only where such act is a crime under both US and host nation law, or only under US law.

(b) The host nation has exclusive jurisdiction to prosecute where the alleged conduct constitutes an offense only under its law.

(1) US has consistently maintained that foreign criminal prosecution of a US military member for performing acts lawful under US law in the execution of official duties would be intolerable.

(2) Theoretically, this problem might arise, for example, where a host nation had sophisticated computer crimes laws impacting various contemplated information operations, with no counterpart under US law, or where US statutes contained a specific statutory exemption or had been authoritatively interpreted not to apply to US military actions. Theoretically, therefore, the host nation would have exclusive jurisdiction to prosecute. However, the US may always contend that any host nation offense without a US counterpart (UCMJ or otherwise), is "service discrediting" under Article 134. But, this is not a basis to knowingly violate the host nation's law.

(3) In practice, such prosecutions are unlikely. US military authorities are unlikely to order certain information operations when they are aware that performance of such activities within the territory of a specific host nation, or that produce harmful effects within its territory, will subject US military personnel to possible host nation criminal prosecution.

(4) Where time and circumstances permit, Commanders contemplating information operations that may conflict with host nation law might choose to consult with host nation officials. Otherwise, Commanders may consider whether such activities should be conducted outside host nation territory, and in a manner that would not make use of or affect host nation communications systems.

VIII IMPLICATIONS OF ESPIONAGE LAW

A. Espionage under International Law.

1. Espionage may be defined as covert collection of intelligence about other nations.

2. Espionage is much narrower than "intelligence," much of which is collected via open source information, voluntary exchanges of information among nations, and technical means such as satellite imagery and signals intelligence that are generally accepted as legal by the international community.

3. Covert methods of collecting intelligence are in most cases designed to go undetected by their target, and if detected are designed to be unattributable to the sponsoring state. Nevertheless, discovery, attribution, and public disclosure occur fairly frequently.

B. Espionage during Armed Conflict.

1. The 1907 Hague Convention IV explicitly recognizes the lawfulness of intelligence collection activities.[49]

2. A "spy" is defined in the LOW as any person who, when acting clandestinely or under false pretenses, obtains or endeavors to obtain information in the area controlled by the belligerent, with the intention of communicating it to a hostile party.[50]

   (a) A spy may be a military member or a civilian, and his citizenship is irrelevant.

   (b) Military personnel captured while wearing their uniforms are not considered spies, even if they are collecting intelligence behind enemy lines.

   (c) Under the LOW, only persons captured while relying on protected civilian status or while wearing an enemy uniform are considered spies.

2. Information operations during an armed conflict will not raise any issue of spying under the LOW unless they involve the presence of individuals inside enemy-controlled territory who:

   (a) Are engaged in collecting information with the intent of communicating it to a hostile party, and

   (b) Are wearing civilian clothing or enemy uniforms.

---

[49] *See* Hague Convention IV respecting the Laws and Customs of War on Land, Oct. 18, 1907, Annex (Regulations), arts. 24, 29-31, 36 Stat. 2295, 1 Bevans 643, *reprinted in* DOCUMENTS ON THE LAWS OF WAR (Adam Roberts & Richard Guelff eds., 2d ed. 1989) at 48, 53-54.
[50] *See id*.

3. It seems unlikely that the notions of "electronic presence" or "virtual presence" will find their way into the LOW concept of spying because:

   (a) Individuals conducting intelligence collection through electronic means are generally not physically located in enemy controlled territory; and

   (b) No issue exists of acting under false pretenses by abusing protected civilian status or by wearing the enemy's uniform.

4. If captured in enemy territory, a spy may be punished under the domestic law of the captor.

C. Espionage in Peacetime.

1. The international legal system generally imposes no sanctions upon nations for acts of espionage, except for the political costs of public denunciation.

   (a) There have been many domestic criminal trials of peacetime spies in many countries, including the US.

   (b) However, there has been almost no activity concerning peacetime espionage within the international legal system except for public complaints and the expulsion of implicated diplomats.

2. Individuals (other than those with diplomatic status) caught spying, however, may be tried for whatever crimes their conduct may constitute under the victim nation's domestic law.

   (a) Such persons might be charged with espionage, unlawful entry into the nation's territory, or with a common crime such as burglary, murder, theft, bribery, obtaining unauthorized access to state secrets, or unauthorized computer intrusions.

   (b) A widespread practice exists of assigning intelligence operatives to embassy staff positions in which they enjoy diplomatic immunity from prosecution. The only remedy for an offended host nation is to declare such persons *personna non gratta*, which obligates the sending nation to remove them from the country.

3. How the world community will react to information operations activities is likely to depend on the practical consequences of the activity. Such activities may be regarded much as is espionage—not a major issue unless significant consequences can be demonstrated.

4. An information operator who may later come into the custody of a victim nation in which he engaged in information operations, might be subject to prosecution of that nation's criminal laws.

   (a) As a practical matter, however, the problems of detection and attribution of information operations at the national level are daunting; the likelihood of being able to prove in court that an individual engaged in certain information operations activity seems unlikely.

   (b) There exists within the US a division of labor between the intelligence community and the uniformed military forces concerning the conduct of "covert Action." The intelligence community generally conducts covert actions in peacetime that do not consist of traditional military activities.

D. Assessment.

1. Information operations activities are unlikely to fall within definition of spying in wartime, although a limited category of activities related to information operations may so qualify.

2. Information operations activities are more likely to fall within the category of peacetime espionage.

3. The reaction of the world community to information operations that do not generate widespread dramatic consequences is likely to be very similar to its reaction to espionage.

IX OBSERVATIONS

There seems to be little likelihood that the international legal system will soon generate a coherent body of "information operations" law.

The most useful approach to the international legal issues raised by information operations activities will continue to be to break out the separate elements and circumstances of particular planned activities and then make an informed judgment as to how existing international legal principles are likely to apply them.

In some areas, such as the law of war, existing legal principles can be applied with considerable confidence.

In other areas, such as the application of use of force principles to adopting an "active defense," it is much less clear where the international community will come out. The result will probably depend much more on the perceived equities of the situations in which the issues first arise in practice.

The growth of international law in these areas will be greatly influenced by what decision-makers say and do at those critical moments.

There are no "show stoppers" in international law for information operations as now contemplated by DOD. There are, however, many areas where legal uncertainties create significant risks, most of which can be considerably reduced by prudent planning.

Since so many of these potential issues are relatively novel, and since the actions taken and public positions announced by nations will strongly influence the development of international law in this area, the involvement of high-level policy officials in planning and executing information operations is much more important at present than is the case with more traditional military activities.

The Framework of peacetime International law

Relevant Multilateral Treaties

1. The International Telecommunications Convention of 1982 (Nairobi Convention).[51] This treaty establishes the International Telecommunications Union, which seek to enhance international interoperability and prevent states from interference with the electromagnetic spectrum. The International Frequency Regulation Board is a regulatory body that allocates the electromagnetic spectrum to prevent interference, but has no enforcement powers over violators.[52] Though some IO activities may violate treaty provisions, violations are more likely to be viewed as contractual violations rather than acts of war.

Art 2 of the Convention defines Harmful Interference as that which "endangers the functioning of a radio navigation service or of other safety services or seriously degrades, obstructs or repeatedly interrupts a radio communication service operating in accordance with the Radio Regulations."

a. Art. 19 allows states to "stop the transmission of any private telegram which may appear dangerous to the security of the state or contrary to their laws" and to "cut off any other private telecommunications which may appear dangerous to the security of the state or contrary to its laws, to public order or to decency."[53]

b. Art. 35, ¶ 158, requires that states and broadcasters must establish and maintain stations "in such a manner as not to cause **harmful interference** to the radio services or communications of other Members or of recognized private operating agencies, or of other duly authorized operating agencies which carry on radio service."

c. Art. 38, ¶ 164, states that even military installations must observe the measures taken to prevent unlawful interference, "so far as possible."

[51] Senate Treaty 99-6, 99th Cong., 1st Sess. (1982)(entered into force for the US on 10 Jan. 1986)(*hereinafter* ITC).
[52] Sara Anne Hook, *Comment, Allocation of the Radio Spectrum: Is the Sky the Limit*?, 3 IND. INT'L & COMP. L. REV. 319, 325 (1993).
[53] ITC, *supra* note 8, Art. 19, ¶¶ 132-3.

2. The United Nations Convention on the Law of the Sea.[54]

a. Art. 17 allows ships of all States "the right of innocent passage through the territorial sea." This language mirrored the earlier provisions of Art. 14(2) of the Convention on the Territorial Sea and the Contiguous Zone.[55] Passage is innocent so long as it is not prejudicial to the peace, good order, or security of the coastal nation.

b. Art 19 lays out an "exhaustive list of activities that would render passage not innocent."[56] The listed restrictions include several with potential impact on IO activities:

(1) Any threat or use of force against the sovereignty, territorial integrity, or political independence of the coastal nation.

(2) Any exercise or practice with weapons of any kind.

(3) Intelligence collection activities detrimental to the security of that coastal nation.

(4) Any act aimed at interfering with any system of communication of the coastal nation.

(5) Any act of propaganda aimed at affecting the defense or security of the coastal nation.

(6) Any other activity not having a direct bearing on passage.

[54] U.N. Doc. A/CONF.62/122, 21 I.L.M. 1261 (10 Dec. 1982).
[55] 15 U.S.T. 1606, T.I.A.S. 5639, 516 U.N.T.S. 205 (29 Apr. 1958).
[56] CENTER FOR OCEANS LAW AND POLICY, ANNOTATED SUPPLEMENT TO THE COMMANDER'S HANDBOOK ON THE LAW OF NAVAL OPERATIONS ¶ 2.3.2.1 n.27 (15 Nov. 1997).

c. Art. 109 provides that all States shall cooperate in the "suppression of unauthorized broadcasting from the high seas" and defines such broadcasting as transmissions which would violate the Nairobi Convention.

3. Space Law. Orbital surveillance is legal and common.[57] Space is used for military communications, command and control, navigation, and weapons guidance. Many IO activities would clearly be permissible within the parameters of the "peaceful use" required by the relevant treaties.

a. Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, Including the Moon and Other Celestial Bodies.[58]

(1) This Treaty mandates that all nations are free to explore and use Outer Space on a basis of equality.

(2) No state may place into earth orbit any objects carrying nuclear weapons or any other kind of "weapon of mass destruction."[59]

(3) Requires states to conduct activities in Outer Space in accordance with international law, to include the United Nations Charter. **NOTE**: This allows a wide range of IO activities which are characterized as either under the authority of the Security Council or are taken pursuant to the rights of individual or collective self defense contained in the Charter.

[57] Glenn H. Reynolds, *International Space Law: Into the Twenty-First Century*, 25 VAND. J. TRANSNAT'L L. 225, 230 (1992).
[58] 18 U.S.T. 2410, T.I.A.S. No. 6347, 610 U.N.T.S. 205 (27 Jan. 1967).
[59] *Id.* art 3(3).

b. The 1971 Agreement Relating to the International Telecommunications Satellite Organization (INTELSAT)[60] and The 1976 Convention on the International Maritime Satellite Organization (INMARSAT)[61] require that space be used for "other than for military purposes" and "peaceful purposes" respectively. State practice has established that these conventions are relevant to IO only because they establish the principle of nondiscrimination among states that use satellites.[62]

IO versus The Proscriptive Threshold of the UN Charter

4. Preamble (emphasis added)➔

We the peoples of the United Nations, determined to
save succeeding generations from the scourge of war …
and for these ends
to *unite our strength to maintain international peace and security*,
and to ensure,
by the *acceptance of these principles* and the *institution of methods, that armed force shall not be used*, save in the common interest …

5. Article 1 of the Charter describes the purpose of the United Nations.

"To maintain international peace and security, and to that end: to take effective collective measures for the prevention and removal of threats to the peace, and for the suppression of acts of aggression or other breaches of the peace, and to bring about by peaceful means, and in conformity with the principles of justice and international law, adjustment or settlement of international disputes or situations which might lead to a breach of the peace."

Prohibitions on the Use of Force.[63]

---

[60] 23 U.S.T. 3813, T.I.A.S. No. 7532 (20 Aug. 1971), *reprinted in* 10 I.L.M. 909 (1971).
[61] 31 U.S.T. 1, T.I.A.S. No. 9605, 1143 U.N.T.S. 105 (3 Sept. 1976).
[62] LAWRENCE T. GREENBERG ET AL, INFORMATION WARFARE AND INTERNATIONAL LAW 22 (1998).
[63] *See also* G.A. Res. 2625, U.N. GAOR, 25th Sess. (1970); G.A. Res. 3314, U.N. GAOR, 29th Sess. (1974)(defining aggression as "the use of armed force by a state against the sovereignty, territorial integrity, or political independence of any state, or in any other manner inconsistent with the purposes of the United Nations).

6. Article 2(3): "All Members shall settle their international disputes by peaceful means in such a manner that international peace and security, and justice, are not endangered."

7. Article 2(4): "All Members shall refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any state, or in any other manner inconsistent with the Purposes of the United Nations."

8. Article 2(7): "Nothing contained in the present Charter shall authorize the United Nations to intervene in matters which are essentially within the domestic jurisdiction of any state[64] or shall require the Members to submit such matters to settlement under the present Charter; but this principle shall not prejudice the application of enforcement measures under Chapter VII."

The Security Council shall determine the existence of any threat to the peace, breach of the peace, or act of aggression and shall make recommendations, or decide what measures shall be taken in accordance with Articles 41 and 42, to maintain or restore international peace and security. Art.

Chapter VII Enforcement Authority of the Security Council

9. **Article 41** has particular relevance to the practice of IO: "The Security Council may decide what measures not involving the use of armed force are to be employed to give effect to its decisions, and it may call upon the Members of the United Nations to apply such measures. These may include **complete or partial interruption** of economic relations and of rail, sea, air, postal, **telegraphic, radio, and other means of communication**, and the severance of diplomatic relations." (emphasis added)

[64] *See generally Declaration on the Inadmissibility of Intervention into the Domestic Affairs of States*, G.A. Res. 2131, U.N. GAOR, 20th Sess., Supp. No. 14, at 108, U.N. Doc. A/6014 (1965)(states may not "intervene, directly or indirectly, for any reason whatsoever, in the internal or external affairs of any other State. Consequently, armed intervention and all other forms of interference or attempted threats against the personality of the State or against its political, economic, and cultural elements, are condemned.")

10. **Article 42 is the Meat of Chapter VII**: "Should the Security Council consider that measures provided for in Article 41 would be inadequate or have proved to be inadequate, it may take such action by air, sea, or land forces as may be necessary to maintain or restore international peace and security. Such action may include demonstrations, blockade, and other operations by air, sea, or land forces of Members of the United Nations."

VIII. INFORMATION OPERATIONS AND THE LAW OF WAR

Expansion of the Kinetic View of Warfare. Protocol I, Art. 49(1) defines "attacks" as "acts of violence against the adversary, whether in offence or defence."

1. Difficulty of Discrimination in offensive IO: Prot. I, Art. 48 mandates that Parties to the conflict distinguish between the civilian population and combatants at all times and between civilian objects and military objectives and direct operations only against military objectives.

2. **THE PROBLEM OF UNANTICIPATED CONSEQUENCES**:[65]

   a. Prot I, Art. 51(2) "The civilian population as such, as well as individual civilians, shall not be the object of attack. Acts or threats of violence the primary purpose of which is to spread terror among the civilian population are prohibited."

   b. Hague IV, Art. 22 "The right of belligerents to adopt means of injuring the enemy is not unlimited."

   c. Prot I, Art. 57(2)(a)(ii), those who plan or decide upon attack shall "take all feasible precautions in the choice of means and methods of attack with a view to avoiding, and in any event, to minimizing, incidental loss of civilian life, injury to civilians, and damage to civilian objects."

The Law of Neutrality[66]

[65] *See, e.g.*, Prot. I, Annex I, arts. 7-13.

3. As a general rule, all acts of hostility in neutral territory, including neutral lands, waters, and airspace are prohibited. In theory, using the wires or digital cables of a network associated with a neutral Party as a conduit for information operations would jeopardize that State's neutrality. If the neutral nation is unable or unwilling to affirmatively maintain its neutrality, the belligerents are allowed to take such measures as are necessary to negate the enemy efforts.[67]

4. Specific IO Related Prohibitions with Regard to Neutral States.

   a. Hague V, Art. 3 forbids a belligerent from erecting a "wireless telegraphy station or other apparatus for the purpose of communicating" on the territory of the neutral, and forbids belligerents from using "any installation of this kind established by them before the war … for purely military purposes." (emphasis added)

   b. Likewise, Art. 5 mandates that the neutral state prevent any belligerent from allowing belligerents to establish communications equipment on its territory, in its airspace, or in its waters.

5. Lawful Activities with IO Implications. Hague V, Art. 8 mandates that a neutral power is not required to "forbid or restrict the use on behalf of the belligerents of telegraph or telephone cables or of wireless telegraphy apparatus belonging to it or to companies or private individuals"

Perfidy versus Lawful Deception

---

[66] *See* Hague Convention No. V Respecting the Rights and Duties of Neutral Powers and Persons in Case of War on Land, Oct. 18, 1907, 36 Stat. 2310, UST 540.

[67] CENTER FOR OCEANS LAW AND POLICY, ANNOTATED SUPPLEMENT TO THE COMMANDER'S HANDBOOK ON THE LAW OF NAVAL OPERATIONS ¶ 7.3 (15 Nov. 1997).

6. Prot. I, Art. 37 prohibits belligerents from killing, injuring, or capturing and adversary by perfidy. The essence of this offense lies in acts designed to gain advantage by falsely convincing the adversary that applicable rules of international law prevent engaging the target when in fact they do not.

7. Examples of Perfidy:

   a. The feigning of an intent to negotiate under a flag of truce or surrender.

   b. The feigning of an incapacitation by wounds or sickness.

   c. The feigning of noncombatant status.

   d. The feigning of protected status by the use of signs, or either UN or neutral parties.

8. IO applications:

   a. The use of enemy codes and signals is a time-honored means of tactical deception. However, misuse of distress signals or of signals exclusively reserved for the use of medical aircraft would be perfidious.[68]

   b. The use of deception measures to thwart precision guided munitions would be allowed, while falsely convincing the enemy not to attack a military target by electronic evidence that it was a hospital would be perfidious.

Nothing in the present Charter shall impair the inherent right of individual or collective self-defense if an armed attack occurs against a Member of the United Nations, until the Security Council has taken measures necessary to maintain international peace and security. Measures taken by Members in the exercise of this right of self-defense shall be immediately reported to the Security Council and shall not in any way affect the authority and responsibility of the Security Council under

[68] Prot. I, Art. 38(1).

the present Charter to take at any time such action as it deems necessary in order to maintain or restore international peace and security.

IX. STATUTORY TOOLS FOR DEFENSIVE INFORMATION OPERATIONS

Telecommunications Statutes

1. Electronic Communications Privacy Act of 1986.[69] Enacted 18 U.S.C. §§ 2701-11, §§ 3121-27, § 1367, § 3117, § 2521, and made numerous amendments to provisions of the Communications Act of 1934.

   a. § 107 of the Act specifically limits its statutory application to law enforcement functions. "Nothing contained … constitutes authority for the conduct of any intelligence activity."

   b. Unlawful for "any person" to "intentionally intercept, use, or disclose or endeavor to intercept, use, or disclose any wire, oral, or electronic communication." 18 U.S.C. § 2511
   NOTE: Must distinguish between real-time interception which is governed by 18 U.S.C. § 2511 and stored communications such as E-Mail that is governed by 18 U.S.C. § 2703.

   c. 9 Statutory Exceptions (of which three are central to IO):

      (1) System Administrator "while engaged in any activity which is necessary incident to the rendition of his service or to the protection of the rights or property of the provider of that service." 18 U.S.C. § 2511(2)(a)(i)

      (2) Not unlawful "where such person is a party to the communication or one of the parties has given consent to such interception." 18 U.S.C. § 2511(2)(c)

[69] Pub. L. No. 99-508, 100 Stat. 1848 (1986).

(3) Not unlawful pursuant to a court order directing such assistance signed by the authorizing judge or a certification in writing by a person designated in 18 U.S.C. § 2518(7) or the Attorney General that no court order is required by law and that all statutory requirements have been met. 18 U.S.C. § 2511(2)(a)(ii)

2. 18 U.S.C. § 2709 Counterintelligence access to telephone toll and transactional records.

a. The Director of the FBI or his designee in a position not lower than Deputy Assistant Director has authority to require a wire or electronic communication service provider to produce subscriber information and toll billing records information or electronic communication transactional records.

b. The FBI must certify that the information sought is relevant to an authorized foreign counterintelligence investigation and there are specific and articulable grounds to believe that the person or entity to whom the information pertains is a foreign power or an agent of a foreign power as defined in the Foreign Intelligence Surveillance Act, 50 U.S.C. § 1801.

3. Computer Crimes[70]

a. 18 U.S.C. § 1029 prohibits a wide range of offenses dealing with knowingly and with intent to defraud using counterfeit access devices (a)(1); trafficking in or using one or more unauthorized access devices during a one year period (which can include unauthorized use of passwords)(a)(2); possessing 15 or more unauthorized or counterfeit access devices (a)(3); or a variety of other offenses dealing with the unlawful procurement of telecommunications services.

(1) Offenses are punishable by either 10 or 15 years confinement with fines.

[70] *See generally* Scott Charney and Kent Alexander *Computer Crime*, 45 EMORY L.J. 931 (1996).

(2) The term "access device" means any card, plate, account number, electronic serial number, personal identification number, or other means of account access that can be used to obtain money, goods, services, or initiate a transfer of funds. (e)(1)

(3) The term "unauthorized access device" means any access device that is lost, stolen, expired, revoked, canceled, or obtained with intent to defraud.

(4) 1998 amendments to the act broadened its coverage to include all telecommunications service as defined in section 3 of title I of the Communications Act of 1934[71] (*codified at* 47 U.S.C. § 153).

b. Computer Fraud and Abuse Act, (*codified as amended at* 18 U.S.C. § 1030). Eleven specified crimes, 6 felony offenses, 5 misdemeanor offenses.

(1) Computer Espionage (a)(1): knowing access or exceeding authorized access obtaining information and willfully communicating, delivering, transmitting to any person not authorized to receive it with reason to believe that the information could be used to the injury of the United States.

(2) Financial Records (a)(2): intentional access without authorization or exceeding authorized access to information from any departement of the US, computer records of financial institutions, or information from a protected computer involved in interstate commerce.

(3) Government Computers (a)(3): intentional access to any nonpublic computer exclusively for the use of the United States or affecting the United States use of the system.

(4) Intent to Defraud (a)(4): knowingly and with intent to defraud accessing a protected computer.

[71] 48 Stat. 1064 , *codified as amended* 47 U.S.C. 151 – 614.

(5) Unlawful Computer Trespassers (a)(5): knowingly causes the transmission of a program, information code, or command and as a result of such conduct, intentionally causes damage to a protected computer.

(6) Password Trafficking (a)(6): knowingly and with intent to defraud traffics (as defined in 18 U.S.C. § 1029) in any password or similar information in any government computer, or in a computer which affects interstate commerce.

(7) Extortion (a)(7): knowingly and with intent to defraud transmits any communication containing a threat to cause damage to a protected computer.

Information Offenses

4. Gathering, Transmitting, or Losing Defense Information, 18 U.S.C. § 793. The information need not be classified to constitute a violation of this statute if the information is not generally accessible to the public.[72] The accused must have had an intent or reason to believe that the information "is to be used" to the injury of the United States.

5. Gathering or Delivering Defense Information to Aid Foreign Government. 18 U.S.C. 794

6. 18 U.S.C. § 798 Disclosure of Classified Information which is "for reasons of national security, specifically designated by a United States Government Agency for limited or restricted dissemination or distribution."[73]

7. The Economic Espionage Act of 1996.

[72] United States v Allen, 31 M.J. 572 (N.M.C.M.R. 1990), *aff'd*, 33 M.J. 309 (C.M.A. 1991), *cert. denied*, 503 U.S. 936 (1992).
[73] *See also* 50 U.S.C. § 783, Communication of Classified Information by Government Officer or Employee.

a. 18 U.S.C. § 1831 prohibits knowing theft, appropriation, duplication, communication, receipt, purchase, or possession of a trade secret intending or knowing that it will benefit any foreign government, instrumentality, or agent.

b. 18 U.S.C. § 1832 prohibits theft of trade secrets without requiring the intent to benefit a foreign government, instrumentality, or agent.

8. Intelligence Identities Protection Act of 1982 (*codified at* 50 U.S.C. §421-26).

a. Whoever, having or having had authorized access to classified information that identifies a covert agent, intentionally discloses any information identifying such covert agent to any individual not authorized to receive classified information, knowing that the information disclosed so identifies such covert agent and that the United States is taking affirmative measures to conceal such covert agent's intelligence relationship to the United States, shall be fined not more than $ 50,000 or imprisoned not more than ten years, or both.

b. Whoever, in the course of a pattern of activities intended to identify and expose covert agents and with reason to believe that such activities would impair or impede the foreign intelligence activities of the United States, discloses any information that identifies an individual as a covert agent to any individual not authorized to receive classified information, knowing that the information disclosed so identifies such individual and that the United States is taking affirmative measures to conceal such individual's classified intelligence relationship to the United States, shall be fined not more than $ 15,000 or imprisoned not more than three years, or both.

Information Operations Warrants for Law Enforcement Purposes.

9. Searching Records and Databases

a. 18 U.S.C. § 2703(c): with subpoena the government can obtain the name, address, local and long distance telephone billing records, telephone number or other subscriber information. The government entity receiving such information is not required to provide notice to the consumer.

b. 18 U.S.C. § 2703(d) allows a court to issue an order for disclosure if the government offers specific and articulable facts that there are reasonable grounds to believe that the contents of electronic communication or the records within the service provider's database or other information sought are relevant and material to an ongoing criminal investigation.

(1) The service provider may move to quash or modify the order if the request is unusually voluminous or would cause an undue burden on the carrier.

(2) § 270 is the mechanism for obtaining subscriber connection logs, sending IP addresses, receiving IP addresses, times of access and log on, content of saved communications, and more.

10. Interception of Wire, Oral, and Electronic Communications.

a. Within DoD, the relevant guidance is contained in DoD.D 5505.9 Interception of Wire, Electronic, and Oral Communications for Law Enforcement Purposes, (20 Apr. 1995)[74] and DoD 0-5505.9-M Procedures for Wire, Electronic, and Oral Interceptions for Law Enforcement Purposes (May 1995).
NOTE THE IMPACT OF THE COMMUNICATIONS ASSISTANCE FOR LAW ENFORCEMENT ACT: The procedures for authorizing a court order for electronic surveillance fit hand in glove with the legal obligation for telecommunications carriers to maintain a technical capability for "expeditiously isolating and enabling" the government to obtain the information sought by court order.[75]

[74] <http://web7.whs.osd.mil/pdf/d55059p.pdf>
[75] Pub. L. No. 103-414, 108 Stat. 4279, *codified at* 47 U.S.C. 1001-21.

b. 18 U.S.C. § 2518 implements a higher standard than normal Fourth Amendment analysis. The DoD guidance implements the Title III standards.

c. The Process to Obtain an Intercept:

(1) The Officer prepares a detailed affidavit showing probable cause that the target is used to facilitate specific, serious, indictable crime. 18 U.S.C. § 2516 prescribes the list of offenses for which intercept authority can be sought.

(2) The US Attorney prepares an application for a Court Order based on the affidavit. The application must contain a full explanation of the information required by statute. *See* 18 U.S.C. § 2518(1).

(3) The Attorney General, Deputy Attorney General, or other designated individual must approve the application.

(4) The judge authorized to issue a court order for electronic surveillance will conduct an *ex parte* proceeding, and issue an order detailing the information required by statute. 18 U.S.C. 2518(4).

The Foreign Intelligence Surveillance Act of 1978[76] (FISA)

11. FISA revolves around the core definition of **FOREIGN INTELLIGENCE INFORMATION**; Information that relates to the ability of the US to protect against the following: Attack or hostile act of a foreign power or agent, Sabotage or international terrorism, Clandestine intelligence activities by an intelligence network or service of a foreign power or by an agent, or Information on foreign power or foreign territory relative and necessary to the national defense and security of the U.S. or the foreign affairs of the U.S.

[76] Pub. L. No. 95-511, 92 Stat. 1783 (1978), *codified as amended* 50 U.S.C. §§ 1801-29. *See also* 18 U.S.C. § 2232 regarding prohibitions on warning an individual of surveillance authorized under the Foreign Intelligence Surveillance Act.

12. FISA is the statutory mechanism for obtaining two major categories of information related to defensive IO:

    a. Acquisition of a "nonpublic communication" by electronic means[77] without the consent of a person who is a party to an electronic communication or, in the case of a nonelectronic communication, without the consent of a person who is visibly present at the place of the communication.

    b. Physical searches seeking to obtain foreign intelligence information.

13. 50 U.S.C. § 1804 outlines the requirements for the order sought from the FISA court.

    a. The identity of the federal officer making the application.[78]

    b. A statement showing that the President has delegated authority to the Attorney General to approve such applications.

    c. The application must have been approved by the Attorney General.

    d. The identity or description of the target must be given.

    e. Facts and circumstances relied on by the applicant supporting the belief that the target is a foreign power or the agent of a foreign power and each of the facilities or places at which the warrant is directed is being used or will be used by the foreign power or the agent of a foreign power.

[77] Such means include wiretaps of phones, teleprinter, facsimile, computers, computer modems, radio intercepts, microwave eavesdropping,

[78] *See* Exec. Order 12,139, 44 Fed. Reg. 30,311 (1979), *reprinted in* 50 U.S.C. § 1803 nt, for a list of federal officals authorized to apply for warrants under FISA.

f. An application must state the minimization procedures to be used.

g. A detailed description of the nature of the information sought and the communications to be monitored also must be included.

h. The Assistant to the President for National Security, or his designee, must certify that the information is foreign intelligence information, and is obtainable by no other means or investigative techniques.

i. Finally, the application:

(1) Must state the past history of applications on the target.

(2) Whether physical entry is necessary to accomplish the electronic surveillance.

(3) The types of devices to be used, the way they will be installed.

(4) The time for which the surveillance is to be monitored. Up to ninety days. (For an official foreign power, it can be for a year). *See* § 1805(d)(1).

X. COMSEC MONITORING.

This is a clearly defined, bright line exception to the general limitations on content monitoring. § 107(b)(1) of the Electronic Communications Privacy Act specifically allows activities intended to "intercept encrypted or other official communications of United States executive branch entities or United States Government contractors for communications security purposes."

1. NSA is the proponent under National Telecommunications and Information Systems Security Directive (NTISS) Directive No. 600, Communications Security Monitoring.

2. COMSEC is one of the tools available to fulfill the DoD mandate to accredit automated information systems and ensure "compliance with automated information systems security requirements."[79]

Implemented within the Army by the newly revised AR 380-53.[80] Information Systems Security Monitoring will be conducted only in support of security objectives. Information Systems Security Monitoring will not be performed to support law enforcement or criminal or counterintelligence investigations. The results of Information Systems Security Monitoring shall not be used to produce foreign intelligence or counterintelligence, as defined in Executive Order 12333.

3. Assigns Functional Responsibility for Specific Parts of the COMSEC Program.

a. Assigns the Judge Advocate General responsibility for coordinating issues with the Office of the General Counsel, ensuring compliance with public laws and applicable regulations, and reviewing all requests to conduct Information Systems Security Monitoring exercises based upon a MACOM request to the DCSINT.

b. CG, U.S. Army Intelligence and Security Command provides the Army support to the Joint COMSEC Monitoring Activity, through the Director, Land Information Warfare Activity (LIWA), develops and disseminates techniques for conducting security penetration and testing.

c. CG, U.S. Army Training and Doctrine Command develops and fields an exportable training package to address the requirements of para. 3-3. The regulation requires that persons conducting Information Systems Monitoring receive formal training in the procedures outlined in AR 380-53, the provisions of AR 381-10, the provisions of AR 381-12, para. 3-1, the provisions of AR 190-53, and the provisions of applicable Federal laws (18 U.S.C. §§ 2510, etc.)

---

[79] U.S. DEP'T OF DEFENSE, DIR. 5200.28, SECURITY REQUIREMENTS FOR AUTOMATED INFORMATION SYSTEMS (21 Mar. 1998).

[80] U.S. DEP'T OF ARMY, FIELD MANUAL 380-53, INFORMATION SYSTEMS SECURITY MONITORING (29 Apr. 1998). <http://www.acert.belvoir.army.mil/ar380_53.pdf>

d. MACOM Commanders will implement procedures to ensure all personnel to include contractors are aware of the provisions of AR 380-53. MACOM commanders will submit certification to the DCSINT on an annual basis of the notification procedures followed within the command.

4. Prerequisites for Information Systems Monitoring.

a. **NOTIFICATION**: Users of official DOD telecommunications will be given notice that-(1) Passing classified information over nonsecure DOD telecommunications systems, other than protected distribution systems or automated information systems accredited for classified processing,is prohibited.(2) Official DOD telecommunications systems are subject to Information Systems Security Monitoring at all times.(3) Use of official DOD telecommunications systems constitutes consent by the user to Information Systems Security Monitoring at any time.

b. **CERTIFICATION:** The Office of the General Counsel has certified the adequacy of the notification procedures in effect, and the OGC and TJAG have given favorable legal review of any proposed Information Systems Security Monitoring that is not based on a MACOM request. *See* para. 2-4 for a specific list of information required prior to certification.

c. **AUTHORIZATION:** The Deputy Chief of Staff for Intelligence has authorized Information Systems Security Monitoring to be conducted within the MACOM involved.

5. Notification Guidance for Automated Information Systems

a. Mandatory forms of notification.

(1) Telephone or communications directory notice.

(2) DD Form 2056. (a) The DD Form 2056 will be applied to the front of all tele-phones(except tactical telephones) within the U.S. Army.(b) The DD Form 2056 will also be applied to the front of all Secure Telephone Units (STUs); however the banner at the top ofthe form containing the words DO NOT DISCUSS CLASSIFIED INFORMATION will be removed or obliterated.(c) The DD Form 2056 will be applied to the front of all datafacsimile devices except those that are an internal part of another device (for example, a facsimile card in a personal computer). The DD Form 2056 will also be applied to the front of all secure datafacsimile devices, but the words DO NOT DISCUSS CLASSIFIEDINFORMATION will be removed.

(3) Computers log-on banner notice. All computers attached or accessible through Government-owned or -leased telecommunications networks must display the banner below. The banner will be placed on the computer in such a way that the user must press a key to get beyond it, thereby demonstrating his or her acceptance of its provisions.(a) The warning banner is not required on computers that are an integral portion of a tactical weapons system, electronic personnel access control system, or intrusion detection system and stand-alone computers not connected to a telecommunications network.(b) Security warning banners for publicly accessible, nonrestricted U.S. Army World Wide Web sites will be in accordance with the current provisions of HQDA, DISC4, Web-site management policy.

ATTENTION! THIS IS A DOD COMPUTER SYSTEM. BEFORE PROCESSING CLASSIFIED INFORMATION , CHECK THE SECURITY ACCREDITATION LEVEL OF THIS SYSTEM. DO NOT PROCESS, STORE, OR TRANSMIT INFORMATION CLASSIFIED ABOVE THE ACCREDITATION LEVEL OF THIS SYSTEM. THIS COMPUTERSYSTEM, INCLUDING ALL RELATED EQUIPMENT, NETWORKS AND NETWORK DEVICES (INCLUDES INTERNET ACCESS) ARE PROVIDED ONLY FOR AUTHORIZED U.S. GOVERNMENT USE. DOD COMPUTER SYSTEMS MAYBE MONITORED FOR ALL LAWFUL PURPOSES, INCLUDINGTO ENSURE THAT THEIR USE IS AUTHORIZED, FOR MANAGEMENTOF THE SYSTEM, TO FACILITATE PROTECTION AGAINST UNAUTHORIZED ACCESS, AND TO VERIFY SECURITY PROCEDURES, SURVIVABILITY, AND OPERATIONAL SECURITY. MONITORING INCLUDES, BUT IS NOT LIMITED TO, ACTIVE ATTACKS BY

AUTHORIZED DOD ENTITIES TO TEST OR VERIFY THE SECURITY OF THIS SYSTE M. DURING MONITORING, INFORMATION MAY BE EXAMINED, RECORDED, COPIED, AND USED FOR AUTHORIZED PURPOSES. ALL INFORMATION, INCLUDING PERSONAL INFORMATION, PLACED ON OR SENT OVER THIS SYSTEM MAY BE MONITORED. USE OF THIS DOD COMPUTER SYSTEM, AUTHORIZED OR UNAUTHORIZED, CONSTITUTES CONSENT TO MONITORIN G. UNAUTHORIZED USE OF THIS DOD COMPUTER SYSTEM MAY SUBJECT YOU TO CRIMINAL PROSECUTION. EVIDENCE OF UNAUTHORIZED USE COLLECTED DURING MONITORING MAY BE USED FOR ADMINISTRATIVE, CRIMINAL, OR OTHER ADVERSE ACTION. USE OF THIS SYSTEM CONSTITUTES CONSENT TO MONITORING FOR ALL LAWFUL PURPOSES.

(4) Periodic notices. Periodic notices will be published at least quarterly in command bulletins.

(5) Initial briefing. Initial briefings to all new personnel will include informing personnel that their use of telecommunications systems constitutes consent to Information Systems Security Monitoring.

b. Optional forms of notification.

(1) Periodic briefings and training classes for all assignedersonnel.

(2) Special memorandums from the commander or responsible senior staff officer to all personnel.

(3) Local notification and consent procedures.

(4) Statements in standing operating procedures (SOPs), signal operation instructions (SOIs), and similar publications or documents.

(5) The following statement may be placed on facsimile coversheets:

ATTENTION! DO NOT PROCESS, STORE, OR TRANSMIT CLASSIFIED INFORMATION ON UNSECURED TELECOMMUNICATIONS

SYSTEMS. OFFICIAL DOD TELECOMMUNICATIONS SYSTEMS, INCLUDING FACSIMILE MACHINES, ARE SUBJECT TO MONITORING FOR INFORMATION SYSTEMS SECURITY MONITORING AT ALL TIMES. USE OF THIS SYSTEM CONSTITUTES CONSENT TO INFOR M ATION SYSTEMS SECURITY MONITORING.

6. Use of Information Acquired During Information Systems Security Monitoring. See para. 2-8(c)(3) for required procedures if materials are required as evidence.

(1) The results of Information Systems Security Monitoring may not be used in a criminal prosecution without prior consultation with the OGC and TJAG. (para. 2-8(5)).

(2) Information obtained through Information Systems Security Monitoring may be used in connection with disciplinary or administrative action against Department of the Army personnel for knowing, willful, or negligent actions that result in the unauthorized disclosure of classified information (*see* AR 380-5, paras 14-101a n d 14 - 102). In this case, the Information Systems Security Monitoring element is authorized to release names, or recorded media, of the telecommunications involved to the supported commander or designated representative for use as evidence. Procedures will be strictly adhered to as follows:

Note the specific requirement in the regulation for JA coordination. Para. 2-8(a)(1)

(a) **The supported commander, after having consulted with the servicing judge advocate (JA), will provide the Information Systems Security Monitoring element with a written request, specifically identifying the telecommunications messages or communications required. The request will identify the servicing JA consulted**.

(b) The Information Systems Security Monitoring element will obtain a signed receipt from the supported commander or designated representative for the requested materials. The receipt will include a statement that the commander or representative is familiar with and will comply with the security requirements and privacy restrictions applicable to the material.

(c) The Information Systems Security Monitoring element will immediately notify its chain of command that the material has been requested and

(d) The Information Systems Security Monitoring unit commander will notify HQDA (DAMI-CHI), in writing, within 5 working days of providing the material to the supported command.

(3) Information may be obtained incidental to an authorized Information Systems Security Monitoring mission that relates directly to a serious crime such as sabotage or threats or plans to commit offenses that threaten a life or could cause significant damage to or loss of Government property (this includes data on Government AIS). This information will be reported immediately by the senior member of the Information Systems Security Monitoring team present when the information is discovered, as follows:

(a) Crimes or incidents identified in AR 381-12, at chapter 3, or AR 381-20, paragraph 4-2, will be reported under the provisions of AR 381-12.

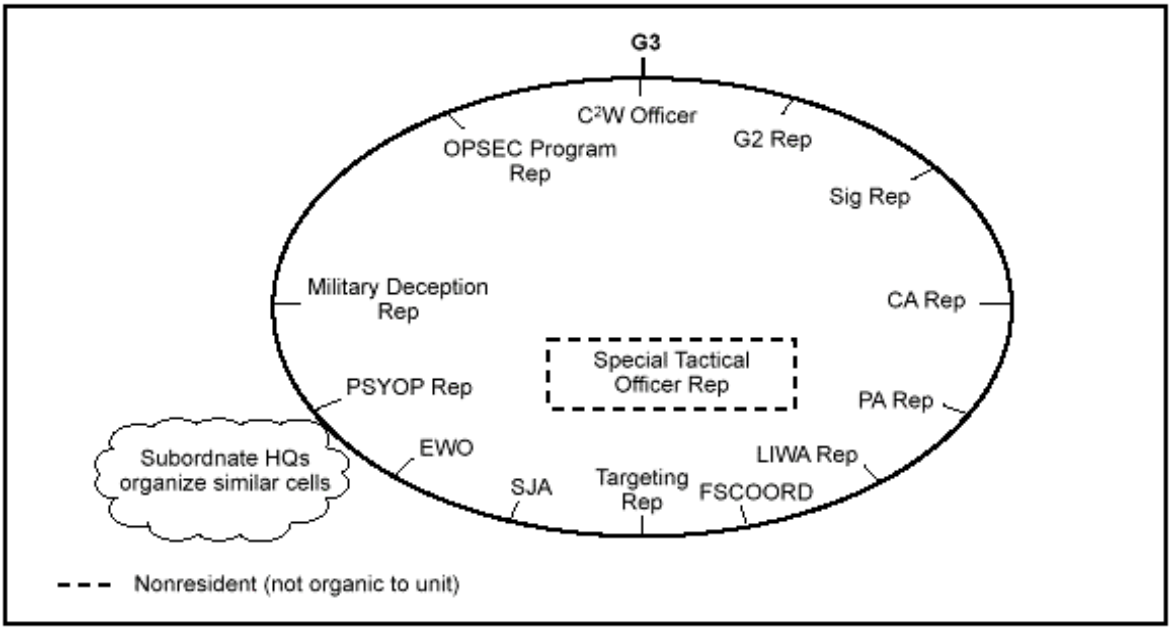
(b) Questionable activity and information relating to violations of Federal law as addressed in procedure 15 of AR 381-10 will be reported under the provisions of AR 381-10.

(c) When evaluating or assessing the security of U.S. Army AIS, Information Systems Security Monitors may detect computer anomalies that could potentially be unauthorized intrusions into Army AIS . When Information Systems Security Monitors detect such anomalies, they must contact the system administrator and ACERT[81] immediately. The system administrator will then follow the procedures of AR 380-19 by taking measures to ascertain that the anomaly is in fact an unauthorized intrusion, notifying counterintelligence (CI) and criminal investigation division (CID) so that the offices may conduct an investigation of the incident.

(d) Information Systems Security Monitors should not support the process of determining if the investigation is properly a law enforcement or intelligence matter, and must discontinue monitoring the suspected intrusion as soon as the system administrator or ACERT has interceded In no case may the Information System Security Monitors continue monitoring the anomaly for more than 24 hours. Data pertaining to the anomaly or suspected intrusion recorded during the 24-hour period will not be accessed until the appropriate legal authorization is obtained to further investigate the activity.

XI. CONCLUSIONS

[81] The Army Computer Emergency Response Team (ACERT) conducts command and control protect operations in support of the Army to ensure the availability, integrity, and confidentiality of the information and information systems used in planning, directing, coordinating, and controlling forces in the accomplishment of the mission across the full spectrum of support to military operations. *See* < http://www.acert.belvoir.army.mil/> Contact at COMM 1-888-203-6332/ DSN 235-1113.


G3
C²W Officer
G2 Rep
OPSEC Program Rep
Sig Rep
Military Deception Rep
CA Rep
Special Tactical Officer Rep
PSYOP Rep
PA Rep
Subordnate HQs organize similar cells
EWO
LIWA Rep
SJA
Targeting Rep
FSCOORD
Nonresident (not organic to unit)