OPERATIONAL LAW HANDBOOK (2006)

Maj Derek I. Grimes
MAJ John Rawcliffe
CPT Jeannine Smith

Editors

Contributing Authors

LTC Eugene Baime
LTC Michael Benjamin
MAJ James Dorn
MAJ Chris Fredrikson
LTC Carissa Gregg
Maj Derek Grimes, USAF
MAJ Lance Hamilton
LCDR Robert Hunt, USN
MAJ Gretchen Jackson
MAJ Chris Jacobs
LCDR Brad Kieserman, USCG
LTC Paul Kantwill
LTC Karl Kuhn
MAJ Russell Miller
LTC J Thomas Parker
Mr. Hays Parks
MAJ Steve Patoir
MAJ John Rawcliffe
LTC Pamela Stahl
MAJ Kurt Takushi
MAJ Frank Vila
Maj Thomas Wagoner
SQNLDR Catherine Wallis, RAAF
MAJ Sean Watts

All of the faculty who have served before us
and contributed to the literature in the field of operational law.

Technical Support

Ms. Terri Thorne, Secretary **Mr. Byrd Eastham, Cover Art**
Ms. Phyllis Bowman, Printing

JA 422
International and Operational Law Department
The Judge Advocate General's Legal Center and School
Charlottesville, Virginia 22903

CHAPTER 18

INFORMATION OPERATIONS

REFERENCES

1. USA PATRIOT Act of 2001, Pub. L. No. 107-56 [*hereinafter* PATRIOT Act].
2. Communication of Classified Information by Government Officer or Employee, 50 U.S.C. § 783.
3. Communications Act of 1934, 48 Stat. 1064 , 47 U.S.C. 151 – 614.
4. Computer Fraud and Abuse Act, 18 U.S.C. §1030.
5. Economic Espionage Act of 1996, 18 U.S.C. §1831-2.
6. Electronic Communications Privacy Act of 1986. Pub. L. No. 99-508, 100 Stat. 1848 (1986).
7. The Foreign Intelligence Surveillance Act of 1978 (FISA) Pub. L. No. 95-511, 92 Stat. 1783 (1978), 50 U.S.C. §§ 1801-29.
8. Intelligence Identities Protection Act of 1982, 50 U.S.C. §421-26.
9. Executive Order 12684.
10. Executive Order 13010.
11. Executive Order 13231.
12. Presidential Decision Directive 62, *Combating Terrorism*, 22 May 1998.
13. Presidential Decision Directive 63, *Critical Infrastructure Protection*, 22 May 1998.
14. Homeland Security Presidential Directive 7, *Critical Infrastructure Identification, Prioritization, and Protection,* 17 December 2003.
15. U.S. DEP'T OF ARMY, ARMY REGULATION 380-53, INFORMATION SYSTEMS SECURITY MONITORING, 29 April 1998.
16. DOD DIR. S-3600.1, INFORMATION OPERATIONS (U), 9 December 1996.
17. DOD DIR 5505.9, Interception of Wire, Electronic, and Oral Communications for Law Enforcement Purposes, 20 April 1995.
18. DOD 0-5505.9-M, Procedures for Wire, Electronic, and Oral Interceptions for Law Enforcement Purposes, May 1995.
19. U.S. DEP'T OF DEFENSE, OFFICE OF GENERAL COUNSEL, *AN ASSESSMENT OF INTERNATIONAL ISSUES IN INFORMATION OPERATIONS,* 2d ed., November 1999.
20. CHAIRMAN, JOINT CHIEFS OF STAFF INSTR. 3210.01A, JOINT INFORMATION OPERATIONS POLICY, 6 November 1998.
21. CHAIRMAN, JOINT CHIEFS OF STAFF INSTR. 6510.01C, INFORMATION ASSURANCE AND COMPUTER NETWORK DEFENSE , May 2001.
22. THE JOINT CHIEFS OF STAFF, JOINT PUB. 3-13, JOINT DOCTRINE FOR INFORMATION OPERATIONS, 9 October 1998.
23. THE JOINT CHIEFS OF STAFF, JOINT PUB. 3-13.1, JOINT DOCTRINE FOR COMMAND AND CONTROL WARFARE (C2W), 7 February 1996.
24. THE JOINT CHIEFS OF STAFF, JOINT PUB. 3-51, JOINT DOCTRINE FOR ELECTRONIC WARFARE, 7 April 2000.
25. THE JOINT CHIEFS OF STAFF, JOINT PUB. 3-53, DOCTRINE FOR JOINT PSYCHOLOGICAL OPERATIONS, 5 September 2003.
26. THE JOINT CHIEFS OF STAFF, JOINT PUB. 3-54, JOINT DOCTRINE FOR OPERATIONS SECURITY, 27 January 1997.
27. U.S. DEP'T OF ARMY, FIELD MANUAL 100-6, INFORMATION OPERATIONS, 27 August 1996.

I. INTRODUCTION

A. "Information Operations involve actions taken to affect adversary information and information systems while defending one's own information and information systems."[1] Information Operations (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. The core IO capabilities are: operations security (OPSEC); psychological operations (PSYOP); military deception (MILDEC); electronic warfare (EW); and Computer Network Operations (CNO). IO-related activities include, but are not limited to, public affairs (PA) and civil affairs (CA) activities.

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 IO policy for Department of Defense (DoD) components, and delineate specific responsibilities.

2. A subset of IO is **Information Warfare** (IW). IW is IO conducted during times of crisis or conflict to achieve or promote specific objectives over a specific adversary or adversaries. 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. IW is any attack against an information system, regardless of the means.

3. IO can be divided into two major categories: Offensive IO and Defensive IO. 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."[2] Defensive IO "integrate and coordinate policies and procedures, operations, personnel, and technology to protect and defend information and information systems."[3]

4. **Offensive IO** applies perception management actions such as PSYOP, OPSEC and MILDEC, and may apply attack options such as EW, physical attack/destruction, and Computer Network Attack (CNA) 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 an 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.[4] Though the vast majority of PSYOP do not raise issues of truthfulness, the 1907 Hague Convention No. IV states that ruses of war are legal so long as they do not amount to treachery or perfidy. PSYOP have played a major role in recent operations, to include Desert Shield/Desert Storm, Bosnia, Kosovo, Operation Enduring Freedom and Operation Iraqi Freedom.

c. **MILDEC** targets adversary decision makers through effects on their intelligence collection, analysis, and dissemination systems. As with PSYOP, there is no prohibition on cover or deception operations, so long as they are not tied to an enemy's reliance on compliance with the law of war. Military deception operations

---

[1] THE JOINT CHIEFS OF STAFF, JOINT PUB 3–13, JOINT DOCTRINE FOR INFORMATION OPERATIONS vii (Oct. 9, 1998), *available at* http://www.dtic.mil/doctrine/jel/new_pubs/jp3_13.pdf (hereinafter JP 3-13).

[2] *Id* at *viii.*

[3] *Id*.

[4] THE JOINT CHIEFS OF STAFF, JOINT PUB 3–53, DOCTRINE FOR JOINT PSYCHOLOGICAL OPERATIONS v (Jul. 10, 1996), *available at* http://www.dtic.mil/doctrine/jel/new_pubs/jp3_53.pdf (hereinafter JP 3-53).

have been used throughout history, including WWII, in order to divert attention from Normandy for the D-Day invasion.

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, which are 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 kinetic weapons against designated targets as an element of an integrated IO effort.

f. **CNO** is the umbrella term for all facets of computer operations, including CNA and Computer Network Defense (CND). **CNA** is defined as operations to disrupt, deny, degrade, or destroy information resident in computers and computer networks or the computers and networks themselves.[5] Specific issues with CNA will be discussed below. The DoD lead for CNO activities is JTF-GNO, which reports to STRATCOM.

5. **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, counter deception, counterpropaganda, counterintelligence (CI), EW, and CNO. 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. 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.[6]

a. **IA** ensures the "availability, integrity, identification and authentication, confidentiality, and non-repudiation" of information systems.[7] IA, in combination with CND, is key to ensuring that our information systems are protected and defended from adversaries, thereby allowing us to share awareness, create knowledge, enhance command and control, and support collaboration and self-synchronization.[8]

b. **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 that eliminate or reduce to an acceptable level the vulnerabilities of friendly actions to adversary exploitation."[9]

---

[5] *See* JP 3-13, *supra* note 1 at I-9.

[6] *Id.* at viii-ix.

[7] *Id*. at III-1.

[8] CHAIRMAN, JOINT CHIEFS OF STAFF INSTR. 6510.01C, INFORMATION ASSURANCE AND COMPUTER NETWORK DEFENSE (1 May 2001), at A-1 (hereinafter CJCSI 6510.01C).

[9] *See* JP 3-13, *supra* note 1 at III-4.

c. **EW**. Along with those activities mentioned above, EW activities that contribute to defensive IO include frequency management, changing call signs, and taking steps to counteract attacks against force radio frequencies, and electro-optical and infrared capabilities.

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

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

f. **Counterintelligence (CI)** activities contribute to defensive IO by providing information and conducting activities to protect and defend friendly information systems against espionage, sabotage, or terrorist activities.

g. **CND** is the mission to "defend computer systems and networks from unauthorized activity, which degrades mission performance and adversely impacts survivability." CND will be discussed below.

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

a. **PA**. PA seek a timely flow of information to both external and internal audiences. PA programs contribute to IA 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."[10] The news media and other information networks' increasing and virtually instantaneous availability to society's leadership, population, and infrastructure can have significant impact on national will, political direction, and national security objectives and policy.

b. **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."[11]

II. DEFENDING U.S. CRITICAL INFRASTRUCTURE AND INFORMATION SYSTEMS

A. "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."[12]

B. 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).

C. Recognizing the vulnerabilities created by U.S. dependence upon information technology, on 15 July 1996, President Clinton promulgated **Executive Order 13010**, establishing the "President's Commission on Critical

[10] *Id*. at I-17.

[11] *Id*.

[12] 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).

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.

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

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

2. **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 U.S. policy to take all necessary measures to swiftly eliminate any significant vulnerability to physical or information attacks on critical U.S. infrastructures, particularly our information systems.

E. On 22 October 2001, President Bush issued **Executive Order 13231**, Critical Infrastructure Protection in the Information Age. In that Order, President Bush states: "It is the policy of the United States to protect against disruption of the operation of information systems for critical infrastructure and thereby help to protect the people, economy, essential human and government services, and national security of the United States and to ensure that any disruptions that occur are infrequent, of minimal duration, and manageable, and cause the least damage possible." To help accomplish this, EO 13231 establishes the President's Critical Infrastructure Protection Board.

F. On 17 December 2003, President Bush issued Homeland Security Presidential Directive 7, Critical Infrastructure Identification, Prioritization, and Protection. This directive tasks Federal departments with the responsibility to "identify, prioritize, and coordinate the protection of critical infrastructure and key resources in order to prevent, deter, and mitigate the effects of deliberate efforts to destroy, incapacitate, or exploit them. Federal departments and agencies will work with State and local governments and the private sector to accomplish this objective." The Secretary of the Department of Homeland Security (DHS) is tasked with coordinating the "overall national effort to enhance the protection of the critical infrastructure and key resources of the United States."

G. These authorities place emphasis on the protection of IO systems tied to critical national infrastructure, including those associated with national security. They also task each agency with responsibility to protect its own systems. However, DHS is the overall coordinator and Department of Justice (DOJ) has the lead in investigation and prosecution of any attacks on those critical IO systems.

III. INTERNATIONAL LEGAL CONSIDERATIONS IN IO

A. IO is governed by both pre-hostilities law, or *jus ad bellum*, and the law of war, or *jus in bello*, once hostilities have begun.

B. **IO in *Jus ad Bellum***. As explained in Chapter 1 of this Handbook, the primary *jus ad bellum* document is the UN Charter, and the ultimate question, based on UN Charter articles 2(4), 39, and 51, is whether a particular application of IO equates to a "use of force" or "armed attack."

1. 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 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."[13]

2. Further, some aspects of IO may not even cross the threshold of a use of force under article 2(4). "The dilemma lies in the fact that CNA [and IO in general] spans the spectrum of consequentiality. Its effects freely range from mere inconvenience (*e.g.*, shutting down an academic network temporarily) to physical destruction (*e.g.*, as in creating a hammering phenomenon in oil pipelines so as to cause them to burst) to death (*e.g.*, shutting down power to a hospital with no back-up generators)."[14]

3. To determine the legality of any pre-hostilities action under the UN Charter, it is necessary to determine where that action would fit along the spectrum of force: below the threshold of a use of force under article 2(4), a "use of force" under article 2(4), or an armed attack under article 51 giving the victim state the right to respond in self-defense.

4. **Offensive IO**. Any offensive IO prior to hostilities must comply with the UN Charter. While the principles are similar with any aspect of IO, the area of CNO is probably the most likely to create significant legal issues.

a. 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. It seems likely that the international community will be more interested in the **consequences** of a CNA than in the means used. A CNA can cause significant property and economic damage, as well as human fatalities, by utilizing the Internet to cause a variety of effects, such as: flooding by opening the flood gates of a dam; train wrecks by switching tracks for oncoming trains; plane crashes by shutting down or manipulating air traffic control systems; large chemical explosions and fires by readjusting the mix of volatile chemicals at an industrial complex; 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 actor. The effect can be the same, if not more severe, as if the destruction was caused by conventional kinetic means of warfare.[15]

b. Though there is little state practice to help determine how the international community will view offensive IO, "it seems likely that the international community will be more interested in the consequences of a computer network attack [or other means of IO] than in its mechanism."[16] This means that the method of IO is less important than the effects of a particular IO when establishing the legality of an action.

5. **Defensive IO**. As with offensive IO, legal issues are most likely to occur in the area of CNO. Equipment necessary for CNA is readily available and inexpensive, and access to many computer systems can be obtained through the Internet. As a result, many U.S. military and non-military information systems are subject to CNA anywhere and anytime. The 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. 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, or mercenaries. When determining lawful actions in response to a CNA, attribution, characterization, the doctrine of neutrals, and the international rules regarding self-defense should guide any U.S. military response.

a. **Attribution** of an attack to the responsible actor is very important in determining an appropriate response. However, 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

---

[13] *Id* at 101.

[14] Michael N. Schmitt, *Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework*, 37 COLUM. J. TRANSNAT'L L 885, at 912.

[15] *See* Sharp, *supra* note 12, at 101-02.

[16] DEP'T OF DEFENSE OFFICE OF THE GENERAL COUNSEL, AN ASSESSMENT OF LEGAL ISSUES IN INFORMATION OPERATIONS, 16 (2d ed. 1999) [hereinafter DoD OGC].

generates false origin information. 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.[17]

b. **Characterization** of the intent and motive underlying attack may also be very difficult, though equally important, when determining an appropriate response. 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 action in defense.[18]

c. **Neutrality**. As a general rule, all acts of hostility in neutral territory, including neutral lands, waters, and airspace, are prohibited. Although a neutral nation may allow belligerents to use information systems that simply relay communications (like phone networks), a belligerent nation has a right to demand that a neutral nation prevent belligerents from using information systems that generate information to support their belligerent activities. If the neutral nation is unable or unwilling to do so, other belligerents may have a limited right of self-defense to take necessary and proportionate action against the neutral nation (*e.g.*, jamming) to prevent such use by the enemy.

(1) A limited exception exists for **communications relay systems**. Articles 8 and 9 of 1907 *Hague Convention respecting Rights and Duties of Neutral Powers and Persons in Case of War on Land* (U.S. 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.

(2) **International consortia** present special problems. Where an international communications system is developed by a military alliance, such as NATO, few neutrality issues are likely to arise. 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. Consortia such as INTELSAT, INMARSAT, ARABSAT, EUTELSAT and EUMETSAT have attempted to deal with this possibility by limiting system uses during armed conflict. However, INMARSAT nations have determined that this language permits use by UN Security Council authorized forces, even while engaged in armed conflict.

d. **Self-Defense**.

(1) 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.[19] Even if the systems attacked were unclassified military logistics systems, an attack upon such systems might seriously threaten a nation's security. 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 state might respond in self-defense to disable the equipment and personnel used to mount the offending attack.

(2) 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. 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).[20]

---

[17] *Id* at 19.

[18] *Id*.

[19] *Id* at 16.

[20] *Id*. at 17

(3) 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. 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. At 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.

(4) 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 kind, 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 CNA, international law in this area will develop through the actions of nations and through the positions the nations adopt publicly as events unfold.

C. **IO in *Jus in Bello***.

1. While some have termed IO, and particularly CNO, as a revolution in military affairs,[21] use of various forms of IO generally require the same legal analysis as any other method or means of warfare. However, there are some aspects of IO that deserve special mention.

2. **Treachery or Perfidy**. Article 37 of Protocol I to the Geneva Conventions prohibits belligerents from killing, injuring, or capturing an 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. 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. 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. "*Morphing*" techniques, while not a violation of the law of war generally, if used to create an image of the enemy's chief of state falsely informing troops that an armistice or cease-fire agreement exists would be considered perfidy, and constitutes a war crime.[22]

3. **Unintended Consequences**. Some have raised the issue of the unintended consequences that might arise from the use of IO in warfare. Some have argued that various means of IO may not be controllable, such as CNO involving a virus or malicious logic, and are therefore illegal.[23] While CNO may increase the number and types of targets available, this increased access does not require an increased standard of care. The same legal analysis is required for any IO targeting, including the analysis of potential collateral damage and unintended consequences.

4. **Civilians**. One of the most unsettled issues is the role of civilians in IO. As mentioned in Chapter 2 of this Handbook, civilians lose their protected status when they take an "active part" (or "direct part," depending on whose view of the law you ascribe to) in hostilities. In the area of IO, "[s]ome countries have elected to contract out information warfare functions, whether those functions involve the maintenance of assets or the conduct of operations. Moreover, computer network attack is a function that may be tasked to government agencies other than the military."[24] State practice in this area is undeveloped, but it appears that the role of civilians in this area will only increase over time.

---

[21] Michael N. Schmitt, *Wired Warfare: Computer Network Attack and Jus in Bello*, 846 INT'L REVIEW OF THE RED CROSS 365, 365 (2002) [hereinafter Schmitt, Wired Warfare], *available at* http://www.icrc.org/Web/eng/siteeng0.nsf/iwpList501/E4E4A03DE3BE1211C1256BF900332F62.

[22] *See* DoD OGC, *supra*, note 16, at 8-9

[23] *See* Schmitt, Wired Warfare, *supra* note 21, at 389

[24] *Id*. at 383.

D. **Assessment.** It is not clear what IO techniques will be considered to be a "use of force," or what kinds of information operations may be considered to constitute "armed attack." 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 actions are likely to be judged by applying traditional Law of War principles. DoD Office of the General Counsel adopts a results test. In their "Assessment," they conclude that "If a coordinated computer network attack shuts down a nation's air traffic control system along with its banking and financial systems and public utilities, and opens the floodgates of several dams resulting in general flooding that causes widespread civilian deaths and property damage, it may well be that no one would challenge the victim nation if it concluded that it was a victim of an armed attack, or of the equivalent to an armed attack."[25] While this is helpful in the event of a catastrophic CNA, it does not provide much guidance for CNAs that affect only one of the systems mentioned.

E. Communications law and IO.[26]

1. **International Communications Law**. International communications law consists primarily of a number of bilateral and multilateral communications treaties. The *International Telecommunications Convention of 1982 (ITC)* (the Nairobi Convention) is the most significant. The ITC is the latest in a series of multilateral agreements that establish the International Telecommunication Union (ITU) (a specialized agency of the UN). 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. They also establish mutual legal obligations among parties, several of which are directly relevant to IO.

a. **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."

b. **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." This provision would appear to restrict IO 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." 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." 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 IO.

d. The ITC permits member nations to interfere with international communications in certain circumstances. 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." 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."

e. 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,

[25] DoD OGC, *supra* note16 at 16.

[26] *See generally* DoD OGC, *supra* note16, at 30-32.

incoming or in transit, provided that it immediately notifies such action to each of the other members through the medium of the Secretary-General."

f. It seems clear that ITC provisions apply primarily in peacetime. The treaty does not specifically state whether it applies during armed conflict. 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. **Domestic Communications Law**. The ITC obligates each member nation to suppress acts by individuals or groups within its territory that interfere with the communications of other members. **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." DoJ, Office of Legal Counsel, issued a written opinion providing in effect that 47 USC § 502 does not apply to actions of the U.S. military executing instructions of the President acting within his constitutional powers to conduct foreign policy and to serve as Commander-in-Chief.

3. **Assessment**. Neither international nor domestic communications law presents any significant barrier to U.S. military IO. International communications law contains no direct and specific prohibition against the conduct of IO by military forces, even in peacetime. Established state practice evidences that nations regard telecommunications treaties as suspended among belligerents during international armed conflict. Domestic communications laws do not prohibit properly authorized military IO.

IV. FOREIGN DOMESTIC LAW AND CNO[27]

A. Foreign domestic laws, like U.S. criminal statutes addressing computer-related offenses, space activities, communications, and the protection of classified information, may have important implications for U.S. forces' conduct of information operations. The state of domestic laws dealing with high-tech misconduct varies enormously from country to country.

B. 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 the state of the nation's domestic criminal law may have a significant effect on U.S. IO conducted in the nation's territory or involving communications through the nation's communications systems.

C. U.S. forces must determine whether local laws prohibit contemplated IO activities. These prohibitions are important because individuals who order or execute prohibited activities might be subject to prosecution in a host nation criminal court.

V. LAW ENFORCEMENT ASPECTS OF IO

A. As mentioned above, DoD has the responsibility to take necessary steps to protect its own information systems. When DoD's information systems are compromised, DoJ has the lead in investigating and prosecuting those responsible, until it is determined to involve some other investigative agency. There are several domestic statutory provisions that provide the basis for criminal prosecution in such cases.

B. Electronic Communications Privacy Act of 1986 (ECPA).[28] ECPA was enacted 18 U.S.C. §§ 2701-11, §§ 3121-27, § 1367, § 3117, § 2521, and made numerous amendments to provisions of the Communications Act of 1934. § 107 of the Act specifically limits its statutory application to law enforcement functions. "Nothing contained … constitutes authority for the conduct of any intelligence activity."

---

[27] *See generally* DoD OGC, *supra* note16, at 39-42.

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

1. ECPA makes it 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. 18 U.S.C. § 2703(c) states that, with a subpoena, the government can obtain a 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. 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. 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. § 209 of the USA PATRIOT Act now authorizes the seizure of stored voice communications under §2703 with a search warrant. § 211 of the USA PATRIOT Act also clarifies that ECPA and "trap and trace" rules govern cable companies' records for telephone and Internet services.

2. There are nine 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); and (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).

C. 18 U.S.C. § 2709, Counterintelligence access to telephone toll and transactional records. 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. The FBI must certify that the information sought is relevant to an authorized foreign counterintelligence investigation and that 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.

D. 18 U.S.C. § 1029 prohibits a wide range of offenses dealing with using counterfeit access devices: knowingly and with intent to defraud (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. Offenses are punishable by either 10 or 15 years confinement with fines.

1. 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, 18 U.S.C. § 1029 (e)(1). The term "unauthorized access device" means any access device that is lost, stolen, expired, revoked, canceled, or obtained with intent to defraud.

2. 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[29] (*codified at* 47 U.S.C. § 153). The USA PATRIOT Act § 377 provides for extraterritorial jurisdiction for certain "access device" offenses under 18 USC § 1029, such as stolen computer passwords, credit card account numbers, or other counterfeit or unauthorized devices.

E. Computer Fraud and Abuse Act, (*codified as amended at* 18 U.S.C. § 1030). The Act contains eleven specified crimes: 6 felony offenses and 5 misdemeanor offenses, including:

1. Computer Espionage, 18 U.S.C. § 1030 (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.

[29] 48 Stat. 1064 , *codified as amended* 47 U.S.C. 151 – 614.

2. Financial Records, 18 U.S.C. § 1030 (a)(2): intentional access without authorization, or exceeding authorized access, to information from any department of the U.S., computer records of financial institutions, or information from a protected computer involved in interstate commerce.

3. Government Computers, 18 U.S.C. § 1030 (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, 18 U.S.C. § 1030 (a)(4): knowingly, and with intent to defraud, accessing a protected computer.

5. Unlawful Computer Trespassers, 18 U.S.C. § 1030 (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, 18 U.S.C. § 1030 (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 that affects interstate commerce.

7. Extortion, 18 U.S.C. § 1030 (a)(7): knowingly, and with intent to defraud, transmits any communication containing a threat to cause damage to a protected computer. § 202 of the USA PATRIOT Act added any felony violation of the Computer Fraud and Abuse Act to the list of offenses that support a voice wiretap order.

F. 18 U.S.C. § 793 deals with Gathering, Transmitting, or Losing Defense Information. The information need not be classified to constitute a violation of this statute if the information is not generally accessible to the public.[30] 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. 18 U.S.C. § 794 deals with Gathering or Delivering Defense Information to Aid Foreign Government. 18 U.S.C. § 798 concerns 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."

G. The Economic Espionage Act of 1996. 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. 18 U.S.C. § 1832 prohibits theft of trade secrets without requiring the intent to benefit a foreign government, instrumentality, or agent.

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

1. 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.

2. 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.

I. Interception of Wire, Oral, and Electronic Communications. Within DoD, the relevant guidance is contained in DoDD 5505.9, Interception of Wire, Electronic, and Oral Communications for Law Enforcement Purposes, (20

[30] 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).

Apr. 1995) and DoD 0-5505.9-M Procedures for Wire, Electronic, and Oral Interceptions for Law Enforcement Purposes (May 1995).

J. The Foreign Intelligence Surveillance Act of 1978[31] (FISA). FISA revolves around the core definition of foreign intelligence information, which is information that relates to the ability of the U.S. 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 a 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.

1. FISA is the statutory mechanism for obtaining two major categories of information related to defensive IO: (1) acquisition of "nonpublic communication" by electronic means[32] 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; and (2) physical searches seeking to obtain foreign intelligence information.

2. § 214 of the USA PATRIOT Act eliminates the requirement of showing specific and articulable facts to believe the targeted line is being used by an agent of a foreign power, or in communication with such an agent to get a FISA pen register, trap and trace authorization. § 218 changes the requirement that obtaining foreign intelligence was "the" purpose of the search to now being "a significant purpose" of the search.

K. USA PATRIOT Act. In addition to those specific provisions mentioned above, the PATRIOT Act also makes the following changes to pre-existing laws. [NOTE: certain PATRIOT Act provisions are subject to a sunset clause and will expire in December 2005 unless they are renewed.]

1. § 203b allows investigative or law enforcement officers to disclose foreign intelligence information without a court order to any other Federal law enforcement, intelligence, protective, immigration, national defense, or national security official to assist in official duties.

2. § 210 updates and expands records available by subpoena to add the means and source of payment, credit card or bank account number, records of session times and durations, and any temporarily assigned network address.

3. § 216 applies to any non-content information; that is, "dialing, routing, addressing, and signaling information" if the information is relevant to an ongoing criminal investigation. It also allows for nationwide Federal pen/trap orders.

4. § 217 allows victims of computer attacks to authorize persons "acting under color of law" (law enforcement or counterintelligence) to monitor trespassers on their computer systems.

5. § 219 allows judges in domestic or international terrorism cases to issue search warrants in any district in which acts may have occurred, for property or persons within or outside district.

6. § 220 allows single jurisdiction search warrants for e-mail.

L. 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." The National Security Agency is the proponent under National Telecommunications and Information Systems Security Directive (NTISS) Directive No. 600, Communications Security Monitoring. COMSEC is one of the tools available to fulfill the DoD mandate to accredit

[31] 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.

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

automated information systems and ensure "compliance with automated information systems security requirements."[33]

1. Implemented within the Army by AR 380-53,[34] 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.

2. There are certain prerequisites for Information Systems Security 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; and (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.

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 IO activities will continue to be to break out the separate elements and circumstances of particular planned activities, and then to make an informed judgment as to how existing international legal principles are likely to apply to them. In some areas, such as the law of war, existing legal principles can be applied with considerable confidence. For example, attacks upon "dual-use" infrastructures (those used for both military and civilian purposes) require that commanders make reasonable efforts to discover foreseeable collateral damage. Commanders must consider whether the system contemplated for attack is essential to public health and safety. The proportionality principle operates in the same way whether an attack is conducted using traditional kinetic weapons, or in the form of CNA. In other areas, such as the application of use of force principles, 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.

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

[34] U.S. DEP'T OF ARMY, ARMY REGULATION 380-53, INFORMATION SYSTEMS SECURITY MONITORING (29 April 1998). available at http://www.acert.belvoir.army.mil/ar380_53.pdf.