

CHAPTER 8

INFORMATION OPERATIONS AND CYBERSPACE OPERATIONS

REFERENCES

1. U.S. DEP'T OF DEF., DIR. 3600.01, INFORMATION OPERATIONS (IO) (May 2, 2013)(Unclassified) [hereinafter DODD 3600.01].
2. U.S. DEP'T OF DEF. OFFICE OF GEN. COUNSEL, *An Assessment of International Legal Issues in Information Operations* (2d. ed. Nov. 1999), 76 Int'l Legal Stud. 459 (2002)(Naval War College Int'l Law Dep't 'Bluebook' series, vol. 76 app.) [hereinafter DoD OGC Assessment].
3. U.S. DEP'T OF DEF., DEPARTMENT OF DEFENSE CYBER STRATEGY (U) (17 Apr 2015)
4. CHAIRMAN OF THE JOINT CHIEF OF STAFF, INSTR. 3121.01B, STANDING RULES OF ENGAGEMENT/ STANDING RULES FOR THE USE OF FORCE FOR US FORCES (U) (13 June 2005)(Classified SECRET) [hereinafter CJCSI 3121.01B]. ***Version 3121.01C pending approval.***
5. CHAIRMAN OF THE JOINT CHIEF OF STAFF, INSTR. 3210.01B, JOINT INFORMATION OPERATIONS POLICY (U) (5 Jan. 2007)(Classified Secret, excerpts in Chapter 5, *infra*) [hereinafter CJCSI 3210.01B].
6. CHAIRMAN OF THE JOINT CHIEF OF STAFF, MANUAL 3130.03, ADAPTIVE PLANNING AND EXECUTION (APEX) PLANNING FORMATS AND GUIDANCE (18 Oct. 12)(Unclassified – Limited Distribution to .mil or .gov domains) [hereinafter CJCSM 3130.03].
7. JOINT CHIEFS OF STAFF, JOINT PUB. 1-02, DICTIONARY OF MILITARY AND ASSOCIATED TERMS (8 Nov. 2010)(as amended through 15 Apr. 2013)(Unclassified) [hereinafter JOINT PUB. 1-02].
8. JOINT CHIEFS OF STAFF, JOINT PUB. 3-13, JOINT DOCTRINE FOR INFORMATION OPERATIONS (27 Nov. 2012)(Unclassified) [hereinafter JOINT PUB. 3-13].
9. JOINT CHIEFS OF STAFF, JOINT PUB. 3-12, CYBERSPACE OPERATIONS (27 Feb. 2013)(Classified SECRET REL/FVEY)[hereinafter JP 3-12, unclassified version JP 3-12R]
10. U.S. DEP'T OF ARMY, FIELD MANUAL 3-13, INFORM AND INFLUENCE ACTIVITIES (25 Jan. 2013) (Unclassified) [hereinafter FM 3-13].
11. U.S. DEP'T OF ARMY, ARMY DOCTRINE REF. PUB. 3-0, UNIFIED LAND OPERATIONS (May 2012) (Unclassified) [hereinafter ADRP 3-0].
12. U.S. DEP'T OF AIR FORCE, DOCTRINE ANNEX. 3-13, INFORMATION OPERATIONS (8 July. 2013) (Unclassified) [hereinafter AFDA 3-13].
13. U.S. DEP'T OF NAVY, NAVY WARFARE PUBLICATION 3-13, NAVY INFORMATION OPERATIONS (Feb. 2014) (Unclassified) [hereinafter, NWP 3-13].
14. U.S. DEP'T OF NAVY, MARINE CORPS OPERATING CONCEPT FOR INFORMATION OPERATIONS (4 Feb. 2013) (Unclassified).
15. TALLINN MANUAL ON THE INTERNATIONAL LAW APPLICABLE TO CYBER WARFARE (Michael N. Schmitt, ed., 2013).

I. INTRODUCTION

A. **Overview:** Information Operations (IO) and Cyberspace Operations (CO), while related, now represent two doctrinally distinct operating concepts. Specifically, IO integrates specific capabilities to affect the decision making of target audiences, while protecting our own decision processes. CO is one of the capabilities under IO, but CO has evolved to the point where it can create effects far beyond the information environment. As such, the Department of Defense now treats cyberspace as an independent “fifth domain” with distinct cyber missions. Despite these differences, IO and CO both take place in the information environment, and as such, share many of the same legal issues. According to Joint Pub. 3-13, Information Operations, information is a strategic resource, vital to national security. Military operations depend on information and information systems for many simultaneous and integrated activities. Success on the battlefield, both immediate and lasting, often depends on success in the information environment. To understand and provide legal advice in this complex area, legal advisors must be familiar with basic IO terminology (section II); capabilities and legal issues raised (section III); and significant international legal authorities (section IV). This chapter addresses these topics.

B. **Sources of Law:** As joint doctrine recognizes, “IO planners deal with legal considerations of an extremely diverse and complex nature.”¹ These include international law, domestic law and policy, military operational plans and directives, and even foreign jurisdiction law. As IO can be conducted across the full spectrum of operations, legal advisors must know not only the authorities governing particular capabilities, but also how to apply them in armed conflict and peacetime situations. When preparing legal advice, take note of two important caveats:

1. **Changing Guidance:** Unlike more established areas of law such as Geneva Conventions obligations, IO/CO legal guidance is constantly changing. New forums such as cyberspace and social media overlap between military and diplomatic missions, and individual tactical decisions can become front-page news and cause strategic effects. In 2010, the Secretary of Defense ordered a Front-End Assessment of strategic communication and information operations, resulting in significant changes to both doctrine and organization.² The Joint Staff subsequently coordinated rewrites of all IO joint doctrine publications, including changes to definitions and accepted terminology for nearly every IO capability. The Department of Defense (DoD) is also updating its IO directives and instructions. Some sources may remain outdated or appear to conflict, and service, theater, or operational guidance may require update. Legal advisors must make a special effort to collate and sensibly apply these sources.

2. **Classified Sources:** Many specific sources of operational guidance remain classified (for example, several Chairman of the Joint Chiefs (CJCS) Instructions specific to IO capabilities). This chapter cites to, but does not discuss, some of these sources.³ Legal advisors are strongly encouraged to seek out, consult, and safeguard classified sources applicable to particular capabilities, commands, and operations. Chances are several will apply.

3. **Operational Guidance:** Specific guidance on IO is found in standard military planning documents, particularly in the Operational Plan (OPLAN), Operational Order (OPORD), and/or Execute Order (EXORD). These documents have standardized formats and annexes, several of which apply directly to IO, and are usually classified to protect military decision-making and strategies. Legal advisors must have a firm grasp of the planning process and standard document formats, and of the roles and responsibilities of varying levels of command to provide input to, promulgate, and execute such orders.⁴ For most IO questions, legal advisors should start their research by looking at existing operational guidance for specific operations and information-related capabilities.⁵

4. **Service-Specific Guidance:** Finally, legal advisors should be sensitive to differences in service-specific guidance. For example, FM 3-13 and ADRP 3-0 both discuss IO and its related capabilities in terms of “inform and influence activities”—a scheme long used by the Army, but not by joint doctrine. Legal advisors may frequently be called on in joint settings to advise other services, and should become familiar with their guidance in order to facilitate communication. The Air Force, Navy, and Marine Corps have all generated their own doctrine and guidance as well.

II. BASIC IO/CO TERMINOLOGY

A. **Overview:** This section defines several basic terms related to IO generally. The primary source for definitions is recently published joint doctrine.⁶ Older sources may employ slightly different terms and definitions.

B. **Information Operations:** “[T]he integrated employment, during military operations, of information-related capabilities in concert with other lines of operation designed to influence, disrupt, corrupt, or usurp the decision making of adversaries and potential adversaries while protecting our own.”⁷

¹ JOINT CHIEFS OF STAFF, JOINT PUB. 3-13, INFORMATION OPERATIONS at III-3 (27 Nov. 2012) [hereinafter JOINT PUB. 3-13]. Unless otherwise noted, all references to Joint Pub. 3-13 refer to the 27 Nov. 2012 version thereof.

² See generally Memorandum from The Secretary of Defense, subject: Strategic Communication and Information Operations in the DoD (25 Jan. 2011) [hereinafter SECDEF 25 Jan 11 Memo].

³ All sources cited herein are unclassified (U) and unrestricted unless otherwise noted. Some sources restrict access to .mil or .gov network domains; others are Unclassified//For Official Use Only (U//FOUO) or classified (e.g., SECRET). This chapter discusses in detail only unrestricted, publicly available and/or previously released information, including unclassified titles and publication numbers of classified documents.

⁴ See JOINT CHIEFS OF STAFF, JOINT PUB. 5-0, JOINT OPERATION PLANNING (11 Aug. 2011). This document describes the joint planning process and its plans and orders. Appendix A lists the standard operational plan format and annexes.

⁵ See JOINT PUB. 3-13, *supra* note 1, ch. 4 (describing how IO and IRCs are integrated into the joint planning process).

⁶ Due to the myriad disciplines comprising IRCs, each with its own governing directives, this chapter focuses discussion on joint doctrine and regulations. It does not cite service-specific guidance, other than general references listed in references above. Lawyers advising service-specific entities will need to seek out and consult applicable service-specific guidance for specific IRCs and functional communities.

C. **Information Environment:** “[T]he aggregate of individuals, organizations, and systems that collect, process, disseminate, or act on information. This environment consists of three interrelated dimensions which continuously interact with individuals, organizations, and systems. These dimensions are the physical, informational, and cognitive . . .”⁸ The information environment forms part of the overall operational environment, which includes “the composite of the conditions, circumstances, and influences that affect employment of capabilities and bear on the decisions of the commander . . .”⁹

D. **Information-Related Capabilities (IRCs):** “[T]he tools, techniques, or activities that affect any of the three dimensions of the information environment. They affect the ability of the target audience (TA) to collect, process, or disseminate information before and after decisions are made.”¹⁰

1. Information operations focus on the integrated application of IRCs as force multipliers to achieve desired effects, not who owns particular capabilities.¹¹ While some IRCs are technology-based, others are not. Different organizations control individual capabilities, at multiple levels of command, and must come together to integrate IO efforts. Legal advisors should have a firm grasp of command and control for IO (i.e., approval and coordinating authorities and lead/supporting organizations for particular capabilities), and should reach out to other lawyers advising these groups and levels to ensure consistent advice across the legal community.

2. Joint Pub. 3-13 eliminates the former¹² hierarchy of core, related, and supporting capabilities and instead lists¹³ the following fourteen IRCs. Note that Cyberspace Operations are often placed into a separate category, due to its emerging importance. This list is representative, not exhaustive, of capabilities:

- Strategic Communication (SC)
- Joint Interagency Coordination Group (JIACG)
- Public Affairs (PA)
- Civil-Military Operations (CMO)
- Cyberspace Operations (CO)
- Information Assurance (IA)
- Space Operations (Space Ops)
- Military Information Support Operations (MISO)
- Intelligence (Intel)
- Military Deception (MILDEC)
- Operations Security (OPSEC)
- Special Technical Operations (STO)
- Joint Electromagnetic Spectrum Operations (JEMSO)
- Key Leader Engagement (KLE)

3. Joint Pub. 3-13 also introduces, eliminates, renames, or reorganizes several capabilities. SC and the JIACG include defense support to public diplomacy and take a whole-of-government approach to IO. CO and MISO introduce new terms for the former capabilities of computer network operations (CNO) and psychological operations (PSYOP), respectively. Intel includes counterintelligence (CI), and recognizes the broader intersection between IO and Intel efforts. JEMSO, a new term, includes both electronic warfare (EW) and joint electromagnetic spectrum management operations (JEMSMO). Finally, Joint Pub. 3-13 now recognizes Space Ops, STO, and KLE IRCs, while it omits physical security, physical attack, and combat camera as these are ends and means.¹⁴ The next section discusses each IRC and its specific sources of guidance.

4. Finally, though joint doctrine provides general guidelines on employing IRCs effectively, legal advisors should always consult operational and tactical guidance contained in approved military plans, orders, and rules of engagement. These sources specify theater-specific criteria and approval authorities for use of IRCs.

E. **Cyberspace:** “A global domain within the information environment consisting of the interdependent network of information technology infrastructures, including the internet, telecommunications networks, computer systems, and embedded processors and controllers. (See Deputy Secretary of Defense Memo of March 12, 2008)

⁷ JOINT PUB. 3-13, *supra* note 1, at I-1.

⁸ *Id.*

⁹ *Id.* at I-1 to I-2. Chapter I of Joint Pub. 3-13 discusses the information environment and its domains, and the application of IO within that environment, in greater detail.

¹⁰ *Id.* at I-3.

¹¹ See *id.* at I-5, II-5; SECDEF 25 Jan 11 Memo, *supra* note 2, at 2.

¹² See JOINT CHIEFS OF STAFF, JOINT PUB. 3-13, INFORMATION OPERATIONS at III-3 (13 Feb. 2006). The 27 Nov. 2012 edition of Joint Pub. 3-13 substantially updates the 13 Feb. 2006 version.

¹³ See JOINT PUB. 3-13, *supra* note 1, at I-1.

¹⁴ Compare *id.*, ch. II (27 Nov. 2012) with JOINT PUB. 3-13, *supra* note 10, ch. II (13 Feb. 2006).

III. SIGNIFICANT LEGAL CONSIDERATIONS IN INFORMATION/CYBERSPACE OPERATIONS

A. Joint Pub. 3-13 warns that:

IO planners deal with legal considerations of an *extremely diverse and complex nature*. Legal interpretations can occasionally differ, given the complexity of technologies involved, the significance of legal interests potentially affected, and the challenges inherent for law and policy to keep pace with the technological changes and implementation of IRCs. Additionally, policies are regularly added, amended, and rescinded in an effort to provide clarity. As a result, IO remains a *dynamic arena*, which can be further complicated by multinational operations, as each nation has its own laws, policies, and processes for approving plans. . . .¹⁵ The nature of IO is such that the exercise of operational authorities requires a detailed and rigorous legal interpretation of authority and/or legality of specific actions.¹⁶

Section IV deals with specific authorities for particular IO capabilities. This section elaborates in greater detail on the legal authorities for IO under the United Nations Charter and the Law of Armed Conflict. Regarding the law generally, the best consolidated assessment is an IO assessment prepared by the DoD Office of General Counsel in 1999.¹⁷ Though dated, many of the issues raised remain the same or similar to those faced by legal advisors today.

B. Authorities and responsibilities:

The authority to employ IRCs, to include Cyberspace Operations, is rooted foremost in Title 10, United States Code (USC). While Title 10, USC, does not specify IO separately, it does provide the legal basis for the roles, missions, and organization of DOD and the Services. Title 10, USC, Section 164, gives command authority over assigned forces to the Combatant Commander (CCDR), which provides that individual with the authority to organize and employ commands and forces, assign tasks, designate objectives, and provide authoritative direction over all aspects of military operations. Cyberspace operations also form an increasing part of the United States intelligence gathering capability. When used for the primary purpose of gathering intelligence (collecting information), the authorities include Executive Order 12333 and National Security Council Intelligence Directive 6. Finally, the rise of cyberspace operations has given added emphasis to the issue of “convergence” between Title 10 and Title 50 operations, and the debate on whether cyberspace operations qualify as “traditional military activities.”¹⁸

DoD and [CJCS] directives delegate authorities to DoD components. Among these directives, DODD 3600.01, Information Operations, is the principal IO policy document. Its joint counterpart, Chairman of the Joint Chiefs of Staff Instruction (CJCSI) 3210.01, Joint Information Operations Policy, provides joint policy regarding the use of IRCs, professional qualifications for the joint IO force, as well as joint IO education and training requirements. Based upon the contents of these two documents, authority to conduct joint IO is vested in the CCDR, who in turn can delegate operational authority to a subordinate JFC, as appropriate.¹⁹

¹⁵ JOINT PUB. 3-13, *supra* note 1, at III-3 (emphasis added).

¹⁶ *Id.* at III-1.

¹⁷ U.S. Dep’t of Def. Office of Gen. Counsel, *An Assessment of International Legal Issues in Information Operations* (2d. ed. Nov. 1999), 76 Int’l Legal Stud. 459 (2002)(Naval War College Int’l Law Dep’t ‘Bluebook’ series, vol. 76 app.) [hereinafter DoD OGC Assessment].

¹⁸ 50 U.S.C. § 3093(e). The concept of “convergence” is one of the biggest issues facing leaders planning both information and cyberspace operations. Generally, this term refers to the institutional and functional overlap between DoD and the intelligence community. Some analysts refer to this as the Title 10/50 debate, though this is not entirely accurate as Title 10 authorities allow intelligence collection and some Title 50 authorities authorize direct action. Under the Covert Action Statute, whenever appropriated funds are spent on a covert action, the President must: (1) find that the operation is necessary for national security, and (2) notify Congress – though this can be done *after* the operation has concluded. Traditional Military Activities (or TMA) are an exception to the Covert Action Statute’s requirements. In the kinetic world, a mission qualified as a traditional military activity if it: (1) was commanded by a military commander, (2) staffed by military personnel, and (3) pursuant to ongoing or anticipated hostilities in which U.S. involvement is apparent or intended to be acknowledged at some point in the future. Some analysts argue that a fourth prong exists, that the operation must be “traditional,” or one that the military has customarily performed in the past. The key question facing the USG is which IO and CO qualify as a Traditional Military Activity.

¹⁹ *Id.*

C. General considerations for legal advice:²⁰

1. “Could the execution of a particular IRC be considered a hostile act by an adversary or potential adversary?” (*jus ad bellum* issues under the United Nations Charter).
2. “Do any non-US laws concerning national security, privacy, or information exchange, criminal and/or civil issues apply? (foreign domestic law, or host nation or coalition partner bilateral agreements)
3. “What are the international treaties, agreements, or customary laws recognized by an adversary or potential adversary that apply to IRCs?” (international law)
4. “How is the joint force interacting with or being supported by US intelligence organizations and other interagency entities?” (domestic law, including intelligence and national security law)
5. Is it “directed at or intended to manipulate audiences, public actions, or opinions in the United States?” (2013 DoDD 3600.01, para. 3.k. requirement)

D. **IO/CO and *Jus ad Bellum*:** Similar to the physical world, the primary *jus ad bellum* document is the United Nations (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 an “armed attack.”²¹

1. 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) but shy of an armed attack under Article 51, or an armed attack under Article 51, giving the victim State the right to respond in self-defense.²² Note that the United States position is different from the UN Charter in the sense that the United States will invoke its right to self-defense against any illegal use of force, not just an armed attack. On September 23, 2012, at the USCYBERCOM Legal Conference, Mr. Harold Koh, then the legal advisor for the Secretary of State, repeated the United States position, rejecting the idea that a “gap” exists between Use of Force and Armed Attack as a trigger to the right of self-defense.

2. Use of force is commonly understood to include a kinetic military attack by one State against the territory, property, or citizens of another State, i.e., an armed attack, some State activities falling short of an armed attack may also cross the threshold of the Article 2(4) use of force. For example, some States and scholars consider the use of economic or political force to be a use of force prohibited by Article 2(4).²³ “The Article 2(4) prohibition on the use of force also covers physical force of a non-military nature committed by any state agency.”²⁴ This economic or political force may cross the use of force threshold, but not the Article 51 armed attack threshold.

3. Some aspects of IO/CO crossing the use of force threshold under Article 2(4) may go one step further, becoming an armed attack and triggering a State’s right to Article 51 self-defense under the UN Charter viewpoint (unlike the economic or political force mentioned above). “The dilemma lies in the fact that [CO and IO] span the spectrum of consequentiality. [Their] 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).”²⁵

4. Determining when an IO/CO amounts to a use of force or an armed attack is difficult at best. 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 may be considered a use of force, to which the victim state may be able to respond legally in self-defense.

²⁰ *Id.* at III-3 (listing these four considerations).

²¹ See THOMAS C. WINGFIELD, *THE LAW OF INFORMATION CONFLICT* pt. II (2000).

²² See *id.* at 128.

²³ See THE CHARTER OF THE UNITED NATIONS: A COMMENTARY 118-19 (Bruno Simma ed., 2002). This is the minority view; the prevailing view and U.S. view is Article 2(4) does not extend to economic and political force. See *id.* Some scholars suggest that Article 2(4) prohibits physical force of a non-military nature, e.g., “the cross-frontier expulsion of populations, the diversion of a river by an up-stream State, the release of large quantities of water down a valley, and the spreading of fire across a frontier.” *Id.*

²⁴ W. G. Sharp, *Critical Infrastructure Protections: A New Era of National Security*, 12 THE FEDERALIST SOC’Y INT’L AND NAT’L SECURITY L. NEWS 1, 101 (1998).

²⁵ 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, 912 (1999) [hereinafter Schmitt, *Thoughts*].

5. Professor Michael Schmitt back in 1999, offered seven factors to determine whether an IO/CO amounts to a use of force under the UN Charter.²⁶ Professor Schmitt was attempting to differentiate military force from economic coercion when creating these factors. He repeated these factors when publishing the 2013 TALLINN MANUAL ON THE INTERNATIONAL LAW APPLICABLE TO CYBER WARFARE, a statement of what the author believed was current customary international law in cyberspace. According to Schmitt, the best approach to analyze an IO *ius ad bellum* issue is to apply a consequence-based analysis, rather than an instrument-based analysis, using the following factors:

- a. **Severity:** Armed attacks threaten physical injury or destruction of property to a much greater degree than other forms of coercion.
- b. **Immediacy:** The negative consequences of armed coercion, or threat thereof, usually occur with great immediacy, while the consequences of other forms of coercion develop more slowly. Thus, the opportunity for the target State or the international community to seek peaceful accommodation is hampered in the former case.
- c. **Directness:** The consequences of armed coercion are more directly tied to the *actus reus* than in other forms of coercion, which often depend on numerous contributory factors to operate. Thus, the prohibition on force precludes negative consequences with greater certainty.
- d. **Invasiveness:** In armed coercion, the act causing the harm usually crosses into the target state, whereas in economic warfare the acts generally occur beyond the target's borders. As a result, even though armed and economic acts may have roughly similar consequences, the former represents a greater intrusion on the rights of the target state and, therefore, is more likely to disrupt international stability.
- e. **Measurability:** While the consequences of armed coercion are usually easy to ascertain (e.g., a certain level of destruction), the actual negative consequences of other forms of coercion are harder to measure. This renders the appropriateness and vehemence of community condemnation less suspect in cases of armed force.
- f. **Presumptive Legitimacy:** In most cases, whether under domestic or international law, the application of violence is deemed illegitimate, absent a specific exception such as self-defense. By contrast, most other forms of coercion—again in the domestic and international sphere—are presumptively lawful, absent a prohibition to the contrary. Thus, the consequences of armed coercion are presumptively impermissible, whereas those of other coercive acts are not (as a very generalized rule).
- g. **Responsibility:** The extent to which the State is responsible for the attack.

6. Professor Schmitt describes an approach to determine whether an IO/CO amounts to an armed attack. “First, a cyber or [IO] attack is an armed attack justifying a forceful response in self-defense if it causes physical damage or human injury or is part of a larger operation that constitutes an armed attack. Second, self-defense is justified when a cyber [or IO] attack is an irrevocable step in an imminent (near-term) and unavoidable attack (preparing the battlefield). Finally, a State may react defensively during the last possible window of opportunity available to effectively counter an armed attack when no reasonable doubt exists that the attack is forthcoming.”²⁷ Thus, Schmitt recognized the need to anticipatory self-defense in cyberspace, though the definition of “imminent” in this realm is up for debate. Note that while the seven factors themselves are not widely used today, they formed the basis for the so-called “effects test” which is in wide use. In fact, during his September 2012 speech to USCYBERCOM, Dept. of State Legal Advisor Harold Koh used aspects of the “effects test” when he stated that a cyber operation was a use of force when it was the proximate and foreseeable cause of death, injury, or physical damage. In addition, Mr. Koh also recognized that the United States reserved the right to use anticipatory self-defense in cyberspace if the circumstances warranted. Finally, In his September 2012 speech, Mr. Koh also noted that the United States would see the disruption of certain vital systems as a use of force giving the United States the right to use force in self-defense. Thus, the United States uses a standard broader than the Schmitt standard, as death, injury, and/or physical damage is not required regarding certain vital systems. Some analysts call this a “modified effects test.”

²⁶ Michael N. Schmitt, *The Sixteenth Waldemar A. Solf Lecture in International Law*, 176 MIL. L. REV. 364, 417 (2003) [hereinafter Schmitt, *Solf Lecture*]; Schmitt, *Thoughts*, *supra* note 25, at 914-15.

²⁷ Schmitt, *Solf Lecture*, *supra* note 26, at 420.

7. **IO/CO on the Offense.** Any offensive IO/CO prior to hostilities must comply with the UN Charter. While the principles are similar to any other aspect of IO, the areas of electronic warfare (EW) and cyberspace operations (CO) are probably the most likely to create significant legal issues.

a. How these principles of international law will be applied to EW and CO 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 EW or a CO than in the means used. An EW or a CO can cause significant property and economic damage, as well as human fatalities. For instance, a State could use a CO 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 actors. . . . The effect can be the same, if not more severe, as if the destruction was caused by conventional kinetic means of warfare.”²⁸

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.”²⁹ At this point, the method of IO is less important than the effects of a particular IO when establishing the legality of an action.

8. **IO/CO on the Defense.** As with offensive IO/CO, legal issues with regard to defensive IO/CO are most likely to occur in the areas of EW and CO. Because equipment necessary for attacks is readily available and inexpensive, and access to many computer systems can be obtained through the Internet, CO poses a particularly important defensive challenge. As a result, many U.S. military and non-military information systems are subject to attack 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. Use of force also applies to all agencies and agents of a State, such as the organized military, militia, security forces, police forces, intelligence personnel, or mercenaries. When determining lawful actions in response to EW or CO, attribution, characterization, and the doctrine of neutrals should guide any U.S. military response.

a. **Attribution** of attack is very important in determining an appropriate response. However, identification of an electronic attack or cyberspace operation originator has often been a difficult problem. This is especially true for a CNA/CO 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. 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.³⁰ To summarize, two facts of attribution exist. The first is the technical side, or finding out the physical source (server for example) of the adversary cyberspace operation. The second aspect of attribution is the legal aspect, determining if a state can held liable for the operation if the source is not a government actor.

b. **Characterization** of the intent and motive underlying an attack may also be very difficult, though equally important when determining an appropriate response. 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 action in defense.³¹

c. **Neutrality.** As a general rule, all acts of hostility in neutral territory, including neutral lands, waters, and airspace, are prohibited. A belligerent nation has a right to demand that a neutral nation prevent belligerents from using its information systems in a manner that violates the nation’s neutrality. If the neutral nation is unable or unwilling to do so, other belligerent(s) 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. It is well settled that creating cyberspace “effects” or striking a cyberspace “target” in a neutral state is a violation of that state’s sovereignty unless consent is given or an exception applies. The more difficult question is whether the mere passage

²⁸ See Sharp, *supra* note 24, at 101-02.

²⁹ DoD OGC Assessment, *supra* note 17, at 483.

³⁰ *Id.* at 19.

³¹ *Id.*

of code through a state's borders ("cyber overflight") is also a violation, even if effects are not being created in the neutral states during passage. This issue is still hotly debated and the U.S. position is classified.

- 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 (to which the 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.
- International consortia (an association or institution for engaging in a joint venture) present special problems. Where an international communications system is developed by a military alliance, such as the North Atlantic Treaty Organization (NATO), few neutrality issues are likely to arise. Other international consortia provide satellite communications and weather data used for both civilian and military purposes. The membership of these consortia virtually guarantees that not all members of a consortium will be allies in future conflicts. Consortia such as the International Communications Satellite Organization (INTELSAT), the International Maritime Satellite Organization (INMARSAT), the Arab Satellite Communications Organization (ARABSAT), the European Telecommunications Satellite Organization (EUTELSAT), and the European Organization for the Exploitation of Meteorological Satellites (EUMETSAT) have attempted to deal with this possibility by limiting system uses during armed conflict. However, INMARSAT nations have determined that the communications relay provision permits use by UN Security Council authorized forces, even while engaged in armed conflict.
- As stated above, if EW or CO 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.³² Even if the systems attacked were unclassified military logistics systems, an attack upon such systems might seriously threaten a nation's security.

d. If a particular EW or CO were considered an armed attack or its equivalent, it follows that the victim nation would be entitled to respond in self-defense by EW, CO or by conventional military means. For example, a State might respond in self-defense to disable the equipment and personnel used to mount the offending attack.

e. 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, 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).³³

f. 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 may have access to information and may corrupt data or degrade the system.

g. 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.

h. It is far from clear the extent to which the world community will regard an EW or a CO as an armed attack or use of force, and how the doctrine of self-defense will be applied to either. The most likely result is an acceptance that a nation subjected to a state-sponsored EA or CO 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 EW and/or CO, international law in this area will develop through the actions of nations and through the positions that nations adopt publicly as events unfold.

E. IO/CO and *Jus in Bello*.

³² *Id.* at 16.

³³ *Id.* at 17.

1. While some have termed IO, and particularly CO, as a revolution in military affairs,³⁴ use of various forms of IO generally require the same legal analysis as any other method or means of warfare.

2. However, IO pose an interesting dilemma; they potentially could run the gamut from mere inconvenience to actual death and destruction in the physical realm. This wide disparity in effects from IO creates a threshold issue that one must examine before applying the *jus in bello* principles.³⁵ Does the IO cause injury, death, damage, or destruction? If so, one must apply *jus in bello* principles; if not, the principles need not be applied to the IO.

3. Applying *jus in bello* principles to IO.

a. Military Necessity/Military Objective.

(1) Article 14 of the Lieber Code defines military necessity as “those measures which are indispensable for securing the ends of war, and which are lawful according to the modern laws and usages of war.” Once a commander determines he or she has a military necessity to take a certain action or strike a certain target, then he or she must determine that the target is a valid military objective. The current definition of a military objective is found in Additional Protocol (AP) I³⁶ to the Geneva Conventions, Article 52(2): “those objects which by their nature, location, purpose or use make an effective contribution to military action and whose total or partial destruction, capture, or neutralization, in the circumstances ruling at the time, offers a definite military advantage.”

(2) The U.S. defines definite military advantage very broadly to include “economic targets of the enemy that indirectly but effectively support and sustain the enemy’s warfighting capability.”³⁷ This broad definition is important in IO because most financial institutions rely heavily on information technology and, under this expansive definition, these economic institutions may become targets for IO.³⁸ For example, a nation’s stock market will generally rely heavily upon information technology like computer systems.

(3) There are specifically protected objects that a force may not target in spite of the fact that they may be military objectives. For example, one may be unable to conduct an IO against a food storage or distribution center.³⁹

b. Distinction/Discrimination.

(1) AP I, Article 48, sets out the rule: “[p]arties to the conflict shall at all times distinguish between the civilian population and combatants and between civilian objects and military objectives and accordingly shall direct their operations only against military objectives.” Additional Protocol I further defines indiscriminate attacks under Article 51(4) as those attacks that:

(a) are “not directed against a specific military objective” (e.g. Desert Storm SCUD missiles);

(b) “employ a method or means of combat, the effects of which cannot be directed at a specified military objective” (e.g., area bombing);

³⁴ 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*]

³⁵ *Id.* at 381.

³⁶ PROTOCOL ADDITIONAL TO THE GENEVA CONVENTIONS OF 12 AUGUST 1949, AND RELATING TO THE PROTECTION OF VICTIMS OF INTERNATIONAL ARMED CONFLICTS (PROTOCOL I), June 8, 1977, 1125 U.N.T.S. 3 (1977), *entered into force* Dec. 7, 1978 (signed by the United States Dec. 12, 1977, not transmitted to U.S. Senate, see S. Treaty Doc. No. 100-2).

³⁷ U.S. NAVAL WAR COLLEGE, ANNOTATED SUPPLEMENT TO THE COMMANDER’S HANDBOOK ON THE LAW OF NAVAL OPERATIONS 8-3 (1997). The United States considers this customary international law. Letter from J. Fred Buzhardt, General Counsel, Department of Defense, to Edward Kennedy, Senator, U.S. Congress (Sept. 22, 1972), *quoted in* Arthur W. Rovine, *Contemporary Practice of the United States Relating to International Law*, 67 AM. J. INT’L L. 118, 123 (1973). *But see* CLAUDE PILLOUD ET AL., COMMENTARY ON THE ADDITIONAL PROTOCOLS OF 8 JUNE 1977 TO THE GENEVA CONVENTIONS OF 12 AUGUST 1949, 636 (Yves Sandoz et al. eds., 1987) [hereinafter COMMENTARY] (stating that “it is not legitimate to launch an attack which only offers potential or indeterminate advantages”).

³⁸ Schmitt, *Wired Warfare*, *supra* note 34, at 381.

³⁹ *See id.* at 385-86. Article 54(2), AP I, prohibits attacks on “objects indispensable to the survival of the civilian population, such as food-stuffs.” The U.S. believes that starvation of civilians shall not be used as a method of warfare, however the U.S. does not subscribe to the belief that starvation of the military would be prohibited. *See* Michael Matheson, Deputy Legal Advisor, U.S. Dep’t of State, Address at the Sixth Annual American Red Cross-Washington College of Law Conference on International Humanitarian Law: A Workshop on Customary International Law and the 1977 Protocols Additional to the 1949 Geneva Conventions (1987) in 2 AM. U.J. INT’L L. & POLICY 419 (1987).

(c) “employ a method or means of combat, the effects of which cannot be limited as required” (use of bacteriological weapons); and

(d) “consequently, in each such case, are of a nature to strike military objectives and civilians or civilian objects without distinction.”

(2) Article 51(2) of AP I requires that “[t]he civilian population as such, as well as individual civilians, shall not be the object of attack.”

(3) According to the commentary to AP I, “[t]he immunity afforded individual civilians is subject to an overriding condition, namely, on their abstaining from all hostile acts. Hostile acts should be understood to be acts which by their nature and purpose are intended to cause actual harm to the personnel and equipment of the armed forces.”⁴⁰ According to AP I, Article 51(3), civilians enjoy the protection against targeting “unless and for such time as they take a direct part in hostilities.” The ICRC Commentary to AP I, Article 51(3), defines direct participation as “acts of war which by their nature or purpose are likely to cause actual harm to the personnel and equipment of the enemy armed forces.”⁴¹ The United States takes a more expansive and functional view of what constitutes direct participation in hostilities. For a more in-depth explanation, consult Chapter 2 of this Handbook.

(4) Government agencies other than the U.S. military have the ability to conduct IO. However, if a civilian takes direct part (defined differently by AP I and the U.S.) in an IO, that civilian becomes an unlawful enemy combatant and loses the protections afforded to civilians under Geneva Convention IV.

(5) Dual-use objects pose another dilemma. A dual-use object is one that is used for both military and civilian purposes. If the object does serve or may serve a military purpose, it may be a valid military target in spite of its civilian purpose. However, the civilian purpose will weigh heavily in the proportionality analysis that must be done for a dual-use target.

(6) Indiscriminate attacks are prohibited by Article 51(4), AP I. This could become an issue for a CO. For instance, if the CO will release a virus, chances are the spread of that virus cannot be controlled, resulting in an indiscriminate attack prohibited by Article 51(4).⁴² Keep in mind the threshold question: this only applies to a CO—in this case a virus—that may cause injury, death, damage, or destruction.

(7) A means or method of warfare that is not directed at a specific military objective violates Article 51(4) as well. For instance, a CO that can be directed at a specific military objective, but is not and rather affects civilian objects, would be prohibited.⁴³ Again one must keep in mind the threshold question.

c. Proportionality.

(1) The test to determine if an attack is proportional is found in AP I, Article 51(5)(b): “[a]n attack which may be expected to cause incidental loss of civilian life, injury to civilians, damage to civilian objects, or a combination thereof, which would be excessive in relation to the concrete and direct military advantage anticipated” violates the principle of proportionality. Note: this principle is only applicable when an attack has the possibility of affecting civilians. If the target is purely military with no known civilian personnel or property in jeopardy, no proportionality analysis need be conducted.

(2) One difficulty in applying the proportionality principle to an IO is determining the proper valuation system for the balancing test.⁴⁴ For instance, how does one value an IO that shuts off basic services such as electricity, water, and/or natural gas?

(3) Another very difficult issue for IO relates to the knock-on effects from an operation. Knock-on effects are “those effects not directly and immediately caused by the attack, but nevertheless the product thereof.”⁴⁵ These knock-on effects are much harder to calculate for IO than kinetic operations and must be considered in the proportionality analysis. For example, an IO that shuts down an electrical grid may have the intended effect of degrading the command and control of the military, but may also have the effect of shutting down electricity for civilian facilities with follow-on effects such as: unsanitary water and therefore death of civilians and

⁴⁰ COMMENTARY, *supra* note 37, at 618.

⁴¹ *Id.* at 619.

⁴² See Schmitt, *Wired Warfare*, *supra* note 34, at 389; DoD OGC Assessment, *supra* note 18, at 472–73.

⁴³ See Schmitt, *Wired Warfare*, *supra* note 34, at 390.

⁴⁴ See *id.* at 392.

⁴⁵ *Id.* at 392.

the spread of disease because the water purification facilities and sewer systems do not work; death of civilians because the life support systems at emergency medical facilities fail; or death of civilians because traffic accidents increase due to a failure of traffic signals.

d. Unnecessary Suffering.

(1) Hague Regulation, Article 22, states that the right of belligerents to adopt means of injuring the enemy is not unlimited. Furthermore, Article 23(e) states that “it is especially forbidden . . . to employ arms, projectiles or material calculated to cause unnecessary suffering.”

e. Treachery or Perfidy. AP I, Article 37 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. Deception measures that 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 armed conflict generally, if used to create an image of the enemy’s Head of State falsely informing troops that an armistice or cease-fire agreement exists would be considered perfidy and would constitute a war crime.⁴⁶

IV. INFORMATION-RELATED CAPABILITIES

A. **Overview:** This section discusses each IRC in greater detail. It lists common legal issues, lead proponents, and capability-specific guidance sources applicable to each capability (in addition to general references listed at the beginning of this chapter). Given the substantial recent changes in IO doctrine and organization discussed in section I.B.1 above, older sources may employ different vocabularies, but remain persuasive until updated or canceled.

B. **Information-Related Capabilities** enumerated in Joint Pub. 3-13:

1. **Strategic Communication (SC):** “Focused United States Government [USG] efforts to understand and engage key audiences to create, strengthen, or preserve conditions favorable for the advancement of [USG] interests, policies, and objectives through the use of coordinated programs, plans, themes, messages, and products synchronized with the actions of all instruments of national power.”⁴⁷

a. Discussion: “SC is a whole-of-government approach, driven by interagency processes and integration that are focused upon effectively communicating national strategy.” SC focuses on IO’s strategic impact, i.e., coordinating and synchronizing efforts to ensure IO objectives complement overall USG objectives.⁴⁸ “SC planning must be integrated into military planning and operations, documented in operation plans (OPLANs) or operation orders (OPORDs), and coordinated and synchronized with [interagency] and multinational partners.”⁴⁹ A principal interagency partner is the U.S. Department of State, which is responsible for the related mission to coordinate public diplomacy.⁵⁰ Though not without controversy,⁵¹ SC remains an important IRC.

b. Common Legal Issue(s): Information fratricide,⁵² i.e. inappropriate messages; Mission overlap with other agencies, e.g. Department of State public diplomacy. At operational and tactical levels, legal advisors

⁴⁶ See DoD OGC Assessment, *supra* note 17, at 472–73.

⁴⁷ JOINT CHIEFS OF STAFF, JOINT PUB. 5-0, JOINT OPERATION PLANNING at II-9 (11 Aug. 2011).

⁴⁸ See JOINT PUB. 3-13 at II-5 to II-6.

⁴⁹ JOINT CHIEFS OF STAFF, JOINT PUB. 3-61, PUBLIC AFFAIRS at I-9 (25 Aug. 2010).

⁵⁰ See 22 U.S.C. § 2732(b)(1) (requiring the Secretary of State to make every effort to “coordinate, subject to the direction of the President, the public diplomacy activities of Federal agencies”). Joint Pub. 3-13 mentions public diplomacy, but notes without explanation that the former doctrinal phrase “defense support to public diplomacy” was approved for removal from joint doctrine.

⁵¹ See, e.g., Memorandum from George E. Little, Assistant to the Secretary of Defense for Public Affairs, subject: Communications Synchronization – A Local Coordination Process (28 Nov. 2012)(critiquing SC as duplicative and purporting to replace the term with ‘communications synchronization’); Admiral Michael G. Mullen, *Strategic Communication: Getting Back to Basics*, 55 JOINT FORCES Q. 2, 4 (4th Q. 2009)(writing as then-Chairman of the Joint Chiefs of Staff, criticizing SC as “arrogant” and arguing it should “integrate and coordinate”).

⁵² “Information fratricide is the result of employing information-related capabilities in a way that causes effects in the information environment that impede the conduct of friendly operations or adversely affect friendly forces.” U.S. DEP’T OF ARMY, FIELD MANUAL 3-13, INFORM AND INFLUENCE ACTIVITIES, para. 1-4 (25 Jan. 2013) [hereinafter FM 3-13].

must ensure IO support and do not undercut USG and command objectives, as defined in theater or operational orders, plans, and other guidance. They must also ensure DoD uses its appropriated funds for the correct missions.

c. Proponents: Undersecretary of Defense for Policy (USD(P)) and the Assistant Secretary of Defense for Public Affairs (ASD(PA)) jointly;⁵³ JIACG representatives on joint staffs.

d. Operational Guidance: Annex Y to the OPLAN addresses Strategic Communications.

e. Sources: NATIONAL FRAMEWORK FOR STRATEGIC COMMUNICATION (2010); UPDATE TO CONGRESS ON NATIONAL FRAMEWORK FOR STRATEGIC COMMUNICATION (2012); JOINT PUB. 3-61, PUBLIC AFFAIRS (25 Aug. 2010); JOINT PUB. 5-0, JOINT OPERATION PLANNING (11 Aug. 2011) (Unclassified); JOINT WARFIGHTING CTR.,⁵⁴ COMMANDER'S HANDBOOK FOR STRATEGIC COMMUNICATION AND COMM. STRATEGY (24 Jun. 2010).

2. **Joint Interagency Coordination Group (JIACG):** “A staff group that establishes regular, timely, and collaborative working relationships between civilian and military operational planners.”⁵⁵

a. Discussion: Interagency coordination occurs between DoD and numerous USG and private entities. Several combatant command (CCMD) staffs include JIACGs to accomplish this coordination, and though IO is not a JIACG's primary focus, “the group's linkage to the IO cell and the rest of the interagency is an important enabler for synchronization of guidance and IO.”⁵⁶

b. Common Legal Issues: Same as SC, discussed in para. III.B.1.a. above.

c. Proponents: Combatant Commands (CCMDs).

d. Operational Guidance: Annex V to the OPLAN addresses Interagency Coordination.

e. Source: Joint Pub. 3-08, Interorganizational Coordination During Joint Operations (24 June 2011).

3. **Public Affairs (PA):** “Those public information, command information, and community engagement activities directed toward both the external and internal publics with interest in the Department of Defense.”⁵⁷

a. Discussion: “PA and IO activities directly support military objectives; counter adversary propaganda, misinformation and disinformation; and deter adversary actions. Although both PA and IO plan and execute public information activities and conduct media analysis, IO may differ with respect to audience, scope, and intent.”⁵⁸ PA provides timely, truthful, and accurate information regarding U.S. intentions and actions both to U.S. and foreign audiences.⁵⁹ Its aims lie in tension with OPSEC (restrict disclosure), MILDEC (deceive the adversary), and to an extent MISO (provide select information to influence, not merely inform). Thus, planners must closely cooperate and deconflict efforts, particularly when both PA and IO target overlapping foreign audiences.⁶⁰ At the same time, PA and IO must maintain sufficient distance within the staff to avoid any appearance of propagandizing U.S. audiences or undermining the command's credibility.⁶¹

b. Common Legal Issues: Requirement that information be truthful; Prohibitions on use of funds for publicity or propaganda purposes within the United States or to influence U.S. public opinion.

c. Proponents: ASD(PA); Joint Staff and service public affairs representatives and staffs.

d. Operational Guidance: Annex F to the OPLAN addresses Public Affairs.

⁵³ See SECDEF 25 Jan 11 Memo, *supra* note 2, at 2. The memo designates these two offices as “SC co-leads” and tasks USD(P) to publish a new DoD directive on SC. The directive remains unpublished as of this writing, as does a proposed new joint doctrine publication on the commander's communication strategy.

⁵⁴ When U.S. Joint Forces Command stood down, the Joint Warfighting Center merged with other organizations and transitioned to supervision by the Joint Staff J7. It is now known as the Joint and Coalition Warfighting Center.

⁵⁵ JOINT CHIEFS OF STAFF, JOINT PUB. 3-08, INTERORGANIZATIONAL COORDINATION DURING JOINT OPERATIONS app. D-1 (24 June 2011).

⁵⁶ JOINT PUB. 3-13, *supra* note 1, at II-7.

⁵⁷ JOINT PUB. 3-61, *supra* note 51, at GL-6 (GL refers to Glossary).

⁵⁸ *Id.* at II-9.

⁵⁹ See *id.* at I-7 to I-9.

⁶⁰ See JOINT PUB. 3-13, *supra* note 1, at II-7.

⁶¹ See JOINT PUB. 3-61, *supra* note 49, at II-9 (noting PA and IO “are separate functional areas.”).

e. Sources: 10 U.S.C. § 2241a⁶² (Supp. 2010) (prohibiting DoD use of funds for publicity or propaganda purposes within the United States); 22 U.S.C. § 1461 and 1461-1a (2006)(similar prohibition, commonly referred to as the ‘Smith-Mundt Act’, for the Dep’t of State); U.S. DEP’T OF DEF., INSTR. 5400.13, PUBLIC AFFAIRS (PA) OPERATIONS (15 Oct. 2008)(Unclassified); U.S. DEP’T OF DEF., INSTR. 5400.14, PROCEDURES FOR JOINT PUBLIC AFFAIRS OPERATIONS (22 Jan. 1996)(Unclassified); U.S. DEP’T OF DEF., DIR. S-3321.1, OVERT PSYCHOLOGICAL OPERATIONS CONDUCTED BY THE MILITARY SERVICES IN PEACETIME AND IN CONTINGENCIES SHORT OF DECLARED WAR (U) (26 July 1984)(Classified Secret); JOINT CHIEFS OF STAFF, JOINT PUB. 3-61, PUBLIC AFFAIRS (25 Aug. 2010)(Unclassified).

4. **Civil-Military Operations (CMO):** “The activities of a commander that establish, maintain, influence, or exploit relations between military forces, governmental and nongovernmental civilian organizations and authorities, and the civilian populace in a friendly, neutral, or hostile operational area in order to facilitate military operations, to consolidate and achieve operational US objectives. Civil-military operations may include performance by military forces of activities and functions normally the responsibility of the local, regional, or national government. These activities may occur prior to, during, or subsequent to other military actions. They may also occur, if directed, in the absence of other military operations. Civil-military operations may be performed by designated civil affairs, by other military forces, or by a combination of civil affairs and other forces.”⁶³

a. Discussion: CMO interact directly with and benefit the local population. CMO representatives can “assist in identifying [target audiences]; synchronizing communications media, assets, and messages; and providing news and information to the local population.” However, CMO remain distinct from IO in that CMO target friendly and neutral populations, with potential secondary impacts to adversary audiences. IO works in the opposite manner, targeting adversaries with potential secondary impacts to friendly and neutral populations. Thus, CMO can yield critical information and goodwill, enabling other IRCs and IO, and should closely coordinate with IO and other IRC planners.⁶⁴

b. Common Legal Issues: Same as SC, discussed in para. III.B.1.a. above (at a tactical, local level).

c. Proponents: Assistant Secretary of Defense for Special Operations and Low Intensity Conflict (ASD(SO/LIC), frequently ASD(SOLIC)); U.S. Special Operations Command (USSOCOM)

d. Operational Guidance: Annex G to the OPLAN addresses Civil-Military Operations.

e. Sources: Humanitarian assistance⁶⁵ fiscal authorities, e.g., 10 U.S.C. § 401 (2006); U.S. DEP’T OF DEF., INSTR. 2205.02, HUMANITARIAN AND CIVIC ASSISTANCE (HCA) ACTIVITIES (2 Dec. 2008); U.S. DEP’T OF DEF., INSTR. 3000.05, STABILITY OPERATIONS (16 Sep. 2009); CHAIRMAN OF THE JOINT CHIEFS OF STAFF, INSTR. 3110.12D, CIVIL AFFAIRS SUPPLEMENT TO THE JOINT STRATEGIC CAPABILITIES PLAN FOR FY 2006 (JSCP FY 06) (U) (15 Apr. 2007)(Classified Secret); JCS, JOINT PUB. 3-57, CIVIL-MILITARY OPERATIONS (8 July 2008).

5. **Cyberspace Operations (CO):** “The employment of cyberspace capabilities where the primary purpose is to achieve objectives in or through cyberspace.”⁶⁶ This term replaces the former doctrinal category of computer network operations (CNO), and any references to CNO should be interpreted as applying to CO. Presidential Policy Directive 20, signed in November 2012, defines Cyberspace Operations in terms of categories. Under PPD 20, cyberspace operations include Cyber Collection, Defensive Cyber Effects Operations (DCEO), and Offensive Cyber Effects Operations (OCEO). PPD 20 defines “cyber effects” as “the manipulation, disruption, denial, degradation, or destruction of computers, information or communications systems, networks, physical or virtual infrastructure controlled by computers or information systems, or information resident thereon.” Note that PPD 20 is still classified TOP SECRET, and full definitions of the above terms are also classified SECRET. JP 3-12, Cyberspace Operations, dated February 2013 and classified SECRET/REL FVEY, uses a different series of terms. JP 3-12 uses different terminology than PPD 20 because PPD 20 applies to Government agencies outside

⁶² Added by National Defense Authorization Act for Fiscal Year 2010, Pub. L. 111-84 § 1031(a)(1) (Oct. 28, 2009), 123 Stat. 2190, 2448. In its entirety, the statute mandates: “Funds available to the Department of Defense may not be obligated or expended for publicity or propaganda purposes within the United States not otherwise specifically authorized by law.” *Id.*

⁶³ JOINT CHIEFS OF STAFF, JOINT PUB. 3-57, CIVIL-MILITARY OPERATIONS at GL-6 (8 July 2008)(GL is Glossary).

⁶⁴ See JOINT PUB. 3-13, *supra* note 1, at II-8 to II-9.

⁶⁵ For a description of DoD Humanitarian Assistance (HA) programs, see the Office of Humanitarian Assistance, Disaster Relief, and Mine Action (HDM) website, Defense Security Cooperation Agency (last revised 10 Apr. 2013). For more information on HA fiscal constraints, see the Fiscal Law chapter in this Handbook.

⁶⁶ JOINT CHIEFS OF STAFF, JOINT PUB. 3-0, JOINT OPERATIONS at GL-8 (11 Aug. 2011)(GL is Glossary).

DoD as well. JP 3-12 uses Offensive Cyberspace Operations (OCO), Defensive Cyberspace Operations (DCO), and Cyberspace Intelligence, Surveillance, and Reconnaissance (ISR). Unclassified versions of JP 3-12 definitions are listed in Joint Publication 1-02 and in JP 3-12(R).

a. Discussion: In the past decade, cyberspace operations have received significant attention, culminating in promulgation of several new strategies and initiatives.⁶⁷ These documents discuss the growing cyberspace threat, which a former Secretary of Defense warned could collectively result in a “cyber Pearl Harbor,”⁶⁸ and which the Director of National Intelligence recently listed⁶⁹ as the top concern facing the United States. To combat these threats, the United States continues to develop cyberspace capabilities and policies.⁷⁰ This subsection summarizes several authorities applicable to military CO for national security. It does not discuss in detail how the Internet or computing devices work, or the types of threats faced in cyberspace, though both subjects are immensely helpful for those advising on CO.⁷¹ Though no international treaty or domestic statute comprehensively governs U.S. military activities in cyberspace, a number of policy and regulatory documents—both classified and unclassified—provide guidance to legal advisors on applying existing laws to CO.

b. Mission: As part of a whole-of-government approach to cyber security, DoD performs three limited yet critical missions. The 2006 *National Military Strategy for Cyberspace Operations* stated:

US law and national policy assign DOD three main roles: defense of the Nation, national incident response, and critical infrastructure protection. These missions may be performed simultaneously. Although partner departments and agencies have responsibilities to secure portions of cyberspace, only DOD conducts *military operations* to defend cyberspace, the critical infrastructure, the homeland, or other vital US interests.⁷²

c. Strategy: The more recent *2011 DoD Strategy for Operating in Cyberspace* outlined five strategic initiatives to fulfill this mission⁷³:

- Treat cyberspace as an operational domain to organize, train, and equip so that DoD can take full advantage of cyberspace’s potential.
- Employ new defense operating concepts to protect DoD networks and systems.

⁶⁷ See generally THE WHITE HOUSE, NATIONAL STRATEGY TO SECURE CYBERSPACE (Feb. 2003); CHAIRMAN OF THE JOINT CHIEFS OF STAFF, THE NATIONAL MILITARY STRATEGY FOR OPERATING IN CYBERSPACE (U) (Dec. 2006)(Classified Secret, redacted unclassified version publicly released under FOIA [hereinafter NMS-CO]; EXECUTIVE OFFICE OF THE PRESIDENT, THE COMPREHENSIVE NATIONAL CYBERSECURITY INITIATIVE (Mar. 2, 2010)(Classified; unclassified summary publicly released); THE WHITE HOUSE, INTERNATIONAL STRATEGY FOR CYBERSPACE: PROSPERITY, SECURITY AND OPENNESS IN A NETWORKED WORLD (May 2011); U.S. DEP’T OF DEF., STRATEGY FOR OPERATING IN CYBERSPACE (July 2011).

⁶⁸ Secretary of Defense Leon Panetta, *Remarks by Secretary Panetta on Cybersecurity to the Business Executives for National Security*, New York City (Oct. 11, 2012)(discussing the cyber threat and Department of Defense initiatives in response).

⁶⁹ See *Open Hearing: Current and Projected National Security Threats to the United States: Hearing Before the Select Committee on Intelligence, United States Senate*, 113th Cong. (Mar. 12, 2013) (Statement for the Record of James R. Clapper, Director of National Intelligence, Worldwide Threat Assessment of the US Intelligence Community, at 1–3).

⁷⁰ See U.S. GOV’T ACCOUNTABILITY OFFICE, RPT. NO. GAO-11-75, DEFENSE DEPARTMENT CYBER EFFORTS: DO D FACES CHALLENGES IN ITS CYBER ACTIVITIES (July 2011) (detailing the evolution of DoD’s cyberspace efforts [pre-JOINT PUB. 3-12]).

⁷¹ Numerous sources address both systems and vulnerabilities. See, e.g., *id.* (discussing threats and incidents), *The Cybersecurity Partnership Between the Private Sector and Our Government: Protecting Our National and Economic Security: Hearing Before the Committee on Commerce, Science, and Transportation and the Committee on Homeland Security and Governmental Affairs, United States Senate*, 113th Cong. (Mar. 7, 2013) (Statement of Gregory C. Wilshusen, Director Information Security Issues), in U.S. GOV’T ACCOUNTABILITY OFFICE, RPT. NO. GAO-13-462T, CYBERSECURITY: A BETTER DEFINED AND IMPLEMENTED NATIONAL STRATEGY IS NEEDED TO ADDRESS PERSISTENT CHALLENGES (Mar. 7, 2013)(discussing systems and threats); U.S. GOV’T ACCOUNTABILITY OFFICE, RPT. NO. GAO-13-187, CYBERSECURITY: NATIONAL STRATEGY, ROLES, AND RESPONSIBILITIES NEEDED TO BE BETTER DEFINED AND MORE EFFECTIVELY IMPLEMENTED (Feb. 14, 2013)(discussing systems, threats, and strategies).

⁷² NMS-CO, *supra* note 67, at 1 (emphasis added). Though DoD published a second strategy statement in 2011 (see generally U.S. DEP’T OF DEF., STRATEGY FOR OPERATING IN CYBERSPACE, *supra* note 69) the NMS-CO has not formally been rescinded as of this writing. The NMS-CO further states, “DoD will execute the full range of military operations (ROMO) in and through cyberspace to defeat, dissuade, and deter threats against US interests.” *Id.* at 2. The U.S. Cyber Command mission statement is: “USCYBERCOM plans, coordinates, integrates, synchronizes, and conducts activities to: direct the operations and defense of specified [DoD] information networks and; [sic] prepare to, and when directed, conduct full-spectrum military cyberspace operations in order to enable actions in all domains, ensure US/Allied freedom of action in cyberspace and deny the same to our adversaries.” U.S. Dep’t of Def., Cyber Command Fact Sheet (Oct. 13, 2010).

⁷³ See generally U.S. DEP’T OF DEF., STRATEGY FOR OPERATING IN CYBERSPACE, *supra* note 67 (outlining initiatives).

- Partner with other U.S. government departments and agencies and the private sector to enable a whole-of-government cybersecurity strategy.
- Build robust relationships with U.S. allies and international partners to strengthen collective cybersecurity.
- Leverage the nation’s ingenuity through an exceptional cyber workforce and rapid technological innovation.

d. The new *2015 DoD Cyber Strategy* of April 17, 2015 outlined many similar goals:

- Build and maintain ready forces and capabilities to conduct cyberspace operations.
- Defend the DoD information network, secure DoD data, and mitigate risks to DoD missions.
- Be prepared to defend the U.S. homeland and U.S. vital interests from disruptive or destructive cyberattacks of significant consequence.
- Build and maintain viable cyber options and plan to use those options to control conflict escalation and to shape the conflict environment at all stages.
- Build and maintain robust international alliances and partnerships to deter shared threats and increase international security and stability.

e. Legal Position: In addition to the strategies and initiatives discussed above, two unclassified statements of U.S. policy stand out regarding cyberspace: a 2011 DoD report to Congress on cyberspace policy,⁷⁴ and the September 2012 speech⁷⁵ by then-U.S. Department of State Legal Advisor Harold Koh at a U.S. Cyber Command legal conference. Both references make clear that the United States accepts the application of established international law of armed conflict legal authorities to CO, though the precise function of some rules remains to be worked out.

f. Joint Doctrine: Recent joint doctrine rewrites formally separated CO from IO. Joint Pub. 3-13 deletes the term computer network operations (CNO) and its three subcategories of attack (CNA), defense (CND), and exploitation (CNE) from joint doctrine.⁷⁶ This terminology has been superseded by the definitions used in PPD 20 and JP 3-12. The new classified Joint Pub. 3-12, *Cyberspace Operations*, sets forth a comprehensive doctrinal framework for CO.⁷⁷ Unclassified definitions of key terms appear in Joint Pub. 1-02:

- **Cyberspace:** “A global domain within the information environment consisting of the interdependent network of information technology infrastructures and resident data, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers.”⁷⁸
- **Cyberspace superiority:** “The degree of dominance in cyberspace by one force that permits the secure, reliable conduct of operations by that force, and its related land, air, maritime, and space forces at a given time and place without prohibitive interference by an adversary.”⁷⁹
- **Offensive cyberspace operations (OCO):** “Cyberspace operations intended to project power by the application of force in or through cyberspace.”⁸⁰
- **Defensive cyberspace operations (DCO):** “Passive and active cyberspace operations intended to preserve the ability to utilize friendly cyberspace capabilities and protect data, networks, net-centric capabilities, and other designated systems.”⁸¹

⁷⁴ U.S. DEP’T OF DEF., *CYBERSPACE POLICY REPORT: A REPORT TO CONGRESS PURSUANT TO THE NATIONAL DEFENSE AUTHORIZATION ACT FOR FISCAL YEAR 2011, SECTION 934* (Nov. 2011)(answering thirteen questions for Congress on DoD’s cyber policies and legal positions—one of the best quick primers for military legal advisors on cyberspace).

⁷⁵ Harold Hongju Koh, Legal Advisor, U.S. Dep’t of State, *International Law in Cyberspace: Remarks as Prepared for Delivery by Harold Hongju Koh to the USCYBERCOM Inter-Agency Legal Conference Ft. Meade, MD, Sept. 18, 2012*, 54 HARV. INT’L L.J. ONLINE 1 (Dec. 2012)(footnoted version of original remarks, with citations to supporting sources).

⁷⁶ See JOINT PUB. 3-13, *supra* note 1, at GL-3 (deleting terms); see generally JOINT PUB. 3-12, *supra* note 69.

⁷⁷ See generally JOINT CHIEFS OF STAFF, JOINT PUB. 3-12, *CYBERSPACE OPERATIONS* (5 Feb. 2013)(Classified Secret) [hereinafter JOINT PUB. 3-12].

⁷⁸ See JOINT CHIEFS OF STAFF, JOINT PUB. 1-02, *DICTIONARY OF MILITARY AND ASSOCIATED TERMS* at 70 (8 Nov. 2010)(as amended through 15 Apr. 2013) [hereinafter JOINT PUB. 1-02] (*citing* JOINT PUB. 3-12).

⁷⁹ *Id.* at 70 (*citing* JOINT PUB. 3-12). JP 1-02 prefers the adjective ‘cyberspace’ to ‘cyber.’ *Id.* at B-4.

⁸⁰ *Id.* at 204 (*citing* JOINT PUB. 3-12).

- **Defensive cyberspace operation response action (DCO-RA):** Deliberate, authorized defensive measures or activities taken *outside* of the defended network to protect and defend Department of Defense cyberspace capabilities or other designated systems.⁸² (emphasis added)
- **Department of Defense information networks (DODIN):** “The globally interconnected, end-to-end set of information capabilities, and associated processes for collecting, processing, storing, disseminating, and managing information on-demand to warfighters, policy makers, and support personnel, including owned and leased communications and computing systems and services, software (including applications), data, and security.”⁸³
- **Department of Defense information network (DODIN) operations:** “Operations to design, build, configure, secure, operate, maintain, and sustain [DoD] networks to create and preserve information assurance on the [DoD] information networks.”⁸⁴

g. Relation to IO: Joint Pub. 3-13 states—

CO are the employment of cyberspace capabilities where the primary purpose is to achieve objectives in or through cyberspace. Cyberspace capabilities, when in support of IO, deny or manipulate adversary or potential adversary decision making, through targeting an information medium (such as a wireless access point in the physical dimension), the message itself (an encrypted message in the information dimension), or a cyber-persona (an online identity that facilitates communication, decision making, and the influencing of audiences in the cognitive dimension). When employed in support of IO, CO generally focus on the integration of offensive and defensive capabilities exercised in and through cyberspace, in concert with other IRCs, and coordination across multiple lines of operation and lines of effort.⁸⁵

h. Common Legal Issues: U.N. Charter (*jus ad bellum* analysis whether a cyberspace act constitutes a threat or use of force under Article 2(4), or an armed attack under Article 51 that justifies actions in self-defense); Law of Armed Conflict (*jus in bello* compliance with treaties and customary norms governing weapons, tactics, targeting, and protection of civilians and civilian property); Neutrality Law (including both a sovereign nation’s right to remain neutral in armed conflicts and its obligation to prevent use of its territory to stage attacks); Communications Law (requiring, in peacetime, non-interference with certain state infrastructures and broadcasts); Intelligence, Privacy, and Free Speech Laws (primarily domestic, restricting the state’s use of certain methods, targets, or actors to gather information and preserving freedom of expression); Criminal Law (prohibiting certain activities in cyberspace and encouraging state cooperation in prosecuting hackers); and National Security Law (protection of critical infrastructure and assets, including cooperation with other agencies and private entities). Coordination and deconfliction with other domestic authorities governing use of related capabilities is also critical.

i. Proponents: DoD Chief Information Officer (CIO);⁸⁶ U.S. Strategic Command (USSTRATCOM), including its sub-unified command, U.S. Cyber Command (USCYBERCOM, whose Commander is dual-hatted as Director of the National Security Agency) and four component cyber commands: U.S. Army Cyber Command (ARCYBER), U.S. 2d Army; U.S. Fleet Cyber Command, U.S. 10th Fleet; U.S. Marine Corps Force Cyberspace Command (MARFORCYBER); U.S. Air Force Cyber Command (AFCYBER), 24th Air Force; the National Security Agency and Central Security Service (NSA/CSS); and other agencies as appropriate to their particular missions and capabilities.

j. Operational Guidance: No specific annex is currently dedicated to CO, though Annex K, Communication Systems, may discuss aspects of CO.

k. Sources: The recently-codified 10 U.S.C. § 111 note on “Military Activities in Cyberspace” recognizes DoD’s capability to conduct offensive operations in cyberspace, as directed by the President.⁸⁷ It

⁸¹ *Id.* at 76 (citing JOINT PUB. 3-12).

⁸² *Id.* at 75 (citing JOINT PUB. 3-12).

⁸³ *Id.* at 78 (citing JOINT PUB. 3-12). JP 1-02 prefers this term over ‘Global Information Grid.’ *Id.* at B-4.

⁸⁴ *Id.* at 78 (citing JOINT PUB. 3-12).

⁸⁵ JOINT PUB. 3-13, *supra* note 1, at II-9.

⁸⁶ See U.S. DEP’T OF DEF., DIR. 5144.02, DoD CHIEF INFORMATION OFFICER (DoD CIO) (22 Apr. 2013).

⁸⁷ Added by National Defense Authorization Act (NDAA) for Fiscal Year 2012, Pub. L. 12–81, div. A, title IX, § 954 (Dec. 31, 2011) (2012 Supp.), 125 Stat. 1551. The codified note states in full:

requires that CO comply with the same policy and legal authorities applicable to kinetic capabilities, and with the War Powers Resolution. In practice, this requires legal review of both capabilities (analogous to weapons reviews under the law of armed conflict) and training of forces on the appropriate use of those capabilities. In addition to those sources and areas of law cited above, the following authorities also apply to cyberspace: Executive and DoD orders, directives, and instructions on protecting critical functions,⁸⁸ infrastructure,⁸⁹ and networks;⁹⁰ DoD policy memoranda establishing U.S. Cyber Command⁹¹ and governing Interactive Internet Activities;⁹² and other classified directives, orders, and rules of engagement.

1. International Legal Developments: Four developments are important sources for legal advisors to consult to understand the United States and other nations' approaches to cyberspace. First, the United States participates as part of a 15-nation Group of Government Experts, studying existing and potential threats from cyberspace and possible cooperative measures to address them.⁹³ Second, in December 2012, the International Telecommunications Union, of which the United States is a member, recently adopted a new set of International Telecommunications Regulations and five legally nonbinding resolutions.⁹⁴ The United States vigorously opposed these resolutions, in part motivated by differences of opinion on Internet freedom of expression and governance.⁹⁵ Third, in 2013, a group of international legal scholars and practitioners, at the invitation of the North Atlantic Treaty Organization (NATO) Cooperative Cyber Defence Centre of Excellence published their opinions in a manual on the law governing cyber warfare, known as the TALLINN MANUAL.⁹⁶ Finally, the United States regularly submits comments and feedback to the United Nations on information and telecommunications in the area of international security. These submissions provide excellent unclassified insights on how the United States Government views international law in cyberspace.⁹⁷ Legal advisors should continue to monitor these international discussions.

Congress affirms that the Department of Defense has the capability, and upon direction by the President may conduct offensive operations in cyberspace to defend our Nation, Allies and interests, subject to—

(1) the policy principles and legal regimes that the Department follows for kinetic capabilities, including the law of armed conflict; and

(2) the War Powers Resolution (50 U.S.C. 1541 et seq.).

Id.; see also H.R. Rep. No. 112-329 pt. 1, at 686 (Dec. 12, 2011)(Conference Report discussion of § 954's purpose).

⁸⁸ See, e.g., DEP'T OF DEF., INSTR. 5200.44, PROTECTION OF MISSION CRITICAL FUNCTIONS TO ACHIEVE TRUSTED SYSTEMS AND NETWORKS (5 Nov. 2012).

⁸⁹ See, e.g., Federal Information Security Management Act (FISMA), 44 U.S.C. § 3541 et seq. (2006); THE WHITE HOUSE, PRESIDENTIAL POLICY DIRECTIVE [21] -- CRITICAL INFRASTRUCTURE SECURITY AND RESILIENCE (Feb. 12, 2013); EXEC. ORDER, NO. 13,636, FEB. 12, 2013, IMPROVING CRITICAL INFRASTRUCTURE CYBERSECURITY, 78 F.R. 11739 (Feb 19, 2013); DEP'T OF DEF., DIR. 3020.40, DoD POLICIES AND RESPONSIBILITIES FOR CRITICAL INFRASTRUCTURE (14 Jan. 2010) (C2, 21 Sep. 2012); DEP'T OF DEF., INSTR. 3020.45, DEFENSE CRITICAL INFRASTRUCTURE PROGRAM (DCIP) MANAGEMENT (21 Apr. 2008).

⁹⁰ See, e.g., U.S. DEP'T OF DEF., DIR. 8000.01, MANAGEMENT OF THE [DoD] INFORMATION ENTERPRISE (10 Feb. 2009); U.S. DEP'T OF DEF., DIR. O-8530.1, COMPUTER NETWORK DEFENSE (CND) (8 Jan. 2001)(U//FOUO); U.S. DEP'T OF DEF., INSTR. O-8530.2, SUPPORT TO COMPUTER NETWORK DEFENSE (CND) (9 Mar. 2001)(U//FOUO); U.S. DEP'T OF DEF., INSTR. 8410.02, NETOps FOR THE GLOBAL INFORMATION GRID (GIG) (19 Dec. 2008); U.S. DEP'T OF DEF., INSTR. 8410.03, NETWORK MANAGEMENT (NM) (29 Aug. 2012); CHAIRMAN OF THE JOINT CHIEFS OF STAFF, MAN. 6510.01B, CYBER INCIDENT HANDLING PROGRAM (10 July 2010).

⁹¹ See Memorandum from The Secretary of Defense, subject: Establishment of a Subordinate Unified U.S. Cyber Command Under U.S. Strategic Command for Military Cyberspace Operations (23 June 2009).

⁹² Directive-Type Memorandum 08-037, Memorandum from the Deputy Secretary of Defense, subject: Policy for Department of Defense (DoD) Interactive Internet Activities (8 June 2007)(two-way internet communications) [hereinafter DTM 08-037].

⁹³ For a sense of the international dialogue regarding cyberspace, and reports and additional information on the Group, see the United Nations Office for Disarmament Affairs information security website. See also U.N. Secretary-General, *Developments in the Field of Information and Telecommunications in the Context of Information Security, Rep. of the Secretary-General*, 14–21, U.N. Doc A/66/152 (July 15, 2011)(submission of United States of America regarding cyberspace).

⁹⁴ See INT'L. TELECOMM. UNION, FINAL ACTS OF THE WORLD CONFERENCE ON INTERNATIONAL TELECOMMUNICATIONS [WCIT] (DUBAI, 2012) (Dec. 14, 2012)(text of new regulations and resolutions, proposed to replace the existing 1988 regulations).

⁹⁵ See U.S. Dep't of State, Media Note: U.S. Intervention at the [WCIT], Dec. 13, 2012 (text of formal U.S. intervention requested at WCIT); U.S. Dep't of State, Transcript of Remarks by Terry Kramer, Ambassador, U.S. Head of Delegation, on the [WCIT] (via Teleconference from Dubai, United Arab Emirates), Dec. 13, 2012 (further explaining U.S. objections).

⁹⁶ See TALLINN MANUAL ON THE INTERNATIONAL LAW APPLICABLE TO CYBER WARFARE (Michael N. Schmitt gen. ed. 2013) (proposing 95 rules with commentaries). Though not an official publication, and reflecting only the personal opinions of participants (not their respective nations), the Tallinn Manual included both U.S. experts and an observer from USCYBERCOM. See *id.* at x–xiii, 9–10. As of this writing, the United States has neither officially endorsed nor rejected the Manual.

⁹⁷ United States Submission to the UN Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security of October, 9, 2014.

m. U.S. Developments/Issues: PPD 20's arrival in 2012 dramatically changed prior US Policy on operations in cyberspace, and has superseded/replaced many prior authorities on cyberspace operations. Most of the documents implementing PPD 20 to DoD are classified Top SECRET. The next edition of the SROE (publication TBD) will likely account for the changes brought by PPD 20. Numerous classified OPORDs and EXORDs exist in this realm as well that remain US policy. In general, the authority to launch cyber operations outside DoD networks will stem from either: (1) PPD 20, or (2) a Presidentially approved OPORD or EXORD that delegates this authority in certain circumstances or for specific military operations. As stated previously in this chapter, an emerging debate exists on the status of cyberspace operations as "traditional military activities," and the issue of convergence between Title 10 and Title 50. In addition, the lines between cyber effects operations and cyber intelligence have become increasingly blurred in recent years, as many intelligence operations may nonetheless carry cyber effects. Again, the key factor for determining whether LOAC or Intelligence Law applies is to look at the primary purpose of the cyberspace operation. Finally, a debate continues in the cyberspace community over the distinction between cyberspace operations and traditional electronic warfare. Operators often prefer to have their missions characterized as EW, since the authority levels for traditional EW are far lower than for cyberspace operations.

n. Other resources: Numerous additional documents and current news stories can be found on the following, regularly updated unclassified portals on cyber security—the National Security Council (NSC); DoD; the U.S. Department of Homeland Security (DHS); the U.S. Computer Emergency Readiness Team (US-CERT); and the NATO LibGuide on Cyberspace Security. The Tallinn Manual is also a useful source for determining the current status of CIL in this field. Finally, the Harold Koh Speech of September 2012 is an excellent source for looking at United States policy at an UNCLASSIFIED level.

6. **Information Assurance (IA):** "Actions that protect and defend information systems by ensuring availability, integrity, authentication, confidentiality, and nonrepudiation."⁹⁸

a. Discussion: IA ensures the reliability of information on DoD information networks and other means of communication, thereby protecting friendly decision-making. IA is the primary objective of DODIN operations (defined above in para. III.B.5.d) and a core focus of other communications equipment operations. "IA is necessary to gain and maintain information superiority. The [Joint Forces commander] relies on IA to protect infrastructure to ensure its availability, to position information for influence, and for delivery of information to the adversary. Furthermore, IA and CO are interrelated and rely on each other to support IO."⁹⁹

b. Common Legal Issues: Communications Law (compliance with international treaties and agreements, and domestic statutes and regulations regarding operation of communications systems); Intelligence, Privacy, and Free Speech Laws (primarily domestic, restricting the state's ability to gather information and preserving freedom of expression); Criminal Law (prohibiting certain activities in cyberspace and encouraging state cooperation in prosecuting hackers); and National Security Law (protection of critical infrastructure and assets, including cooperation with other agencies and private entities).

c. Proponents: DoD Chief Information Officer (CIO).

d. Operational Guidance: No specific annex is currently dedicated to IA, though Annex K, Communications Systems, may discuss aspects of IA.

e. Sources: 10 U.S.C. § 2224 (2006), the Defense IA Program;¹⁰⁰ U.S. DEP'T OF DEF., DIR. 8000.01, MANAGEMENT OF THE DEPARTMENT OF DEFENSE INFORMATION ENTERPRISE (10 Feb. 2009) (Unclassified); U.S. DEP'T OF DEF., DIR. 8500.01E, INFORMATION ASSURANCE (IA) (24 Oct. 2002) (Unclassified); U.S. DEP'T OF DEF., DIR. O-8530.1, COMPUTER NETWORK DEFENSE (CND) (8 Jan. 2001)(Unclassified//For Official Use Only (FOUO)); U.S. DEP'T OF DEF., INSTR. 8410.02, NETOPS FOR THE GLOBAL INFORMATION GRID (GIG) (19 Dec. 2008) (Unclassified); U.S. DEP'T OF DEF., INSTR. 8500.2, INFORMATION ASSURANCE (IA) IMPLEMENTATION (6 Feb. 2003) (Unclassified); U.S. DEP'T OF DEF., INSTR. 8510.01, DoD INFORMATION ASSURANCE CERTIFICATION AND ACCREDITATION PROCESS (DIACAP) (28 Nov. 2007)(Unclassified); U.S. DEP'T OF DEF., INSTR. 8580.1, INFORMATION ASSURANCE (IA) IN THE DEFENSE ACQUISITION SYSTEM (9 July 2004)(Unclassified); U.S. DEP'T OF DEF., INSTR. 8581.01, INFORMATION ASSURANCE (IA) POLICY FOR SPACE SYSTEMS USED BY [DoD] (8 June 2010)

⁹⁸ See JOINT PUB. 1-02, *supra* note 80, at 135 (*citing* JOINT PUB. 3-12).

⁹⁹ JOINT PUB. 3-13, *supra* note 1, at II-9.

¹⁰⁰ The NDAA for FY13 added two new requirements to be codified as notes to this section. See National Defense Authorization Act for Fiscal Year 2013, Public Law 112-239 §§ 933, 941 (Jan. 2, 2013) 126 Stat. 1632, 1884–85, 1889–90 (tasking DoD to implement a baseline software assurance policy, criteria for cleared defense contractors to report penetration of their networks).

(Unclassified); CHAIRMAN OF THE JOINT CHIEFS OF STAFF, INSTR. 6510.01F, INFORMATION ASSURANCE (IA) AND SUPPORT TO COMPUTER NETWORK DEFENSE (CND) (9 Feb. 2011)(Unclassified); JOINT PUB. 3-12.

7. **Space Operations (Space Ops):** “US space operations are comprised of four mission areas: space force enhancement; space support; space control; and space force application.”¹⁰¹

a. Discussion: Regarding IO, “[s]pace capabilities are a significant force multiplier when integrated with joint operations. Space operations support IO through the space force enhancement functions of intelligence, surveillance, and reconnaissance; missile warning; environmental monitoring; satellite communications; and space-based positioning, navigation, and timing.”¹⁰²

b. Common Legal Issues: Space Law (see Chapter 10 on Sea, Air, and Space Law in this Handbook); may also raise issues similar to CO as discussed above.

c. Proponent: U.S. Strategic Command and its subordinate command, the Joint Functional Component Command for Space.

d. Operational Guidance: Annex N to the OPLAN addresses Space Operations.

e. Sources: U.S. DEP’T OF DEF., DIR. 3100.10, SPACE POLICY (18 Oct. 2012)(Unclassified); U.S. DEP’T OF DEF., DIR. 5101.02E, DOD EXECUTIVE AGENT (EA) FOR SPACE (25 Jan. 2013)(Unclassified); U.S. DEP’T OF DEF., DIR. S-3100.13, SPACE FORCE APPLICATION (14 Sept. 2000)(Classified Secret); U.S. DEP’T OF DEF., DIR. S-3100.14, SPACE FORCE ENHANCEMENT (14 Sept. 2000)(Classified Secret); CHAIRMAN OF THE JOINT CHIEFS OF STAFF (CJCS), JOINT PUB. 3-14, SPACE OPERATIONS (6 Jan. 2009)(Unclassified). *See also* Chapter 10 on Sea, Air, and Space Law of this Handbook.

8. **Military Information Support Operations (MISO):** “Planned operations to convey selected information and indicators to foreign audiences to influence their emotions, motives, objective reasoning, and ultimately the behavior of foreign governments, organizations, groups, and individuals in a manner favorable to the originator’s objectives.”¹⁰³

a. Discussion: MISO, formerly known as psychological operations (PSYOP), “focuses on the cognitive dimension of the information environment where its [target audience] includes not just potential and actual adversaries, but also friendly and neutral populations.”¹⁰⁴ MISO may be conducted across the full spectrum of military operations, “such as stability operations, security cooperation, maritime interdiction, noncombatant evacuation, foreign humanitarian operations, counterdrug, force protection, and counter-trafficking.”¹⁰⁵

b. Common Legal Issues: U.N. Charter (*jus ad bellum* analysis whether an action or message constitutes a threat of force under Article 2(4)); Law of Armed Conflict (*jus in bello* compliance with treaties and customary norms, e.g., rules on treachery and perfidy,¹⁰⁶ as well as prisoner of war and detainee treatment¹⁰⁷);

¹⁰¹ CHAIRMAN OF THE JOINT CHIEFS OF STAFF (CJCS), JOINT PUB. 3-14, SPACE OPERATIONS at ix (6 Jan. 2009).

¹⁰² JOINT PUB. 3-13, *supra* note 1, at II-9.

¹⁰³ JOINT PUB. 3-13, *supra* note 1, at II-9 to II-10.

¹⁰⁴ See Memorandum from The Secretary of Defense, subject: Changing the Term Psychological Operations (PSYOP) to Military Information Support Operations (MISO) (3 Dec. 2010)(describing name change rationale); *Id.* at II-10 (quotation).

¹⁰⁵ *Id.*

¹⁰⁶ Examples of MISO-related conduct violating the prohibitions on treachery and perfidy include advertising a bounty for an enemy’s death, broadcasting to an enemy that an armistice has been agreed upon when such is not the case, feigning surrender to facilitate an attack, or threatening an enemy that no survivors will be taken. *See* CONVENTION RESPECTING THE LAWS AND CUSTOMS OF WAR ON LAND AND ITS ANNEX: REGULATIONS RESPECTING THE LAWS AND CUSTOMS OF WAR ON LAND, arts. 23–24, Oct. 18, 1907, 36 Stat. 2277, 205 Consol. T.S. 277, *entered into force and for the United States* Jan. 26, 1910 (permitting ruses of war but forbidding treacherous conduct or improper use of the Red Cross emblem) [hereinafter Hague IV for the Convention, Hague Regulations for the Annex]; U.S. DEP’T OF ARMY, FIELD MANUAL 27-10, THE LAW OF LAND WARFARE, paras. 48–55, 467 (18 July 1956) (C1, 15 July 1976) (discussing examples of ruses, treachery, and perfidy) [hereinafter FM 27-10]; *see also* AP I, arts. 37–38, 40 (expanding the rules on perfidy, improper use, and threatening an enemy); Matheson, *supra* note 40, at 422–24 (stating the U.S. position on AP I, including that individual combatants shall not kill, injure, or capture enemy personnel by resort to perfidy; internationally recognized protective emblems, e.g., the Red Cross, shall not be improperly used; and no order shall be given to permit no survivors nor may an adversary be threatened with such an order or hostilities conducted on that basis).

¹⁰⁷ The Geneva Conventions and Army Regulation 190-8 forbid publishing photographic images of enemy prisoners of war, or subjecting prisoners of war or others (including detainees or internees) to outrages upon personal dignity, such as humiliating or degrading treatment. *See* CONVENTION RELATIVE TO THE TREATMENT OF PRISONERS OF WAR, arts. 3, 13, Aug. 12, 1949, 6 U.S.T.

Communications Law (international law prohibiting harmful interference with radio broadcasts, and domestic or foreign laws regulating broadcasting); Law of the Sea (restricting pirate radio broadcasts and delineating territorial boundaries); Intelligence, Privacy, and Free Speech Laws (primarily domestic, restricting the state's use of certain methods, targets, or actors to gather information, and preserving freedom of expression); Other U.S. domestic law restrictions (e.g., attribution vs. covert action,¹⁰⁸ copyright and trademark restrictions, and prohibition on propaganda directed at U.S. audiences,¹⁰⁹ State Department public diplomacy mission); and international agreements (e.g., on status of forces) or foreign domestic law, which may place limits on activities of military information support units.

c. Proponents: USD(P) (normally overseen by ASD(SOL/IC)); USSOCOM.¹¹⁰

d. Operational Guidance: Generally contained in Appendix 3 to Annex C of the OPORD or OPLAN. MISO generally proceed according to a specific IO plan. In creating a MISO plan, one must conduct research and analysis of critical information, develop themes and actions, and produce and disseminate the MISO product. In planning the dissemination phase, one must consider the most effective type of MISO product for a particular area; for example, leaflets, radio broadcasts, TV broadcasts, and/or internet-based products may each work better as delivery platforms in certain areas of the world than they would in others. Furthermore, **MISO products must not be directed at domestic (i.e. U.S.) audiences**. Approved trans-regional or theater-specific plans provide guidance and parameters for individual products addressing these requirements. Legal advisors assist both in developing plans and in ensuring products comply therewith.

e. Sources: U.S. DEP'T OF DEF., DIR. S-3321.1, OVERT PSYCHOLOGICAL OPERATIONS CONDUCTED BY THE MILITARY SERVICES IN PEACETIME AND IN CONTINGENCIES SHORT OF DECLARED WAR (U) (26 July 1984) (Classified Secret); Directive-Type Memorandum (DTM) 08-037, Memorandum from the Deputy Secretary of Defense, subject: Policy for Department of Defense (DoD) Interactive Internet Activities (8 June 2007)(two-way internet communications); CHAIRMAN OF THE JOINT CHIEFS OF STAFF, INSTR. 3110.05E, MILITARY INFORMATION SUPPORT OPERATIONS SUPPLEMENT TO THE JOINT STRATEGIC CAPABILITIES PLAN (30 Sep. 2011)(U//FOUO); JOINT CHIEFS OF STAFF, JOINT PUB. 3-13.2, MILITARY INFORMATION SUPPORT OPERATIONS (7 Jan. 2010) (C1, 20 Dec. 2011) (available via JDEIS, access restricted to .mil or .gov network).

9. **Intelligence (Intel)**: “The product resulting from the collection, processing, integration, evaluation, analysis, and interpretation of available information concerning foreign nations, hostile or potentially hostile forces or elements, or areas of actual or potential operations. The term is also applied to the activity which results in the product and to the organizations engaged in such activity.”¹¹¹ JP 2-0, 1-02 139

a. Discussion: “Intelligence is a vital military capability that supports IO. The utilization of information operations intelligence integration (IOII) greatly facilitates understanding the interrelationship between the physical, informational, and cognitive dimensions of the information environment,” and a greater understanding of peoples, cultures, societies, networks, and the flow of information, as well as the predicted and actual reaction of audiences to particular messages.¹¹²

b. Common Legal Issues: The rules governing intelligence operations are extremely complex and require careful study. In particular, intelligence laws and regulations may limit the use of certain sources or methods

3316, T.I.A.S. 3364, 75 U.N.T.S. 135, *entered into force* Oct. 21, 1950, *for the United States* Feb. 2, 1956 (forbidding outrages upon personal dignity, including humiliation or degrading treatment; protecting prisoners of war against insults and public curiosity; art. 3 is common to all four Geneva Conventions); AP I, *supra* note 37, art. 75 (similar protection for civilian detainees); U.S. DEP'T OF ARMY, REG. 190-8, ENEMY PRISONERS OF WAR, RETAINED PERSONNEL, CIVILIAN INTERNEES AND OTHER DETAINEES, paras. 1.5.d., 1.9 (1 Oct. 1997)(restricting photographing, filming, and video taping of such persons).

¹⁰⁸ See 50 U.S.C. § 413b (2006)(defining covert action as “activity or activities of the [USG] to influence political, economic, or military conditions abroad, where it is intended that the role of the [USG] will not be apparent or acknowledged publicly”, and requiring Presidential approval for such actions, unless one of four exceptions applies, including “traditional . . . military activities [TMA] or routine support to such activities”). Legal advisors should consult operational guidance governing attribution, and ensure MISO (arguably TMA) are military operations, distinct from U.S. State Department public diplomacy efforts.

¹⁰⁹ Previously, U.S. military forces observed this restriction by policy, motivated by a statute applicable to the U.S. State Department public diplomacy mission (22 U.S.C § 1461-1a, part of the Smith-Mundt Act). A new statute directed at DoD, recently codified at 10 U.S.C. 2241a (2010 Supp.), directs: “Funds available to the [DoD] may not be obligated or expended for publicity or propaganda purposes within the United States not otherwise specifically authorized by law.”

¹¹⁰ See SECDEF 25 Jan 11 Memo, *supra* note 2, at 2.

¹¹¹ JOINT PUB. 2-0, JOINT INTELLIGENCE, at GL-11 (22 June 2007)(GL refers to Glossary).

¹¹² See JOINT PUB. 3-13, *supra* note 1, at II-10.

for analysis or dissemination of IO products. For example, DoDD 3600.01, para. 1 now requires that “DoD IO information gathering programs and activities . . . coordinated and deconflicted with DoD intelligence activities as set forth in DoD Directive S-5200.37 . . . and DoD 5240.1-R” and that human-derived information gathering activities in support of IO “remain separate from authorized HUMINT and related intelligence activities.” For an overview of intelligence law, and notably the restrictions on collections on U.S. persons by members of the Intelligence Community, see Chapter 6 of this Handbook.

c. Proponents: Undersecretary of Defense for Intelligence (USD(I)); various organizations in the Intelligence Community as detailed in Executive Order 12,333.

d. Operational Guidance: Annex B to the OPLAN addresses Intelligence.

e. Sources: OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE, INTELLIGENCE COMMUNITY LEGAL REFERENCE BOOK (2012) (listing numerous statutes, orders, and other resources); Chapter 6, Intelligence Law and Interrogation Operations, of this Handbook (listing several military-specific sources).

10. **Military Deception (MILDEC):** “Actions executed to deliberately mislead adversary military, paramilitary, or violent extremist organization decision makers, thereby causing the adversary to take specific actions (or inactions) that will contribute to the accomplishment of the friendly mission.”¹¹³

a. Discussion: “One of the oldest IRCs used to influence an adversary’s perceptions is MILDEC.” Military Deception operations have been used throughout history. Famous examples include the Trojan Horse and World War II efforts to divert attention from Normandy for the D-Day invasion. The focus of MILDEC is desired behavior—not merely to mislead, but to cause adversaries or potential adversaries “to behave in a manner advantageous to the friendly mission, such as misallocation of resources, attacking at a time and place advantageous to friendly forces, or avoid taking action at all.” In several ways, MILDEC differs from other IRCs, and is controlled on a strict need-to-know basis due to the sensitive nature of its plans, goals, and objectives.¹¹⁴

b. Means and Techniques: There are three means by which a force may conduct MILDEC: physical (i.e. dummy and decoy equipment), technical (i.e. the emission of biological or chemical odors or nuclear particles), and administrative (i.e. the conveyance or denial of oral, pictorial, documentary, or other physical evidence). There are four different deception techniques a force may employ: feints (offensive actions to deceive the enemy about actual offensive actions), demonstrations (a show of force to cause the enemy to select an unfavorable course of action), ruses (cunning tricks to deceive the enemy for a friendly advantage), and displays (the simulation, disguising, and/or portrayal of friendly objects, units, or capabilities).

c. Common Legal Issues: U.N. Charter (*jus ad bellum* analysis whether actions constitute a threat or use of force under Article 2(4), or an armed attack under Article 51 that justifies actions in self-defense); Law of Armed Conflict (*jus in bello* compliance with treaties and customary norms, particularly those governing ruses and perfidy and protection of civilians and civilian property);¹¹⁵ Neutrality Law (including both a sovereign nation’s right to remain neutral in armed conflicts and its obligation to prevent use of its territory to stage attacks); Communications Law (requiring, in peacetime, non-interference with certain state infrastructures and broadcasts); Intelligence, Privacy, and Free Speech Laws (primarily domestic, restricting the state’s use of certain methods, targets, or actors to gather information and preserving freedom of expression). For purposes of 50 U.S.C. § 413b,

¹¹³ JOINT PUB. 1-02, *supra* note 80, at 179 (citing JOINT CHIEFS OF STAFF, JOINT PUB. 3-13.4, MILITARY DECEPTION (26 Jan. 2012))

¹¹⁴ See JOINT PUB. 3-13, *supra* note 1, at II-10 to II-12.

¹¹⁵ Per JOINT PUB. 3-13.4, “Certain deception techniques may amount to ‘perfidious acts’ due to their treacherous nature. Perfidious acts are prohibited under the law of armed conflict (LOAC) because they undermine the effectiveness of the law of war and thereby jeopardize the safety of civilians and noncombatants and/or the immunity of protected structures and activities. Acts of perfidy are deceptions designed to invite the confidence of the enemy to lead him to believe that he is entitled to, or is obliged to accord, protected status under the LOAC, with the intent to betray that confidence. Under this deception technique, the deceiving unit intends to use the enemy’s compliance with the law of war to gain an advantage with respect to the enemy. Acts of perfidy include, but are not limited to, feigning surrender or waving a white flag in order to lure the enemy into a trap; misuse of protective signs, signals, and symbols in order to injure, kill, or capture the enemy; and using an ambulance or medical aircraft marked with the Red Cross, Red Crescent, or Red Crystal to carry armed combatants, weapons, or ammunition in order to attack or elude enemy forces.” The United States does not support the prohibition on the use of enemy emblems and uniforms during military operations contained in AP I, Article 39. See Matheson, *supra* note 40, at 422–24. However, U.S. forces do not kill, wound, or capture the enemy while wearing such uniforms or emblems, and must remove enemy markings from enemy weapons before using them in combat. U.S. forces also must apply the principles of necessity, distinction, proportionality, and unnecessary suffering to MILDEC activities, including the obligation to take steps to minimize civilian death, injury, or property damage.

military deception techniques constitute a traditional military activity. Military Deception actions cannot *intentionally* target or mislead the U.S. public, Congress, or the U.S. media.

- d. Proponents: USD(P), Joint Staff.¹¹⁶
- e. Operational Guidance: Generally contained in Appendix 3 to Annex C of the OPORD or OPLAN.
- f. Sources: U.S. DEP'T OF DEF., INSTR. S-3604.1, (U) [DOD] MILITARY DECEPTION (11 Mar. 2013) (Classified Secret); CHAIRMAN OF THE JOINT CHIEFS OF STAFF, INSTR. 3211.01E, JOINT POLICY FOR MILITARY DECEPTION (U) (25 Oct. 2010)(Classified Secret); JOINT CHIEFS OF STAFF, JOINT PUB. 3-13.4, MILITARY DECEPTION (26 Jan. 2012) (available via JDEIS, access restricted to .mil or .gov network)

11. **Operations Security (OPSEC):** “A process of identifying critical information and subsequently analyzing friendly actions attendant to military operations and other activities.”¹¹⁷

a. Discussion: OPSEC facilitates IO’s mission to ‘protect our own’ information and decision-making. “OPSEC is a standardized process designed to meet operational needs by mitigating risks associated with specific vulnerabilities in order to deny adversaries critical information and observable indicators. OPSEC identifies critical information and actions attendant to friendly military operations to deny observables to adversary intelligence systems.” Beyond information, the OPSEC process also serves to protect personnel and physical assets. Other IRCs and non-IO communities frequently satisfy OPSEC requirements to mitigate vulnerabilities.¹¹⁸

b. Common Legal Issues: Securing critical infrastructure (see discussion of IA, para. III.B.6 above); Freedom of Information Act (FOIA); Unauthorized disclosures of information. “OPSEC practices must balance the responsibility to account to the American public with the need to protect critical information. The need to practice OPSEC should not be used as an excuse to deny noncritical information to the public.”¹¹⁹

- c. Proponents: USD(P); Joint Staff. OPSEC is also an obligation at all levels of command.
- d. Operational Guidance: May be contained in Appendix 3 to Annex C of the OPORD or OPLAN, though other sections or annexes of the OPLAN may also discuss OPSEC.
- e. Sources: U.S. DEP'T OF DEF., DIR. 5205.02E, DoD OPERATIONS SECURITY (OPSEC) PROGRAM (20 June 2012); U.S. DEP'T OF DEF., MAN. 5205.02-M, DoD OPERATIONS SECURITY (OPSEC) PROGRAM MANUAL (3 Nov 2008); JOINT CHIEFS OF STAFF, JOINT PUB. 3-13.3, OPERATIONS SECURITY (4 Jan. 2012).

12. **Special Technical Operations (STO):** Specialized operations utilizing classified technical tactics, techniques, and procedures.

a. Discussion: “IO need to be deconflicted and synchronized with STO. Detailed information related to STO and its contribution to IO can be obtained from the STO planners at [Combatant Command] or Service component headquarters. IO and STO are separate, but have potential crossover . . .” so coordination is critical.¹²⁰

- b. Common Legal Issues, Proponents, and Sources: Various.
- c. Operational Guidance: Annex S to the OPLAN addresses Special Technical Operations.

13. **Joint Electromagnetic Spectrum Operations (JEMSO):** “Those activities consisting of electronic warfare [EW] and joint electromagnetic spectrum management operations [JEMSMO] used to exploit, attack, protect, and manage the electromagnetic operational environment to achieve the commander’s objectives.”¹²¹

a. Discussion: “All information-related mission areas increasingly depend on the electromagnetic spectrum (EMS). JEMSO, consisting of EW and joint EMS management operations, enable EMS-dependent systems to function in their intended operational environment. EW is the mission area ultimately responsible for securing and maintaining freedom of action in the EMS for friendly forces while exploiting or denying it to

¹¹⁶ See SECDEF 25 Jan 11 Memo, *supra* note 2, at 2.

¹¹⁷ JOINT PUB. 1-02, *supra* note 78, at 179 (citing JOINT CHIEFS OF STAFF, JOINT PUB. 3-13.4, OPERATIONS SECURITY (4 Jan. 2012))

¹¹⁸ See JOINT PUB. 3-13, *supra* note 1, at II-12.

¹¹⁹ *Id.*

¹²⁰ *Id.*

¹²¹ JOINT CHIEFS OF STAFF, JOINT PUB. 6-01, JOINT ELECTROMAGNETIC SPECTRUM MANAGEMENT OPERATIONS (JEMSO), at GL-5 (20 Mar. 2012);

adversaries. JEMSO therefore supports IO by enabling successful mission area operations.”¹²² EW may utilize technologies such as jamming equipment that have an effect in the physical domain, and JEMSMO must consider international, foreign, and domestic rules allocating and protecting frequencies in the EMS.

b. **Electronic Warfare:** EW refers to any military action involving the use of electromagnetic (EM) and directed energy to control the EM spectrum or to attack the adversary. It includes three major subdivisions: Electronic Attack (EA), Electronic Protection (EP), and Electronic Warfare Support (ES). EW contributes to the success of IO by using offensive and defensive tactics and techniques in a variety of combinations to shape, disrupt, and exploit adversarial use of the EM spectrum while protecting friendly freedom of action in that spectrum.¹²³

- **Electronic Attack (EA):** The use of EM energy, directed energy, or anti-radiation weapons to attack personnel, facilities, or equipment with the intent of degrading, neutralizing, or destroying adversary combat capability. It is considered a form of fires.
- **Electronic Protection (EP):** Actions taken to protect personnel, facilities, and equipment from any effects of friendly or enemy use of EM spectrum that degrade, neutralize, or destroy friendly combat capability.
- **Electronic Warfare Support (EWS):** Actions tasked by, or under direct control of, an operational commander to search for, intercept, identify, and locate or localize sources of intentional and unintentional radiated EM energy for the purpose of immediate threat recognition, targeting, planning, and conduct of future operations.

c. **Common Legal Issues:** Particularly for EW, U.N. Charter (*jus ad bellum* analysis whether act constitutes a threat or use of force under Article 2(4), or an armed attack under Article 51 that justifies actions in self-defense); Law of Armed Conflict (*jus in bello* compliance with treaties and customary norms governing weapons, tactics, targeting, and protection of civilians and civilian property); Neutrality Law (including both a sovereign nation’s right to remain neutral in armed conflicts and its obligation to prevent use of its territory to stage attacks). For all aspects of JEMSO, Communications Law (international, foreign, and domestic, regulating the EMS and requiring, in peacetime, no harmful interference with certain state infrastructures and broadcasts); Law of the Sea (delineating territorial boundaries); Free Speech Laws (primarily domestic, preserving freedom of expression); Criminal Law (primarily domestic or foreign, prohibiting certain interferences with broadcasts); and National Security Law (attribution vs. covert action, discussed earlier). Due to the continued expansion of wireless networking and the integration of computers and radio frequency communications, there will be operations and capabilities that blur the line between CO and EW and that may require case-by-case determination when EW and CO are assigned separate release authorities.

d. **Proponents:** USD(P) [IO]; USD for Acquisition, Technology, and Logistics (AT&L) [JEMSO]; USSTRATCOM.

e. **Operational Guidance:** Generally contained in Appendix 3 to Annex C of the OPORD or OPLAN.

f. **Sources:** U.S. DEP’T OF DEF., DIR. 3600.01, INFORMATION OPERATIONS (IO) (2 May 2013); U.S. DEP’T OF DEF., DIR. 3222.4, ELECTRONIC WARFARE (EW) AND COMMAND AND CONTROL WARFARE (C2W) COUNTERMEASURES (31 July 1992) (C1, 28 Jan. 1994); CHAIRMAN OF THE JOINT CHIEFS OF STAFF, INSTR. 3210.04A, JOINT ELECTRONIC WARFARE REPROGRAMMING POLICY (U) (10 Feb. 2011)(Classified Secret); CHAIRMAN OF THE JOINT CHIEFS OF STAFF, INSTR. 3210.04A, JOINT ELECTRONIC WARFARE REPROGRAMMING POLICY (U) (10 Feb. 2011)(Classified Secret); CHAIRMAN OF THE JOINT CHIEFS OF STAFF, MAN. 3212.02C, PERFORMING ELECTRONIC ATTACK IN THE UNITED STATES AND CANADA FOR TESTS, TRAINING, AND EXERCISES (U) (20 Mar. 2011)(U//FOUO); CHAIRMAN OF THE JOINT CHIEFS OF STAFF, MAN. 3320.04, ELECTRONIC WARFARE IN SUPPORT OF JOINT ELECTROMAGNETIC SPECTRUM OPERATIONS (U) (10 Feb. 2011)(Classified Secret); JOINT CHIEFS OF STAFF, JOINT PUB. 3-13.1, ELECTRONIC WARFARE (8 Feb. 2012)(available via JDEIS, access restricted to .mil or .gov network).

14. **Key Leader Engagement (KLE):** “KLEs are deliberate, planned engagements between US military leaders and the leaders of foreign audiences that have defined objectives, such as a change in policy or supporting the JFC’s objectives.”¹²⁴

¹²² JOINT PUB. 3-13, *supra* note 1, at II-12.

¹²³ *See generally* JOINT CHIEFS OF STAFF, JOINT PUB. 3-13.1, ELECTRONIC WARFARE (8 Feb. 2012)(discussing EW and its three sub-divisions in greater detail).

¹²⁴ *Id.* at II-13.

a. Discussion: “These engagements can be used to shape and influence foreign leaders at the strategic, operational, and tactical levels, and may also be directed toward specific groups such as religious leaders, academic leaders, and tribal leaders; e.g., to solidify trust and confidence in US forces. KLEs may be applicable to a wide range of operations such as stability operations, counterinsurgency operations, noncombatant evacuation operations, security cooperation activities, and humanitarian operations.”

b. Common Legal Issues: Vary according to the engagement. Watch for overpromising or making promises that cannot legally, ethically, or fiscally be fulfilled; or accidentally concluding international agreements without authorization. Consult the relevant chapters in this Handbook on these subjects. Regarding IO specifically, U.S. forces must observe the U.N. Charter and Law of Armed Conflict obligations, including those regarding threats, ruses, and perfidy.

c. Proponents: Vary according to the engagement.

d. Operational Guidance: No specific annex is currently dedicated to key leader engagements.

e. Sources: Vary according to the engagement. KLE is a relatively new doctrinal term, though the concept is as old as warfare. Admiral Mullen’s admonishment to align messages with actions is apropos. Legal advisors must ensure that commanders know the legal limitations for issues likely to arise in a KLE.¹²⁵

¹²⁵ See WINGFIELD, *supra* note 21, at 4.