XVI – Cyber Operations

Chapter Contents

16.1 INTRODUCTION

This Chapter addresses the law of war and cyber operations. It addresses how law of war principles and rules apply to relatively novel cyber capabilities and the cyber domain.

As a matter of U.S. policy, the United States has sought to work internationally to clarify how existing international law and norms, including law of war principles, apply to cyber operations.[1]

Precisely how the law of war applies to cyber operations is not well-settled, and aspects of the law in this area are likely to continue to develop, especially as new cyber capabilities are developed and States determine their views in response to such developments.[2]

---

[1] *See, e.g.*, *United States Submission to the U.N. Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (2014–15)*, 1 ("But the challenge is not whether existing international law applies to State behavior in cyberspace. As the 2012–13 GGE affirmed, international law does apply, and such law is essential to regulating State conduct in this domain. The challenge is providing decision-makers with considerations that may be taken into account when determining how existing international law applies to cyber activities. Despite this challenge, history has shown that States, through consultation and cooperation, have repeatedly and successfully applied existing bodies of law to new technologies. It continues to be the U.S. view that all States will benefit from a stable international ICT [information and communication technologies] environment in which existing international law is the foundation for responsible State behavior in cyberspace."); Barack Obama, *International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World*, 9 (May 2011) ("The development of norms for state conduct in cyberspace does not require a reinvention of customary international law, nor does it render existing international norms obsolete. Long-standing international norms guiding state behavior—in times of peace and conflict—also apply in cyberspace. Nonetheless, unique attributes of networked technology require additional work to clarify how these norms apply and what additional understandings might be necessary to supplement them. We will continue to work internationally to forge consensus regarding how norms of behavior apply to cyberspace, with the understanding that an important first step in such efforts is applying the broad expectations of peaceful and just interstate conduct to cyberspace."); DEPARTMENT OF DEFENSE, *Department of Defense Cyberspace Policy Report: A Report to Congress Pursuant to the National Defense Authorization Act for Fiscal Year 2011, Section 934*, 7-8 (Nov. 2011) ("The United States is actively engaged in the continuing development of norms of responsible state behavior in cyberspace, making clear that as a matter of U.S. policy, long-standing international norms guiding state behavior also apply equally in cyberspace. Among these, applying the tenets of the law of armed conflict are critical to this vision, although cyberspace's unique aspects may require clarifications in certain areas.").

[2] Department of Defense, Office of the General Counsel, *An Assessment of International Legal Issues in Information Operations* (2nd ed., Nov. 1999), *reprinted in* 76 U.S. NAVAL WAR COLLEGE INTERNATIONAL LAW STUDIES 459,

16.1.1 Cyberspace as a Domain. As a doctrinal matter, DoD has recognized cyberspace as an operational domain in which the armed forces must be able to defend and operate, just like the land, sea, air, and space domains.[3]

Cyberspace may be defined as "[a] global domain within the information environment consisting of interdependent networks of information technology infrastructures and resident data, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers."[4]

16.1.2 Description of Cyber Operations. Cyberspace operations may be understood to be those operations that involve "[t]he employment of cyberspace capabilities where the primary purpose is to achieve objectives in or through cyberspace."[5] Cyber operations: (1) use cyber capabilities, such as computers, software tools, or networks; and (2) have a primary purpose of achieving objectives or effects in or through cyberspace.

16.1.2.1 *Examples of Cyber Operations*. Cyber operations include those operations that use computers to disrupt, deny, degrade, or destroy information resident in computers and computer networks, or the computers and networks themselves. Cyber operations can be a form of advance force operations, which precede the main effort in an objective area in order to prepare the objective for the main assault. For example, cyber operations may include reconnaissance (*e.g.*, mapping a network), seizure of supporting positions (*e.g.*, securing access to key network systems or nodes), and pre-emplacement of capabilities or weapons (*e.g.*, implanting cyber access tools or malicious code). In addition, cyber operations may be a method of acquiring foreign intelligence unrelated to specific military objectives, such as understanding

---

464-65 (2002) ("The international community ordinarily does not negotiate treaties to deal with problems until their consequences have begun to be felt. This is not all bad, since the solution can be tailored to the actual problems that have occurred, rather than to a range of hypothetical possibilities. One consequence, however, is that the resulting law, whether domestic or international, may be sharply influenced by the nature of the events that precipitate legal developments, together with all their attendant policy and political considerations. … Similarly, we can make some educated guesses as to how the international legal system will respond to information operations, but the direction that response actually ends up taking may depend a great deal on the nature of the events that draw the nations' attention to the issue. If information operations techniques are seen as just another new technology that does not greatly threaten the nations' interests, no dramatic legal developments may occur. If they are seen as a revolutionary threat to the security of nations and the welfare of their citizens, it will be much more likely that efforts will be made to restrict or prohibit information operations by legal means. These are considerations that national leaders should understand in making decisions on using information operations techniques in the current formative period, but it should also be understood that the course of future events is often beyond the control of statesmen.").

[3] William J. Lynn III, Deputy Secretary of Defense, *Defending a New Domain: The Pentagon's Cyberstrategy*, 89 FOREIGN AFFAIRS 97, 101 (Sept./Oct. 2010) ("As a doctrinal matter, the Pentagon has formally recognized cyberspace as a new domain of warfare. Although cyberspace is a man-made domain, it has become just as critical to military operations as land, sea, air, and space. As such, the military must be able to defend and operate within it.").

[4] JOINT PUBLICATION 3-12, *Cyberspace Operations,* GL-4 (Feb. 5, 2013) ("(U) Cyberspace. A global domain within the information environment consisting of interdependent networks of information technology infrastructures and resident data, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers.").

[5] JOINT PUBLICATION 3-0, *Joint Operations* (Aug. 11, 2011) ("cyberspace operations. The employment of cyberspace capabilities where the primary purpose is to achieve objectives in or through cyberspace.").

technological developments or gaining information about an adversary's military capabilities and intent.

16.1.2.2 *Examples of Operations That Would Not Be Regarded as Cyber Operations*. Cyber operations generally would not include activities that merely use computers or cyberspace without a primary purpose of achieving objectives or effects in or through cyberspace. For example, operations that use computer networks to facilitate command and control, operations that use air traffic control systems, and operations to distribute information broadly using computers would generally not be considered cyber operations.

Operations that target an adversary's cyberspace capabilities, but that are not achieved in or through cyberspace, would not be considered cyber operations. For example, the bombardment of a network hub, or the jamming of wireless communications, would not be considered cyber operations, even though they may achieve military objectives in cyberspace.

16.1.3 Cyber Operations – Notes on Terminology. DoD doctrine and terminology for cyber operations continue to develop.

16.1.3.1 *"Cyber" Versus "Cyberspace" as an Adjective*. The terms "cyber" and "cyberspace" when used as an adjective (*e.g.*, cyber attack, cyber defense, cyber operation) are generally used interchangeably.

16.1.3.2 *Cyber Attacks or Computer Network Attacks*. The term "attack" often has been used in a colloquial sense in discussing cyber operations to refer to many different types of hostile or malicious cyber activities, such as the defacement of websites, network intrusions, the theft of private information, or the disruption of the provision of internet services.

Operations described as "cyber attacks" or "computer network attacks," therefore, are not necessarily "attacks" for the purposes of applying rules on conducting attacks during the conduct of hostilities.[6] Similarly, operations described as "cyber attacks" or "computer network attacks" are not necessarily "armed attacks" for the purposes of triggering a State's inherent right of self-defense under *jus ad bellum*.[7]

16.2 Application of the Law of War to Cyber Operations

Specific law of war rules may apply to cyber operations, even though those rules were developed before cyber operations were possible. When no more specific law of war rule or other applicable rule applies, law of war principles provide a general guide for conduct during cyber operations in armed conflict.

16.2.1 Application of Specific Law of War Rules to Cyber Operations. Specific law of war rules may be applicable to cyber operations, even though these rules were developed long before cyber operations were possible.

---

[6] *Refer to* § 16.5.1 (Cyber Operations That Constitute "Attacks" for the Purpose of Applying Rules on Conducting Attacks).

[7] *Refer to* § 16.3.3 (Responding to Hostile or Malicious Cyber Operations).

The law of war affirmatively anticipates technological innovation and contemplates that its existing rules will apply to such innovation, including cyber operations.[8] Law of war rules may apply to new technologies because the rules often are not framed in terms of specific technological means. For example, the rules on conducting attacks do not depend on what type of weapon is used to conduct the attack. Thus, cyber operations may be subject to a variety of law of war rules depending on the rule and the nature of the cyber operation. For example, if the physical consequences of a cyber attack constitute the kind of physical damage that would be caused by dropping a bomb or firing a missile, that cyber attack would equally be subject to the same rules that apply to attacks using bombs or missiles.[9]

Cyber operations may pose challenging legal questions because of the variety of effects they can produce. For example, cyber operations could be a non-forcible means or method of conducting hostilities (such as information gathering), and would be regulated as such under rules applicable to non-forcible means and methods of warfare.[10] Other cyber operations could be used to create effects that amount to an attack and would be regulated under the rules on conducting attacks.[11] Moreover, another set of challenging issues may arise when considering whether a particular cyber operation might be regarded as a seizure or destruction of enemy property and should be assessed as such.[12]

16.2.2 Application of Law of War Principles as a General Guide to Cyber Operations. When no specific rule applies, the principles of the law of war form the general guide for conduct during war, including conduct during cyber operations.[13] For example, under the principle of humanity, suffering, injury, or destruction unnecessary to accomplish a legitimate military purpose must be avoided in cyber operations.[14]

---

[8] Harold Hongju Koh, Legal Adviser, Department of State, *International Law in Cyberspace: Remarks as Prepared for Delivery to the USCYBERCOM Inter-Agency Legal Conference (Sept. 18, 2012)*, *reprinted in* 54 HARVARD INTERNATIONAL LAW JOURNAL ONLINE, 3 (Dec. 2012) ("**Cyberspace is not a 'law-free' zone where anyone can conduct hostile activities without rules or restraint.** Think of it this way. This is not the first time that technology has changed and that international law has been asked to deal with those changes. In particular, because the tools of conflict are constantly evolving, one relevant body of law—international humanitarian law, or the law of armed conflict—affirmatively anticipates technological innovation, and contemplates that its existing rules will apply to such innovation.").

[9] Harold Hongju Koh, Legal Adviser, Department of State, *International Law in Cyberspace: Remarks as Prepared for Delivery to the USCYBERCOM Inter-Agency Legal Conference (Sept. 18, 2012)*, *reprinted in* 54 HARVARD INTERNATIONAL LAW JOURNAL ONLINE, 3-4 (Dec. 2012) ("In analyzing whether a cyber operation would constitute a use of force, most commentators focus on whether the direct physical injury and property damage resulting from the cyber event looks like that which would be considered a use of force if produced by kinetic weapons. For example, cyber activities that proximately result in death, injury, or significant destruction would likely be viewed as a use of force. … Only a moment's reflection makes you realize that this is common sense: if the physical consequences of a cyber attack work the kind of physical damage that dropping a bomb or firing a missile would, that cyber attack should equally be considered a use of force.").

[10] *Refer to* § 5.26 (Non-Forcible Means and Methods of Warfare).

[11] *Refer to* § 5.5 (Rules on Conducting Assaults, Bombardments, and Other Attacks).

[12] *Refer to* § 5.17 (Seizure and Destruction of Enemy Property).

[13] *Refer to* § 2.1.2.2 (Law of War Principles as a General Guide).

[14] *Refer to* § 2.3 (Humanity).

Certain cyber operations may not have a clear kinetic parallel in terms of their capabilities and the effects they create.[15] Such operations may have implications that are quite different from those presented by attacks using traditional weapons, and those different implications may well yield different conclusions.[16]

16.3 CYBER OPERATIONS AND *JUS AD BELLUM*

Cyber operations may present issues under the law of war governing the resort to force (*i.e.*, *jus ad bellum*).[17]

16.3.1 Prohibition on Cyber Operations That Constitute Illegal Uses of Force Under Article 2(4) of the Charter of the United Nations. Article 2(4) of the Charter of the United Nations states that "[a]ll Members shall refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any state, or in any other manner inconsistent with the Purposes of the United Nations."[18]

Cyber operations may in certain circumstances constitute uses of force within the meaning of Article 2(4) of the Charter of the United Nations and customary international law.[19] For example, if cyber operations cause effects that, if caused by traditional physical means, would be regarded as a use of force under *jus ad bellum*, then such cyber operations would likely also be regarded as a use of force. Such operations may include cyber operations that: (1) trigger a nuclear plant meltdown; (2) open a dam above a populated area, causing destruction; or (3) disable air traffic control services, resulting in airplane crashes.[20] Similarly, cyber operations

---

[15] Harold Hongju Koh, Legal Adviser, Department of State, *International Law in Cyberspace: Remarks as Prepared for Delivery to the USCYBERCOM Inter-Agency Legal Conference (Sept. 18, 2012)*, *reprinted in* 54 HARVARD INTERNATIONAL LAW JOURNAL ONLINE, 7 (Dec. 2012) ("I have also noted some clear-cut cases where the physical effects of a hostile cyber action would be comparable to what a kinetic action could achieve: for example, a bomb might break a dam and flood a civilian population, but insertion of a line of malicious code from a distant computer might just as easily achieve that same result. As you all know, however, there are other types of cyber actions that do not have a clear kinetic parallel, which raise profound questions about exactly what we mean by 'force.'").

[16] Department of Defense, Office of the General Counsel, *An Assessment of International Legal Issues in Information Operations* (2nd ed., Nov. 1999), *reprinted in* 76 U.S. NAVAL WAR COLLEGE INTERNATIONAL LAW STUDIES 459, 490 (2002) ("In the process of reasoning by analogy to the law applicable to traditional weapons, it must always be kept in mind that computer network attacks are likely to present implications that are quite different from the implications presented by attacks with traditional weapons. These different implications may well yield different conclusions.").

[17] *Refer to* § 1.11 (*Jus ad Bellum*).

[18] U.N. CHARTER art. 2(4).

[19] Harold Hongju Koh, Legal Adviser, Department of State, *International Law in Cyberspace: Remarks as Prepared for Delivery to the USCYBERCOM Inter-Agency Legal Conference (Sept. 18, 2012)*, *reprinted in* 54 HARVARD INTERNATIONAL LAW JOURNAL ONLINE, 3 (Dec. 2012) ("Cyber activities may in certain circumstances constitute uses of force within the meaning of Article 2(4) of the UN Charter and customary international law.").

[20] Harold Hongju Koh, Legal Adviser, Department of State, *International Law in Cyberspace: Remarks as Prepared for Delivery to the USCYBERCOM Inter-Agency Legal Conference (Sept. 18, 2012)*, *reprinted in* 54 HARVARD INTERNATIONAL LAW JOURNAL ONLINE, 4 (Dec. 2012) ("Commonly cited examples of cyber activity that

that cripple a military's logistics systems, and thus its ability to conduct and sustain military operations, might also be considered a use of force under *jus ad bellum*.[21] Other factors, besides the effects of the cyber operation, may also be relevant to whether the cyber operation constitutes a use of force under *jus ad bellum*.[22]

Cyber operations that constitute uses of force within the meaning of Article 2(4) of the Charter of the United Nations and customary international law must have a proper legal basis in order not to violate *jus ad bellum* prohibitions on the resort to force.[23]

16.3.2 Peacetime Intelligence and Counterintelligence Activities. International law and long-standing international norms are applicable to State behavior in cyberspace,[24] and the question of the legality of peacetime intelligence and counterintelligence activities must be considered on a case-by-case basis. Generally, to the extent that cyber operations resemble traditional intelligence and counter-intelligence activities, such as unauthorized intrusions into computer networks solely to acquire information, then such cyber operations would likely be treated similarly under international law.[25] The United States conducts such activities via cyberspace, and such operations are governed by long-standing and well-established considerations, including the possibility that those operations could be interpreted as a hostile act.[26]

16.3.3 Responding to Hostile or Malicious Cyber Operations. A State's inherent right of self-defense, recognized in Article 51 of the Charter of the United Nations, may be triggered by

---

would constitute a use of force include, for example, (1) operations that trigger a nuclear plant meltdown, (2) operations that open a dam above a populated area causing destruction, or (3) operations that disable air traffic control resulting in airplane crashes.").

[21] Department of Defense, Office of the General Counsel, *An Assessment of International Legal Issues in Information Operations* (2nd ed., Nov. 1999), *reprinted in* 76 U.S. NAVAL WAR COLLEGE INTERNATIONAL LAW STUDIES 459, 483 (2002) ("Even if the systems attacked were unclassified military logistics systems, an attack on such systems might seriously threaten a nation's security. For example, corrupting the data in a nation's computerized systems for managing its military fuel, spare parts, transportation, troop mobilization, or medical supplies may seriously interfere with its ability to conduct military operations. In short, the consequences are likely to be more important than the means used.").

[22] Harold Hongju Koh, Legal Adviser, Department of State, *International Law in Cyberspace: Remarks as Prepared for Delivery to the USCYBERCOM Inter-Agency Legal Conference (Sept. 18, 2012)*, *reprinted in* 54 HARVARD INTERNATIONAL LAW JOURNAL ONLINE, 4 (Dec. 2012) ("In assessing whether an event constituted a use of force in or through cyberspace, we must evaluate factors including the context of the event, the actor perpetrating the action (recognizing challenging issues of attribution in cyberspace), the target and location, effects and intent, among other possible issues.").

[23] *Refer to* § 1.11.3 (Prohibition on Certain Uses of Force).

[24] *Refer to* § 16.1 (Introduction).

[25] Department of Defense, Office of the General Counsel, *An Assessment of International Legal Issues in Information Operations* (2nd ed., Nov. 1999), *reprinted in* 76 U.S. NAVAL WAR COLLEGE INTERNATIONAL LAW STUDIES 459, 518 (2002).

[26] DEPARTMENT OF DEFENSE, *Department of Defense Cyberspace Policy Report: A Report to Congress Pursuant to the National Defense Authorization Act for Fiscal Year 2011, Section 934*, 6-7 (Nov. 2011).

cyber operations that amount to an armed attack or imminent threat thereof.[27] As a matter of national policy, the United States has expressed the view that when warranted, it will respond to hostile acts in cyberspace as it would to any other threat to the country.[28]

Measures taken in the exercise of the right of national self-defense in response to an armed attack must be reported immediately to the U.N. Security Council in accordance with Article 51 of the Charter of the United Nations.[29]

16.3.3.1 *Use of Force Versus Armed Attack*. The United States has long taken the position that the inherent right of self-defense potentially applies against any illegal use of force.[30] Thus, any cyber operation that constitutes an illegal use of force against a State potentially gives rise to a right to take necessary and proportionate action in self-defense.[31]

16.3.3.2 *No Legal Requirement for a Cyber Response to a Cyber Attack*. There is no legal requirement that the response in self-defense to a cyber armed attack take the form of a cyber action, as long as the response meets the requirements of necessity and proportionality.[32]

---

[27] Harold Hongju Koh, Legal Adviser, Department of State, *International Law in Cyberspace: Remarks as Prepared for Delivery to the USCYBERCOM Inter-Agency Legal Conference (Sept. 18, 2012)*, *reprinted in* 54 HARVARD INTERNATIONAL LAW JOURNAL ONLINE, 4 (Dec. 2012) ("Question 4: *May a state ever respond to a computer network attack by exercising a right of national self-defense?* Answer 4: **Yes. A state's national right of self-defense, recognized in Article 51 of the UN Charter, may be triggered by computer network activities that amount to an armed attack or imminent threat thereof.**"); Barack Obama, *International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World*, 10 (May 2011) ("**Right of Self-Defense:** Consistent with the United Nations Charter, states have an inherent right to self-defense that may be triggered by certain aggressive acts in cyberspace.").

[28] Barack Obama, *International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World*, 14 (May 2011) ("When warranted, the United States will respond to hostile acts in cyberspace as we would to any other threat to our country. All states possess an inherent right to self-defense, and we recognize that certain hostile acts conducted through cyberspace could compel actions under the commitments we have with our military treaty partners. We reserve the right to use all necessary means—diplomatic, informational, military, and economic—as appropriate and consistent with applicable international law, in order to defend our Nation, our allies, our partners, and our interests. In so doing, we will exhaust all options before military force whenever we can; will carefully weigh the costs and risks of action against the costs of inaction; and will act in a way that reflects our values and strengthens our legitimacy, seeking broad international support whenever possible.").

[29] *Refer to* § 1.11.5.6 (Reporting to the U.N. Security Council).

[30] *Refer to* § 1.11.5.2 (Use of Force Versus Armed Attack).

[31] Harold Hongju Koh, Legal Adviser, Department of State, *International Law in Cyberspace: Remarks as Prepared for Delivery to the USCYBERCOM Inter-Agency Legal Conference (Sept. 18, 2012)*, *reprinted in* 54 HARVARD INTERNATIONAL LAW JOURNAL ONLINE, 7 (Dec. 2012) ("To cite just one example of this, the United States has for a long time taken the position that the inherent right of self-defense potentially applies against *any* illegal use of force. In our view, there is no threshold for a use of deadly force to qualify as an "armed attack" that may warrant a forcible response. But that is not to say that any illegal use of force triggers the right to use any and all force in response—such responses must still be *necessary* and of course *proportionate*.").

[32] Harold Hongju Koh, Legal Adviser, Department of State, *International Law in Cyberspace: Remarks as Prepared for Delivery to the USCYBERCOM Inter-Agency Legal Conference (Sept. 18, 2012)*, *reprinted in* 54 HARVARD INTERNATIONAL LAW JOURNAL ONLINE, 4 (Dec. 2012) ("There is no legal requirement that the response to a cyber armed attack take the form of a cyber action, as long as the response meets the requirements of necessity and proportionality.").

16.3.3.3 *Responses to Hostile or Malicious Cyber Acts That Do Not Constitute Uses of Force*. Although cyber operations that do not constitute uses of force under *jus ad bellum* would not permit injured States to use force in self-defense, those injured States may be justified in taking necessary and appropriate actions in response that do not constitute a use of force.[33] Such actions might include, for example, a diplomatic protest, an economic embargo, or other acts of retorsion.[34]

16.3.3.4 *Attribution and Self-Defense Against Cyber Operations*. Attribution may pose a difficult factual question in responding to hostile or malicious cyber operations because adversaries may be able to hide or disguise their activities or identities in cyberspace more easily than in the case of other types of operations.[35]

A State's right to take necessary and proportionate action in self-defense in response to an armed attack originating through cyberspace applies whether the attack is attributed to another State or to a non-State actor.[36]

16.3.3.5 *Authorities Under U.S. Law to Respond to Hostile Cyber Acts*. Decisions about whether to invoke a State's inherent right of self-defense would be made at the national level because they involve the State's rights and responsibilities under international law. For example, in the United States, such decisions would generally be made by the President.

---

[33] Department of Defense, Office of the General Counsel, *An Assessment of International Legal Issues in Information Operations* (2nd ed., Nov. 1999), *reprinted in* 76 U.S. NAVAL WAR COLLEGE INTERNATIONAL LAW STUDIES 459, 482 (2002) ("There is also a general recognition of the right of a nation whose rights under international law have been violated to take countermeasures against the offending state, in circumstances where neither the provocation nor the response involves the use of armed force. For example, an arbitral tribunal in 1978 ruled that the United States was entitled to suspend French commercial air flights into Los Angeles after the French had suspended U.S. commercial air flights into Paris. Discussions of the doctrine of countermeasures generally distinguish between countermeasures that would otherwise be violations of treaty obligations or of general principles of international law (in effect, reprisals not involving the use of armed force) and retorsions – actions that may be unfriendly or even damaging, but which do not violate any international legal obligation. The use of countermeasures is subject to the same requirements of necessity and proportionality as apply to self-defense.").

[34] *Refer to* § 18.17 (Retorsion).

[35] DEPARTMENT OF DEFENSE, *Department of Defense Cyberspace Policy Report: A Report to Congress Pursuant to the National Defense Authorization Act for Fiscal Year 2011, Section 934*, 4 (Nov. 2011) ("The same technical protocols of the Internet that have facilitated the explosive growth of cyberspace also provide some measure of anonymity. Our potential adversaries, both nations and non-state actors, clearly understand this dynamic and seek to use the challenge of attribution to their strategic advantage. The Department recognizes that deterring malicious actors from conducting cyber attacks is complicated by the difficulty of verifying the location from which an attack was launched and by the need to identify the attacker among a wide variety and high number of potential actors.").

[36] *United States Submission to the U.N. Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security 2012-2013*, 2 ("As the United States noted in its 2010 submission to the GGE, the following established principles would apply in the context of an armed attack, whether it originated through cyberspace or not: • The right of self-defense against an imminent or actual armed attack applies whether the attacker is a State actor or a non-State actor."). *Refer to* § 1.11.5.4 (Right of Self-Defense Against Non-State Actors).

The Standing Rules of Engagement for U.S. forces have addressed the authority of the U.S. armed forces to take action in self-defense in response to hostile acts or hostile intent, including such acts perpetrated in or through cyberspace.[37]

16.4 CYBER OPERATIONS AND THE LAW OF NEUTRALITY

The law of neutrality may be important in certain cyber operations. For example, under the law of neutrality, belligerent States are bound to respect the sovereign rights of neutral States.[38] Because of the interconnected nature of cyberspace, cyber operations targeting networked information infrastructures in one State may create effects in another State that is not a party to the armed conflict.[39]

16.4.1 Cyber Operations That Use Communications Infrastructure in Neutral States. The law of neutrality has addressed the use of communications infrastructure in neutral States, and in certain circumstances, these rules would apply to cyber operations.

The use of communications infrastructure in neutral States may be implicated under the general rule that neutral territory may not serve as a base of operations for one belligerent against another.[40] In particular, belligerent States are prohibited from erecting on the territory of a neutral State any apparatus for the purpose of communicating with belligerent forces on land or sea, or from using any installation of this kind established by them before the armed conflict on the territory of a neutral State for purely military purposes, and which has not been opened for the service of public messages.[41]

However, merely relaying information through neutral communications infrastructure (provided that the facilities are made available impartially) generally would not constitute a violation of the law of neutrality that belligerent States would have an obligation to refrain from

---

[37] *See, e.g.*, CHAIRMAN OF THE JOINT CHIEFS OF STAFF INSTRUCTION 3121.01B, *Standing Rules of Engagement/Standing Rules for the Use of Force for U.S. Forces*, ¶6b(1) (June 13, 2005), *reprinted in* INTERNATIONAL AND OPERATIONAL LAW DEPARTMENT, THE JUDGE ADVOCATE GENERAL'S LEGAL CENTER & SCHOOL, U.S. ARMY, OPERATIONAL LAW HANDBOOK 95 (2007) ("Unit commanders always retain the inherent right and obligation to exercise unit self-defense in response to a hostile act or demonstrated hostile intent. Unless otherwise directed by a unit commander as detailed below, military members may exercise individual self-defense in response to a hostile act or demonstrated hostile intent.").

[38] *Refer to* § 15.3.1 (Neutral Rights).

[39] Harold Hongju Koh, Legal Adviser, Department of State, *International Law in Cyberspace: Remarks as Prepared for Delivery to the USCYBERCOM Inter-Agency Legal Conference (Sept. 18, 2012)*, *reprinted in* 54 HARVARD INTERNATIONAL LAW JOURNAL ONLINE, 6 (Dec. 2012) ("States conducting activities in cyberspace must take into account the sovereignty of other states, including outside the context of armed conflict. The physical infrastructure that supports the Internet and cyber activities is generally located in sovereign territory and subject to the jurisdiction of the territorial state. Because of the interconnected, interoperable nature of cyberspace, operations targeting networked information infrastructures in one country may create effects in another country. Whenever a state contemplates conducting activities in cyberspace, the sovereignty of other states needs to be considered.").

[40] *Refer to* § 15.5 (Prohibition on the Use of Neutral Territory as a Base of Operations).

[41] *Refer to* § 15.5.3 (Prohibition Against Establishment or Use of Belligerent Communications Facilities in Neutral Territory).

and that a neutral State would have an obligation to prevent.[42] This rule was developed because it was viewed as impractical for neutral States to censor or screen their publicly available communications infrastructure for belligerent traffic.[43] Thus, for example, it would not be prohibited for a belligerent State to route information through cyber infrastructure in a neutral State that is open for the service of public messages, and that neutral State would have no obligation to forbid such traffic. This rule would appear to be applicable even if the information that is being routed through neutral communications infrastructure may be characterized as a cyber weapon or otherwise could cause destructive effects in a belligerent State (but no destructive effects within the neutral State or States).[44]

16.5 CYBER OPERATIONS AND *JUS IN BELLO*

This section addresses *jus in bello* rules and cyber operations.

16.5.1 Cyber Operations That Constitute "Attacks" for the Purpose of Applying Rules on Conducting Attacks. If a cyber operation constitutes an attack, then the law of war rules on

---

[42] *Refer to* § 15.5.3.1 (Use of Neutral Facilities by Belligerents Not Prohibited).

[43] Colonel Borel, *Report to the Conference from the Second Commission on Rights and Duties of Neutral States on Land*, *in* JAMES BROWN SCOTT, THE REPORTS TO THE HAGUE CONFERENCES OF 1899 AND 1907, 543 (1917) ("We are here dealing with cables or apparatus belonging either to a neutral State or to a company or individuals, the operation of which, for the transmission of news, has the character of a public service. There is no reason to compel the neutral State to restrict or prohibit the use by the belligerents of these means of communication. Were it otherwise, objections of a practical kind would be encountered, arising out of the considerable difficulties in exercising control, not to mention the confidential character of telegraphic correspondence and the rapidity necessary to this service. Through his Excellency Lord Reay, the British delegation requested that it be specified that 'the liberty of a neutral State to transmit messages, by means of its telegraph lines on land, its submarine cables or its wireless apparatus, does not imply that it has any right to use them or permit their use in order to render manifest assistance to one of the belligerents'. The justice of the idea thus stated was so great as to receive the unanimous approval of the Commission.").

[44] *See* DEPARTMENT OF DEFENSE, *Department of Defense Cyberspace Policy Report: A Report to Congress Pursuant to the National Defense Authorization Act for Fiscal Year 2011, Section 934*, 8 (Nov. 2011) ("***The issue of the legality of transporting cyber 'weapons' across the Internet through the infrastructure owned and/or located in neutral third countries without obtaining the equivalent of 'overflight rights.'*** There is currently no international consensus regarding the definition of a 'cyber weapon.' The often low cost of developing malicious code and the high number and variety of actors in cyberspace make the discovery and tracking of malicious cyber tools difficult. Most of the technology used in this context is inherently dual-use, and even software might be minimally repurposed for malicious action."); Department of Defense, Office of the General Counsel, *An Assessment of International Legal Issues in Information Operations* (2nd ed., Nov. 1999), *reprinted in* 76 U.S. NAVAL WAR COLLEGE INTERNATIONAL LAW STUDIES 459, 489 (2002) ("There need be less concern for the reaction of nations through whose territory or communications systems a destructive message may be routed. If only the nation's public communications systems are involved, the transited nation will normally not be aware of the routing such a message has taken. Even if it becomes aware of the transit of such a message and attributes it to the United States, there would be no established principle of international law that it could point to as being violated. As discussed above, even during an international armed conflict international law does not require a neutral nation to restrict the use of its public communications networks by belligerents. Nations generally consent to the free use of their communications networks on a commercial or reciprocal basis. Accordingly, use of a nation's communications networks as a conduit for an electronic attack would not be a violation of its sovereignty in the same way that would be a flight through its airspace by a military aircraft.").

conducting attacks must be applied to those cyber operations.[45] For example, such operations must comport with the requirements of distinction and proportionality.[46]

For example, a cyber attack that would destroy enemy computer systems could not be directed against ostensibly civilian infrastructure, such as computer systems belonging to stock exchanges, banking systems, and universities, unless those computer systems met the test for being a military objective under the circumstances.[47] A cyber operation that would not constitute an attack, but would nonetheless seize or destroy enemy property, would have to be imperatively demanded by the necessities of war.[48]

16.5.1.1 *Assessing Incidental Injury or Damage During Cyber Operations*. The proportionality rule prohibits attacks in which the expected loss of life or injury to civilians, and damage to civilian objects incidental to the attack, would be excessive in relation to the concrete and direct military advantage expected to be gained.[49]

For example, in applying the proportionality rule to cyber operations, it might be important to assess the potential effects of a cyber attack on computers that are not military objectives, such as private, civilian computers that hold no military significance, but that may be networked to computers that are valid military objectives.[50]

In assessing incidental injury or damage during cyber operations, it may be important to consider that remote harms and lesser forms of harm, such as mere inconveniences or temporary losses, need not be considered in applying the proportionality rule.[51] For example, a minor, brief disruption of internet services to civilians that results incidentally from a cyber attack against a military objective generally would not need to be considered in a proportionality analysis.[52] In

---

[45] *Refer to* § 5.5 (Rules on Conducting Assaults, Bombardments, and Other Attacks).

[46] *Refer to* § 5.6 (Discrimination in Conducting Attacks); § 5.12 (Proportionality in Conducting Attacks).

[47] *Refer to* § 5.7 (Military Objectives).

[48] *Refer to* § 5.17.2 (Enemy Property – Military Necessity Standard).

[49] *Refer to* § 5.12 (Proportionality in Conducting Attacks).

[50] Harold Hongju Koh, Legal Adviser, Department of State, *International Law in Cyberspace: Remarks as Prepared for Delivery to the USCYBERCOM Inter-Agency Legal Conference (Sept. 18, 2012)*, *reprinted in* 54 HARVARD INTERNATIONAL LAW JOURNAL ONLINE, 8 (Dec. 2012) ("As you all know, information and communications infrastructure is often shared between state militaries and private, civilian communities. The law of war requires that civilian infrastructure not be used to seek to immunize military objectives from attack, including in the cyber realm. But how, exactly, are the jus in bello rules to be implemented in cyberspace? Parties to an armed conflict will need to assess the potential effects of a cyber attack on computers that are not military objectives, such as private, civilian computers that hold no military significance, but may be networked to computers that are valid military objectives. Parties will also need to consider the harm to the civilian uses of such infrastructure in performing the necessary proportionality review. Any number of factual scenarios could arise, however, which will require a careful, fact-intensive legal analysis in each situation.").

[51] *Refer to* § 5.12.2 (Types of Harm – Loss of Life, Injury, and Damage).

[52] *Cf.* Program on Humanitarian Policy and Conflict Research at Harvard University, *Commentary on the HPCR Manual on International Law Applicable to Air and Missile Warfare*, 28 (A.1.e.7) (2010) ("The definition of 'attacks' also covers 'non-kinetic' attacks (i.e. attacks that do not involve the physical transfer of energy, such as certain CNAs [computer network attacks]; see Rule 1(m)) that result in death, injury, damage or destruction of persons or objects. Admittedly, whether 'non-kinetic' operations rise to the level of an 'attack' in the context of the

addition, the economic harms in the belligerent State resulting from such disruptions, such as civilian businesses in the belligerent State being unable to conduct e-commerce, generally would not need to be considered in a proportionality analysis.[53]

Even if cyber operations that constitute attacks are not expected to result in excessive incidental loss of life or injury or damage such that the operation would be prohibited by the proportionality rule, the party to the conflict nonetheless would be required to take feasible precautions to limit such loss of life or injury and damage in conducting those cyber operations.[54]

16.5.2 Cyber Operations That Do Not Amount to an "Attack" Under the Law of War. A cyber operation that does not constitute an attack is not restricted by the rules that apply to attacks.[55] Factors that would suggest that a cyber operation is not an "attack" include whether the operation causes only reversible effects or only temporary effects. Cyber operations that generally would not constitute attacks include:

- defacing a government webpage;
- a minor, brief disruption of internet services;
- briefly disrupting, disabling, or interfering with communications; and
- disseminating propaganda.

Since such operations generally would not be considered attacks under the law of war, they generally would not need to be directed at military objectives, and may be directed at civilians or civilian objects. Nonetheless, such operations must not be directed against enemy civilians or civilian objects unless the operations are militarily necessary.[56] Moreover, such operations should comport with the general principles of the law of war.[57] For example, even if a cyber operation is not an "attack" or does not cause any injury or damage that would need to be considered under the proportionality rule, that cyber operation still should not be conducted in a way that unnecessarily causes inconvenience to civilians or neutral persons.

16.5.3 Duty to Take Feasible Precautions and Cyber Operations. Parties to a conflict must take feasible precautions to reduce the risk of incidental harm to the civilian population and

---

law of international armed conflict is a controversial issue. There was agreement among the Group of Experts that the term 'attack' does not encompass CNAs that result in an inconvenience (such as temporary denial of internet access).").

[53] *Refer to* § 5.12.2 (Types of Harm – Loss of Life, Injury, and Damage).

[54] *Refer to* § 16.5.3 (Duty to Take Feasible Precautions and Cyber Operations).

[55] *Refer to* § 5.5 (Rules on Conducting Assaults, Bombardments, and Other Attacks).

[56] *Refer to* § 5.3.2.1 (Non-Violent Measures That Are Militarily Necessary).

[57] *Refer to* § 16.2.2 (Application of Law of War Principles as a General Guide to Cyber Operations).

other protected persons and objects.[58] Parties to the conflict that employ cyber operations should take precautions to minimize the harm of their cyber activities on civilian infrastructure and users.[59]

The obligation to take feasible precautions may be of greater relevance in cyber operations than other law of war rules because this obligation applies to a broader set of activities than those to which other law of war rules apply. For example, the obligation to take feasible precautions to reduce the risk of incidental harm would apply to a party conducting an attack even if the attack would not be prohibited by the proportionality rule.[60] In addition, the obligation to take feasible precautions applies even if a party is not conducting an attack because the obligation also applies to a party that is subject to attack.[61]

16.5.3.1 *Cyber Tools as Potential Measures to Reduce the Risk of Harm to Civilians or Civilian Objects*. In some cases, cyber operations that result in non-kinetic or reversible effects can offer options that help minimize unnecessary harm to civilians.[62] In this regard, cyber capabilities may in some circumstances be preferable, as a matter of policy, to kinetic weapons because their effects may be reversible, and they may hold the potential to accomplish military goals without any destructive kinetic effect at all.[63]

As with other precautions, the decision of which weapon to use will be subject to many practical considerations, including effectiveness, cost, and "fragility," *i.e.*, the possibility that once used an adversary may be able to devise defenses that will render a cyber tool ineffective in the future.[64] Thus, as with special kinetic weapons, such as precision-guided munitions that have

---

[58] *Refer to* § 5.3.3 (Affirmative Duties to Take Feasible Precautions for the Protection of Civilians and Other Protected Persons and Objects).

[59] *United States Submission to the U.N. Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security 2012-2013*, 4 ("The law of war also requires warring States to take all practicable precautions, taking into account military and humanitarian considerations, to avoid and minimize incidental death, injury, and damage to civilians and civilian objects. In the context of hostilities involving information technologies in armed conflict, parties to the conflict should take precautions to minimize the harm of such cyber activities on civilian infrastructure and users.").

[60] *Refer to* § 5.11 (Feasible Precautions in Conducting Attacks to Reduce the Risk of Harm to Protected Persons and Objects).

[61] *Refer to* § 5.14 (Feasible Precautions to Reduce the Risk of Harm to Protected Persons and Objects by the Party Subject to Attack).

[62] *Refer to* § 5.11.3 (Selecting Weapons (Weaponeering)).

[63] *United States Submission to the U.N. Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security 2012-2013*, 4 ("Cyber operations that result in non-kinetic or reversible effects can be an important tool in creating options that minimize unnecessary harm to civilians. In this regard, cyber capabilities may in some circumstances be preferable, as a matter of policy, to kinetic weapons because their effects may be reversible, and they may hold the potential to accomplish military goals without any destructive kinetic effect at all.").

[64] Department of Defense, Office of the General Counsel, *An Assessment of International Legal Issues in Information Operations* (2nd ed., Nov. 1999), *reprinted in* 76 U.S. NAVAL WAR COLLEGE INTERNATIONAL LAW STUDIES 459, 490 (2002) ("Another possible implication of a defender's technological prowess may arise when a nation has the capacity for graduated self-defense measures. Some may argue that a nation having such capabilities must select a response that will do minimal damage. This is a variant of the argument that a nation possessing

the potential to produce less incidental damage than other kinetic weapons, cyber capabilities usually will not be the only type of weapon that is legally permitted.

16.5.4 Prohibition on Improper Use of Signs During Cyber Operations. Under the law of war, certain signs may not be used improperly.[65] These prohibitions may also be applicable during cyber operations. For example, it would not be permissible to conduct a cyber attack or to attempt to disable enemy internal communications by making use of communications that initiate non-hostile relations, such as prisoner exchanges or ceasefires.[66] Similarly, it would be prohibited to fabricate messages from an enemy's Head of State falsely informing that State's forces that an armistice or cease-fire had been signed.[67]

On the other hand, the restriction on the use of enemy flags, insignia, and uniforms only applies to concrete visual objects; it does not restrict the use of enemy codes, passwords, and countersigns.[68] Thus, for example, it would not be prohibited to disguise network traffic as though it came from enemy computers or to use enemy codes during cyber operations.

16.5.5 Use of Civilian Personnel to Support Cyber Operations. As with non-cyber operations, the law of war does not prohibit States from using civilian personnel to support their cyber operations, including support actions that may constitute taking a direct part in hostilities.[69]

Under the GPW, persons who are not members of the armed forces, but who are authorized to accompany them, are entitled to POW status.[70] This category was intended to include, *inter alia*, civilian personnel with special skills in operating military equipment who

---

precision-guided munitions must always use them whenever there is a potential for collateral damage. That position has garnered little support among nations and has been strongly rejected by the United States. There is broad recognition that the risk of collateral damage is only one of many military considerations that must be balanced by military authorities planning an attack. One obvious consideration is that a military force that goes into a protracted conflict with a policy of always using precision-guided munitions whenever there is any potential for collateral damage will soon exhaust its supply of such munitions. Similarly, military authorities must be able to weigh all relevant military considerations in choosing a response in self-defense against computer network attacks. These considerations will include the probable effectiveness of the means at their disposal, the ability to assess their effects, and the "fragility" of electronic means of attack (i.e., once they are used, an adversary may be able to devise defenses that will render them ineffective in the future).").

[65] *Refer to* § 5.24 (Improper Use of Certain Signs).

[66] *Refer to* § 12.2 (Principle of Good Faith in Non-Hostile Relations).

[67] Department of Defense, Office of the General Counsel, *An Assessment of International Legal Issues in Information Operations* (2nd ed., Nov. 1999), *reprinted in* 76 U.S. NAVAL WAR COLLEGE INTERNATIONAL LAW STUDIES 459, 473 (2002) ("Perfidy: It may seem attractive for a combatant vessel or aircraft to avoid being attacked by broadcasting the agreed identification signals for a medical vessel or aircraft, but such actions would be a war crime. Similarly, it might be possible to use computer 'morphing' techniques to create an image of the enemy's chief of state informing his troops that an armistice or cease-fire agreement had been signed. If false, this would also be a war crime.").

[68] *Refer to* § 5.23.1.5 (Use of Enemy Codes, Passwords, and Countersigns Not Restricted).

[69] *Refer to* § 4.15.2.2 (Employment in Hostilities).

[70] *Refer to* § 4.15 (Persons Authorized to Accompany the Armed Forces).

support and participate in military operations, such as civilian members of military aircrews.[71] It would include civilian cyber specialists who have been authorized to accompany the armed forces.

Civilians who take a direct part in hostilities forfeit protection from being made the object of attack.[72]

16.6 LEGAL REVIEW OF WEAPONS THAT EMPLOY CYBER CAPABILITIES

DoD policy requires the legal review of the acquisition of weapons or weapon systems.[73] This policy would include the review of weapons that employ cyber capabilities to ensure that they are not *per se* prohibited by the law of war.[74] Not all cyber capabilities, however, constitute a weapon or weapons system. Military Department regulations address what cyber capabilities require legal review.[75]

The law of war does not prohibit the development of novel cyber weapons. The customary law of war prohibitions on specific types of weapons result from State practice and *opinio juris* demonstrating that a type of weapon is illegal; the mere fact that a weapon is novel or employs new technology does not mean that the weapon is illegal.[76]

Although which issues may warrant legal analysis would depend on the characteristics of the weapon being assessed, a legal review of the acquisition or procurement of a weapon that employs cyber capabilities likely would assess whether the weapon is inherently indiscriminate.[77] For example, a destructive computer virus that was programmed to spread and destroy uncontrollably within civilian internet systems would be prohibited as an inherently

---

[71] *Refer to* § 4.15 (Persons Authorized to Accompany the Armed Forces).

[72] *Refer to* § 5.9 (Civilians Taking a Direct Part in Hostilities).

[73] *Refer to* § 6.2 (DoD Policy of Reviewing the Legality of Weapons).

[74] Harold Hongju Koh, Legal Adviser, Department of State, *International Law in Cyberspace: Remarks as Prepared for Delivery to the USCYBERCOM Inter-Agency Legal Conference (Sept. 18, 2012)*, *reprinted in* 54 HARVARD INTERNATIONAL LAW JOURNAL ONLINE, 6 (Dec. 2012) ("States should undertake a legal review of weapons, including those that employ a cyber capability. Such a review should entail an analysis, for example, of whether a particular capability would be inherently indiscriminate, i.e., that it could not be used consistent with the principles of distinction and proportionality. The U.S. Government undertakes at least two stages of legal review of the use of weapons in the context of armed conflict: first, an evaluation of new weapons to determine whether their use would be per se prohibited by the law of war; and second, specific operations employing weapons are always reviewed to ensure that each particular operation is also compliant with the law of war.").

[75] *See, e.g.*, DEPARTMENT OF THE ARMY REGULATION 27-53, *Review of Legality of Weapons Under International Law* (Jan. 1, 1979); SECRETARY OF THE NAVY INSTRUCTION 5000.2E, *Department of the Navy Implementation and Operation of the Defense Acquisition System and the Joint Capabilities Integration and Development System* (Sept. 1, 2011); DEPARTMENT OF THE AIR FORCE INSTRUCTION 51-402, *Legal Reviews of Weapons and Cyber Capabilities* (Jul. 27, 2011).

[76] *Refer to* § 6.2.1 (Review of New Types of Weapons).

[77] *Refer to* § 6.7 (Inherently Indiscriminate Weapons).

indiscriminate weapon.[78]

[78] *United States Submission to the U.N. Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security 2012-2013*, 3 ("Weapons that cannot be directed at a specific military objective or whose effects cannot be controlled would be inherently indiscriminate, and per se unlawful under the law of armed conflict. In the traditional kinetic context, such inherently indiscriminate and unlawful weapons include, for example, biological weapons. Certain cyber tools could, in light of the interconnected nature of the network, be inherently indiscriminate in the sense that their effects cannot be predicted or controlled; a destructive virus that could spread uncontrollably within civilian internet systems might fall into this category. Attacks using such tools would be prohibited by the law of war.").