MILITARY LAW REVIEW

Volume 219 Spring 2014

CYBER WARFARE

GARY D. SOLIS*

I. Introduction

This discussion is out of date. Cyber warfare policy, techniques, and strategies, along with their associated laws of armed conflict (LOAC), are evolving so rapidly that it is difficult to stay current. A snapshot of the topic must suffice.

Much has been made of the revolution in LOAC necessitated by the advent of cyber warfare. But, "this is by no means the first time in the history of [LOAC] that the introduction of a new weapon has created the misleading impression that great legal transmutations are afoot…*viz*., the submarine."[1] Hannibal's elephants also elicited a similar erroneous impression. In fact, cyber warfare issues may be resolved in terms of traditional law of war concepts, although there is scant demonstration of its application because, so far, instances of cyber warfare have been rare. Nevertheless, although cyber questions are many, the law of war offers as many answers.

A threshold question: does existing LOAC apply to cyber issues? Yes, it does. The International Court of Justice (ICJ), in its 1996 *Nuclear Weapons* Advisory Opinion, notes that LOAC applies to "any use of

* Lieutenant Colonel, U.S. Marine Corps (Retired). J.D., University of California at Davis; L.L.M. (Criminal Law) George Washington University Law School; Ph.D., The London School of Economics & Political Science (Law of War); Professor of Law, U.S. Military Academy (Retired). Professor Solis currently teaches the law of armed conflict at Georgetown University Law Center and George Washington University Law School.

[1] Yoram Dinstein, *Concluding Remarks*, *in* 89 INTERNATIONAL LAW STUDIES: CYBER WAR AND INTERNATIONAL LAW 276, 286 (Naval War C. 2013).

force, regardless of the weapons employed."[2] Whether a 500-pound bomb or a computer is used to effect death and destruction, a weapon is a weapon. The U.S. position is made clear in the 2011 *International Strategy for Operating in Cyberspace*, when it says, "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."[3] Internationally, Article 36 of 1977 Additional Protocol I, requiring testing of new weapons and weapons systems for conformance with LOAC, illustrates that the law of war and international humanitarian law (IHL) rules apply to new technologies.

Defining many aspects of cyber warfare is problematic because there is no multi-national treaty that directly deals with cyber warfare. So far, many aspects of cyber war are not agreed upon. The law of war, as well as customary international law, lacks cyber-specific norms, and state practice in regard to the interpretation of applicable norms is slow to evolve. There is not even agreement as to whether cyber attack is one or two words. What can be said is that the *jus ad bellum* and *jus in bello* apply to cyber operations and it is safe to follow existing LOAC/IHL, as the United States' *International Strategy for Operating in Cyberspace* urges.

What is cyber warfare? It is not cybercrime—the use of computers in violation of domestic law for criminal purposes. In the United States, the *Computer Fraud and Abuse Act* defines Internet criminal acts.[4] European Union members of the NATO alliance have domestic laws implementing the 1995 E.U. Data Privacy Directive. Typical cybercrimes include access offenses, the impairment of data, misuse of devices, and interception of data offenses. Traditional criminal offenses such as fraud, child pornography, and copyright infringement may be facilitated through Internet access.[5] On an international level, cybercrime is addressed by the Council of Europe's 2001 *Convention on Cybercrime*, currently the only multinational treaty addressing the

---

[2] Legality of the Threat or Use of Nuclear Weapons, Advisory Opinion, 1995, I.C.J. 226–67, ¶ 39 (July 8).

[3] White House, *International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World* 9 (May, 2011), *available at* http://www.slideshare.net/DepartmentofDefense/department-of-defense-strategy-for-operating-in-cyberspace.

[4] 10 U.S.C. § 1030 (2014).

[5] JONATHAN CLOUGH, PRINCIPLES OF CYBERCRIME (Cambridge Univ. Press 2010). .

criminal cyber problem. Nevertheless, cyber warfare and cyber crime should not be confused.

The word "cyber" is not found in the 1949 Geneva Conventions or the 1977 Additional Protocols. In common usage, "cyber" relates to computers and computer networks; not only the Internet but all computer networks in the world, including everything they connect with and control. Cyber warfare may be defined as "warfare waged in space, including defending information and computer networks, *deterring* information attacks, as well as denying an adversary's ability to do the same. It can include offensive information operations mounted against an adversary…"[6] Cyber warfare, then, includes defense, offense, and deterrence.

Cyber warfare may be engaged in by states, by agents of states, and by non-state actors or groups. It does not necessarily constitute terrorism, but it may, depending on one's definition of terrorism. The U.S. Federal Emergency Management Agency defines cyber terrorism as "unlawful attacks and threats of attack against computers, networks, and the information stored therein when done to intimidate or coerce a government or its people in furtherance of political or social objectives."[7] Cyber terrorism is a relatively minor threat today, but its potential is obvious.

II. The Internet as Battlefield

The importance of the Internet to military, government, commercial, and private interests requires no discussion. We daily read and hear of cyber breaches and cyber incidents involving critical national

---

[6] STEVEN A. HILDRETH, CONG. RESEARCH SERV., RL30735, CYBERWARFARE 16 (2001) (emphasis in original). There is no definition of cyber warfare in Joint Publication 1-02, *Department of Defense Dictionary of Military and Associated Terms* (amended through October 15, 2013). Another definition is offered by the International Committee of the Red Cross (ICRC): "[M]eans and methods of warfare that consist of cyber operations amounting to or conducted in the context of an armed conflict within the meaning of IHL . . ." Cordula Droege, *Get Off My Cloud: Cyber Warfare, International Humanitarian Law, and the Protection of Civilians*, 94/886 INT'L REV. RED CROSS, 533, 538 (Summer, 2012).

[7] CLAY WILSON, CONG. RESEARCH SERV., RL32114, BOTNETS, CYBERCRIME, AND CYBERTERRORISM: VULNERABILITIES AND POLICY ISSUES FOR CONGRESS 3 (2008) (citations omitted).

infrastructure. China and Russia are usually identified as primary actors in those breaches.

China is particularly aggressive in its cyber intrusions and cyber theft of intellectual property.[8] China's cyber operations have been so frequent[9] and serious[10] that they have been the subject of repeated diplomatic,[11] even presidential,[12] entreaties and complaints.

Pursuant to a 1998 agreement, China has two network monitoring stations in Cuba, one located in the northernmost city of Benjucal to monitor U.S. Internet traffic, the other northeast of Santiago de Cuba to monitor U.S. Department of Defense (DoD) traffic.[13] Such penetrations are not particularly challenging to them, in part because China is familiar with U.S. Internet routers; most routers are brands of the U.S firm Cisco, but all brands of Cisco routers are made in China.

The Chinese People's Liberation Army's strategic cyber command is located in the 3rd General Staff Department, whose estimated 130,000 personnel focus on signals intelligence and defense information systems. Unit 61398 of the 2nd Bureau conducts the 3rd General Staff Department's cyber operations against America out of its Shanghai headquarters.[14] In recent years, Unit 61398 has been busy.

"Night Dragon" involved China's cyber theft of hundreds of terabytes of secret aspects of the then-new U.S. F-35 fighter from

---

[8] Li Zhang, *A Chinese Perspective on Cyber War*, 94/886 INT'L REV. RED CROSS 801 (Summer 2012) (offering a different, far milder viewpoint).

[9] David E. Sanger & Nicole Perlroth, *Chinese Hackers Resume Attacks on U.S. Targets*," N.Y. TIMES, 20 May 2013, at A1; Edward Wong, *Hackers Find China is Land of Opportunity*," N.Y. TIMES, May 23, 2013, at A1; David E. Sanger, *In Cyberspace, New Cold War*, N.Y. TIMES, Feb. 24, 2013, at A1.

[10] David E. Sanger, *China's Military is Accused by U.S. in Cyberattacks*, N.Y. TIMES, May 7, May 2013, at A1; Ellen Nakashima, *Key U.S. Weapon Designs Hacked, Officials Point Finger at China*, N.Y. TIMES, May 28, 2013, at A1; Ernesto Londoño, *Pentagon Accuses China of Hacking*, N.Y. TIMES, May 7, 2013, at A6.

[11] David E. Sanger & Mark Landler, *U.S. and China Will Hold Talks About Hacking*, N.Y. TIMES, June 2, 2013, at A1; Mark Lander & David E. Sanger, *U.S. Demands Chinese Block Cyberattacks*, N.Y. TIMES, Mar. 12, 2013, at A1.

[12] Philip Rucker, *Obama Warns Xi on Continued Cybertheft*, N.Y. TIMES, June 9, 2013, at A5.

[13] RICHARD A. CLARKE & ROBERT K. KNAKE, CYBER WAR 58 (2010).

[14] MANDIANT INTELLIGENCE CENTER REPORT: ADVANCED PERSISTENT THREAT 1: EXPOSING ONE OF CHINA'S CYBER ESPIONAGE UNITS (2013) (widely available on-line).

Lockheed Martin's data storage system. That theft began in 2007 and continued undiscovered through 2009.[15]

In September 2011, a virus of unknown (or undisclosed) origin infected classified U.S. Air Force drone control stations at Creech Air Force Base, in Nevada. The virus was repeatedly wiped off and, just as often, promptly returned. It exhibited no immediate effects and Predator and Reaper missions in Afghanistan and Iraq continued uninterrupted. The Air Force said, "We think it's benign. But we just don't know."[16]

In 2010, the Vice-Chairman of the Joint Chiefs of Staff noted that, "penetrations of Pentagon systems were efforts to map out U.S. government networks and learn how to cripple America's command-and-control systems as part of a future attack."[17]

Many DoD computer systems in the Pentagon that involve classified material are safeguarded from intrusion by security devices referred to as "tokens." Access to Pentagon computers requires the user's password and a random number that is provided by the user's token. The token is a small key-shaped thumb-drive-like object manufactured by several civilian information security companies. The token generates a new random six-digit number every sixty seconds. To unlock classified network computers, users insert their token into their computer's USB port and enter the number then showing in a small window on the token. In March 2011, "an extremely sophisticated"[18] cyber attack by "a foreign intelligence service"[19] hacked the computer system of RSA Security, a major civilian information security company, and gained data pertaining to the manufacture and the capabilities of the tokens that RSA Security supplies the Pentagon. "RSA has tens of millions of dollars worth of contracts across the federal government. Agencies with large contracts include . . . the Defense Department and its service branches."[20]

---

[15] CLARKE & KNAKE, *supra* note 13, at 233; Jason Healey, *A Brief History of US Cyber Conflict*, *in* JASON HEALEY, ED., A FIERCE DOMAIN: CONFLICT IN CYBERSPACE, 1986 TO 2012, at 14, 68 (Cyber Conflict Stud. Ass'n 2013).

[16] *Wired*, Oct. 7, 2011, *available at* http://www.wired.com/dangerroom. *See also Virus Hits Networks Used for Drone Flights*, WASH. POST, OCT. 9, 2011, at A7.

[17] J.P. London, *Made in China*, U.S. NAVAL INST. PROCEEDINGS, Apr. 2011, at 54, 56. The then-Vice-Chairman was General James Cartwright.

[18] Ellen Nakashima, *Agencies Probe Breach at Information Security Firm*, WASH. POST, Mar. 24, 2011, at A2.

[19] Thom Shaker & Elisabeth Bumiller, *After Suffering Damaging Cyberattack, the Pentagon Takes Defensive Action*, N.Y. TIMES, July 15, 2011, at A-6.

[20] Nakashima, *supra* note 18.

Rather than attacking DoD computers directly, the March 2011 cyber attack targeted the firm that provided cyber security for the computers. Three months later, "confirming the fears of security experts about the safety of the . . . tokens,"[21] hackers using the stolen RSA token data attacked Lockheed Martin, one of the nation's largest defense contractors and the maker of fighter aircraft and satellites. (This is not the same Lockheed Martin attack mentioned above.) Soon thereafter, the DoD admitted that the March 2011 cyber attack was "one of its worst digital attacks in history [losing] 24,000 Pentagon files during a single intrusion."[22] A Deputy Secretary of Defense confirmed "that over the years crucial files stolen . . . have included plans for missile tracking systems, satellite navigation devices, surveillance drones and top-of-the-line jet fighters."[23] "Bad as it was to lose secrets, that wasn't the worst threat from government hacking. Once a system has been compromised, the attacker can choose its fate; he can keep the system alive and milk it for its secrets; or he can kill it—shut it down for as long as he likes."[24]

China is hardly alone it its cyber boldness. Shortly after midnight on 6 September 2007, seventy-five miles inside Syria, at least four Israeli F-15 Eagle and F-16 Falcon fighter-bombers attacked and destroyed their Syrian target. The U.S. government had known the attack was planned and did not oppose it.[25] Although there were no casualties, it "was, by almost any definition, an act of war. But . . . nothing was heard from the government of Israel. . . . It was not until October 1st that Syrian President Bashar Assad . . . acknowledged that the Israeli warplanes had hit their target, which he described as an 'unused military building.'"[26] In fact, the Israelis had bombed into rubble a partially completed gas-cooled, graphite-moderated nuclear reactor, designed and built with years of assistance from North Korea. A month after the attack, Benjamin Netanyahu, then the Israeli Governments' opposition leader, admitted to

---

[21] Christopher Drew, *Stolen Data Is Tracked to Hacking at Lockheed*, N.Y. TIMES, June 4, 2011, at B-1.

[22] Shaker & Bumiller, *supra* note 19. Other sources say the attack was on a defense contractor's computer system (e.g., Ellen Nakashima, *U.S. Cyber Approach 'Too Predictable*', WASH. POST, July 15, 2011, at A2).

[23] *Id.*

[24] STEWART BAKER, SKATING ON STILTS: WHY WE AREN'T STOPPING TOMORROW'S TERRORISM 20 (Hoover Inst. Press 2010).

[25] GEORGE W. BUSH, DECISION POINTS 420–22 (2010) and much more revealing, ROBERT M. GATES, DUTY: MEMOIRS OF A SECRETARY AT WAR 171–77 (2014),.

[26] Seymour M. Hersh, *A Strike in the Dark*, NEW YORKER, Feb. 11 and 18, 2008, at 58.

the strike.[27] Post-attack photographs of the target site released by the United States showed mangled control rods and what appear to be elements of the reactor cooling system.[28] Unaddressed by press reports of the bombing was how Israeli warplanes managed to penetrate Syrian airspace, conduct an attack, and escape, all without a shot fired at them by Syria's modern air defense system. The answer, related by Richard Clarke, former U.S. National Coordinator for Security, Infrastructure Protection, and Counterterrorism, is an example of a cyber attack that prepped a battlefield:

> Israel had "owned" Damascus's pricey air defense network the night [of the attack]. What appeared on [Syrian] radar screens was what the Israeli Air Force had put there, an image of nothing . . . Syrian air defense missiles could not have been fired because there had been no targets in the system for them to seek out. Syrian air defense fighters could not have scrambled . . . because their Russian-built systems required them to be vectored toward the target aircraft by ground-based controllers. The Syrian . . . controllers had seen no targets.[29]

Israel screened its kinetic attack with a cyber attack that cloaked Syrian air defense radar screens with a false image of a clear sky. Clarke continues, "Whatever method the Israelis used to trick the Syrian air defense network, it was probably taken from a playbook they borrowed from the [United States]"[30]

These examples did not involve armed conflict in the traditional sense. They illustrate the danger cyber warfare poses for the national defense of a victim state, and the potential degradation of military command and control systems that could result in the death or wounding of combatant victims of a cyber attack.

---

[27] Steven Lee Myers & Steven Erlanger, *Bush Declines to Lift Veil of Secrecy Over Israeli Airstrike in Syria*, N.Y. TIMES, Sept. 21, 2007, at A12.
[28] David E. Sanger, *Bush Administration Releases Images to Bolster Its Claim About Syrian Reactor*, N.Y. TIMES, Apr. 25, 2008, at A5.
[29] CLARKE & KNAKE, *supra*, note 13, at 5.
[30] *Id.* at 8.

III. *Jus ad Bellum* and *Jus in Bello* in Cyber Warfare

In considering cyber warfare, one must be aware of the *jus ad bellum*, the law applicable to the initial resort to armed force, before considering the application of the *jus in bello*. That is because cyber attacks will occur when no armed conflict is, or has been, in progress between the victim state and attacking state, or its proxies. Whether a cyber attack is state-initiated, state-sponsored, or conducted by independent non-state actors, an initial question is not the applicable LOAC/IHL (the *jus in bello*), but whether it is lawful to initiate an armed response (the *jus ad bellum*) in the first place.

Jus ad bellum, sometimes thought of as "Just War theory," has a long and often disreputable history.

> Attempts to place war within a legal framework date back to the earliest articulation of the theory of "just war," by virtue of which war was considered a "just" response to illegal aggression. Ultimately, it was a means to restore the rights offended by the aggressor as well as a means of punishment. By relying on the validity of the cause for war, this doctrine brought into place a legal regime that reflected "the belligerent's right to resort to force."[31]

In the fifth century B.C., China "recognized rules stipulating that no war should begin without just cause. . . ."[32] Xenophon, in *Cyropaedia* (4th century B.C.), wrote about when to wage war, as did the Roman, Cicero, in his 1st century B.C. work, *De Republica*. Early Christians, notably Saints Ambrose and Constantine, developed Just War doctrine. "The central notion here is that the use of force requires justification—the presumption is always against violence—but violence may be permitted to protect other values."[33] Thomas Aquinas and Francisco de Vitoria carried Just War doctrine from the Roman Empire into the Dark Ages.

---

[31] Jasmine Moussa, *Can* jus ad bellum *Override* jus in bello? *Reaffirming the Separation of the Two Bodies of Law*, 872 INT'L REV. RED CROSS 963, 966 (Dec. 2008).
[32] PAUL CHRISTOPHER, THE ETHICS OF WAR AND PEACE 8 (2d ed. 1994).
[33] *Id.* at 23.

Hugo Grotius, looking to natural law, provided a sharper focus to Just War theory in his 1625 work, *On the Law of War and Peace*. "Modern Just War theory recognizes as many as eight conditions that are necessary to justify a nation's resorting to arms. Grotius . . . accepts only six."[34] In Grotius's teaching, there first must be a just cause prior to resorting to arms; this forbids wars of anticipation. Second, the positive aims of going to war must be proportional to the evil that the war itself will cause. Next, there must be a reasonable chance of success, thus rejecting futile or suicidal armed resistance. Fourth, wars must be publicly declared, allowing public debate of the wisdom of going to war. Only a legitimate authority may declare war; rogue commanders may not take a state to war. Finally, war must always be the last resort, undertaken only if the other five preconditions have been met and no other solution remains. These six preconditions may be debated but, basically, they encompass classic Just War theory, traditionally termed "*jus ad bellum*"—the circumstances in which states may rightfully resort to armed force.

Today, Just War theory has largely been overtaken by the United Nations Charter, which provides international legislation, as it were, mandating when states may lawfully resort to force.

"The reason for adopting a rigorous distinction between *jus ad bellum* and *jus in bello* is the need for a bright-line cleavage that is workable in the field of battle. Soldiers do not have to think about who started the war. They know that, regardless of who started the conflict, certain means of warfare are clearly illegal."[35] *Jus ad bellum* theory provides a background for deciding how to respond to attacks, including cyber attacks, and how they may lawfully be countered.

---

[34] *Id.* at 82. Some theorists add a seventh requirement, one rejected by Grotius, that a war must be waged for the ends of peace.

[35] GEORGE P. FLETCHER & JENS DAVID OHLIN, DEFENDING HUMANITY: WHEN FORCE IS JUSTIFIED AND WHY 21–22 (Oxford Univ. Press 2008). There is a view that if the war is itself unlawful, any offensive act by a soldier of the offending state is similarly unlawful and the actor-soldier therefore is a criminal. *See, e.g.*, Thomas Nagel, *War and Massacre*, 1 PHIL. & PUB. AFF. 123 (1972) (discussing U.S. soldiers in the Vietnam conflict. This position is clearly a minority view).

IV. What Constitutes a Cyber Attack?

The United States initiates offensive cyber warfare operations, of course.[36] "DoD officials reportedly stated that the United States could confuse enemies by using cyber attack to open floodgates, control traffic lights, or scramble the banking systems in other countries."[37] (Such a confident statement brings to mind the Marine Corps tactical adage that when the enemy is in range, so are you.) But does every offensive cyber operation constitute a cyber attack?

Some civilian and government computer networks are so essential to a nation's well-being that the state will protect them at almost any cost. In the United States, military and civilian computer networks relating to communications, transportation, power, water, and electrical systems, gas and oil storage, as well as banking and finance systems, are referred to as "critical national infrastructure."[38] Because they are vital to the functioning of the state, computer network attacks (CNAs) against the critical national infrastructure are considered more serious than those against many significant military objectives.

In May 2007, Estonia suffered massive cyber intrusions in the form of rolling CNAs, widely believed to have been initiated by Russian actors using as many as a million bots rented from scores of nations as distant as the United States.[39] Estonia's critical national infrastructure was brought to a standstill, apparently by Russian civilian hackers encouraged and/or coordinated by their government.[40] Then, in August 2008, the first cyber attack that coincided with an armed conflict occurred when, shortly before attacking Georgia by kinetic means, Russia overwhelmed Georgian government websites with distributed-denial-of-service attacks. The next year, in mid-2009, the American-

---

[36] William Matthews, *Pentagon Expanding Domestic Cyber Role*, MARINE CORPS TIMES, Nov. 1, 2010, at 12 (reporting an agreement between the Department of Homeland Security and the Department of Defense to share DoD's electronic spying experience and expertise).

[37] Wilson, *supra* note 7, at 18.

[38] Executive Order 13,010 (17 July 1996) (describing critical national infrastructure as including "telecommunications, electrical power systems, gas and oil storage and transportation, banking and finance, transportation, water supply systems, emergency services . . . and continuity of government.").

[39] A "bot," also called a "zombie," is a computer in which malware has been entrenched and, akin to a human "sleeper agent," lays inactive until triggered by the attacker. A network of bots constitutes a "botnet."

[40] Healey, *supra* note 15, at 68.

Israeli Stuxnet worm first appeared, eventually attacking and destroying a third of Iran's centrifuges, crucial to the country's nuclear enrichment program.

An armed attack by frontal assault, naval gunfire, or aerial bombing make clear that a kinetic attack (one using "traditional" explosive weapons) is underway. Cyber warfare, however, sometimes allows room to question if an attack is even occurring and whether LOAC/IHL applies. If a college student hacks a Blueland military command computer network, how is the network's Command Duty Officer (CDO) to know the intrusion is not the precursor of an all-out Redland cyber or kinetic attack? Further complicating the CDO's calculation is her inability to immediately know who mounted the intrusion, or from where it originated.

The distinction between the terms, "cyber *intrusion,*" and "cyber *attack*," is meaningful: in LOAC/IHL, a cyber *attack* may raise the lawful right to respond with armed force. A cyber *intrusion,* or any other cyber operation short of an attack, does not.

What, then, constitutes an "attack"? Additional Protocol I, Article 49.1 explains, "'Attacks' means acts of violence against the adversary, whether in offense or in defense." The term "acts of violence" appears to be applicable to cyber attacks. Additional Protocol I's *Commentary* notes, "It is quite clear that the meaning given [the word 'attack' in Article 49.1] is not exactly the same as the usual meaning of the word. In the larger dictionaries the idea of instigating the combat and striking the first blow is predominant . . . . [C]losest to the meaning of the term as used in the Protocol [is], 'to set upon with hostile action.'"[41] That fairly describes a cyber attack.

Further defining "attack," the *Commentary* asks whether the laying of landmines constitutes an attack: "The general feeling [of the Protocol Drafting Committee] was that there is an attack whenever a person is directly endangered by a mine laid . . . . [A]n attack is unrelated to the concept of aggression or the first use of armed force; it refers simply to the use of armed force to carry out a military operation . . . ."[42] Significantly for cyber warfare, this indicates that when an individual is

---

[41] YVES SANDOZ, CHRISTOPHE SWINARSKI & BRUNO ZIMMERMAN, EDS., COMMENTARY ON THE ADDITIONAL PROTOCOLS—1977, ¶ 1879, at 603 (1987).
[42] *Id.* ¶¶ 1881–82, at 603.

"directly endangered" it constitutes an attack. "An 'armed attack,'" adds a European writer, "can be committed by means of conventional weapons . . . but also by unconventional means . . . Arguably, the same would be true in the hypothetical case of a so-called 'computer network attack' (CNA) were it to cause fatalities or large-scale property destruction . . . ."[43]

Such reference to fatalities and property destruction suggests an objective guide for determining when a cyber operation constitutes a cyber attack:

> Some States, including the [United States], have adopted a "results test" as a way of determining whether IO [cyber information operations] constitute a use of force or an armed attack. Such a test attempts to adapt traditional State-centric kinetic concepts of the use of force in assessing whether the deliberate actions of an aggressor cause injury, death, damage, and destruction to the military forces, citizens, and property of a State, such that those actions are likely to be judged by applying traditional *jus ad bellum* and *jus in bello* principles.[44]

Several definitions of cyber attack are available in scholarly and military writings. "[T]he term 'cyber attack' is regularly used in the mass media to denote an extremely wide range of cyber conduct, much of which falls below the threshold of an 'armed attack' as understood in the *jus ad bellum,* or an attack as defined in LOAC."[45]

For either international or non-international armed conflicts, one excellent definition of cyber *attack* is: a trans-border cyber operation, whether offensive or defensive, that is reasonably expected to cause injury or death to persons, or damage or destruction to objects.[46]

---

[43] TOM RUYS, 'ARMED ATTACK' AND ARTICLE 51 OF THE UN CHARTER 176 (Cambridge Univ. Press 2010).

[44] TERRY D. GILL & DIETER FLECK, THE HANDBOOK OF THE INTERNATIONAL LAW OF MILITARY OPERATIONS ¶ 4.01.3, at 52–53 (Oxford Univ. Press 2010).

[45] Laurie R. Blank, *International Law and Cyber Threats from Non-State Actors*, 89 INT'L L. STUD. 406, 437 (2013).

[46] MICHAEL N. SCHMITT, TALLINN MANUAL ON THE INTERNATIONAL LAW APPLICABLE TO CYBER WARFARE Rule 30, at 106 (Cambridge Univ. Press, 2013). A trans-border element is added by, *id.* Rule 13, at 54. In agreement, Droege, supra note 6, at 546. *See also* Michael N. Schmitt, *Wired Warfare: Computer Network Attack and* Jus in Bello, 846 INT'L REV. OF THE RED CROSS 365, 373 (June 2002). As with so many aspects of

What extent of death, injury, damage, or destruction is required to constitute a cyber attack? The law of armed conflict does not specify. Cyber theft, cyber intelligence gathering, and cyber intrusions that involve brief or periodic interruption of non-essential cyber services, do not qualify as cyber attacks, however.[47]

> [The definition of cyber attack] should not be understood as excluding cyber operations against data (non-physical entities, of course) from the ambit of the term attack. Whenever an attack on data results in the injury or death of individuals or damage or destruction of physical objects, those individuals or objects constitute the "object of attack" and the operation therefore qualifies as an attack.[48]

An attack is determined by the violence of its consequences, not the violence of its means.

Although there is no internationally agreed-upon definition, cyber *intrusions* are cyber operations that do not rise to the level of a cyber *attack*. Cyber intrusions may be described as covert actions employing small-scale operations against a specific computer, computer system, or user, whose individual compromise would have significant value, such as a government's nuclear command and control system.[49] The difference is that intrusions do not cause death, wounding, destruction, or physical damage.

What if there have been a series of minor cyber intrusions from a common source, none of them individually rising to the threshold of an attack? Can they, in the aggregate, rise to an armed attack? Only if the related incidents, taken together, rise to the requisite scale and effect.

---

cyber warfare, there is no broad agreement as to what constitutes an attack. "The unsatisfactory answer to 'what is a cyber attack?' is: exactly what we decide is a cyber attack at a given time under given circumstances that cannot be determined in advance." Colonel Gary D. Brown, *The Wrong Questions About Cyberspace*, 217 MIL. L. REV. 214, 221 (Fall 2013).

[47] SCHMITT, *supra* note 46, at 55.

[48] *Id.* Rule 30.6, at 107–08.

[49] Robert D. Williams, *(Spy) Game Change: Cyber Networks, Intelligence Collection and Covert Action*, 79-4 GEO. WASH. L. REV. 1162, 1185 (June 2011) (citing NAT'L RESEARCH COUNCIL, TECHNOLOGY, POLICY, LAW, AND ETHICS REGARDING U.S. ACQUISITION AND USE OF CYBERATTACK CAPABILITIES § 4.2.1, at 194 (William A. Owens et al., eds., 2009).

What about that Blueland Command Duty Officer whose military computer network was hacked by a college student? The resulting damage, if any, will likely have been inflicted by the time or before she became aware of the hack; at the moment of awareness of the intrusion (or attack), all she knows is there has been a cyber operation involving penetration of the network. She will alert her superiors that the system may have been breached, although she would not know how, by whom, from where, or to what extent. This illustrates that, absent such specific knowledge, one cannot know whether an attack had been executed.

V. A Cyber Attack Is a Use of Armed Force

Nowhere is the term "use of force" clearly defined. The UN Charter Article 2(4) provides, "All members [of the UN] shall refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any State . . . ."[50] Exceptions are use of force authorized by the Security Council, and self-defense pursuant to Article 51. Customary international law also applies the prohibition to non-UN members, although *not* to non-state actors or organized armed groups.

Whether a cyber attack constitutes a use of force matters because UN Charter Article 51 requires that an armed counter-attack, if any, be a response not to a use of force, but to a use of *armed* force. The initial question, then, is whether cyber attacks constitute a use of force and, if so, the second question: are they a use of *armed* force?

> Ultimately, it is the victim state that determines whether . . . an act was use of force and what response it will take; however, these decisions are always subject to judgment by the international community.[51]

Professor Michael Schmitt notes, "Since the advent of cyber operations, States and scholars have struggled mightily to define the threshold at which an act becomes a 'use of force.' The interpretive dilemma lies in the application of the norm to cyber operations that . . . produce severe

---

[50] U.N. Charter art. 2(4).

[51] Lieutenant Commander Brian Evans & Rick Lanchantin, *Lifting the Fog on Cyber Strategy*, U.S. NAVAL INST. PROCEEDINGS, Oct. 2013, at 66, 68.

non-physical consequences."[52] The UN Charter offers no defining criteria. While the required degree of injury or damage remains unresolved, a cyber *intrusion* (a cyber operation short of an attack) into another state's cyber systems would not constitute a use of force, nor would it violate international law.[53] The ICJ, rejecting a narrow interpretation of "use of force," held in the *Nicaragua* case that "scale and effects" are to be considered in determining if particular actions amount to an attack.[54] "In other words, 'scale and effects' is a shorthand term that captures the quantitative and qualitative factors to be analyzed in determining whether a cyber operation qualifies as a use of force."[55] In regard to the required threshold of harm:

> [A]ny cyber operation causing greater than *de minimus* damage or injury suffices . . . . In particular, operations that non-destructively target critical infrastructure may come to be viewed by States as presumptive use of force. The same approach might be applied to military targets or State systems designed to provide cyber security. Another possibility is that States will begin to treat data destruction as the functional equivalent of physical destruction for use of force characterization purposes whenever the destruction of the data severely disrupts societal, economic or governmental functions.[56]

A cyber attack, as opposed to a cyber intrusion, constitutes a "use of force" if undertaken by a state's armed forces, intelligence services, or a private contractor whose conduct is attributable to the state, and its scale and effects are comparable to non-cyber operations that rise to a level of a use of force.[57]

---

[52] Michael N. Schmitt, *The Law of Cyber Warfare:* Quo Vadis*?*, 25-1 STAN. L. & POL. REV. 9 (forthcoming 2014).
[53] SCHMITT, *supra* note 46, Rule 10.8, at 44.
[54] Military and Paramilitary Activities in and Against Nicaragua (Merits), 1986 I.C.J. 14, ¶ 195 (June 27) (Judgment),.
[55] SCHMITT, *supra* note 46, Rule 11.1, at 46.
[56] Schmitt, *supra* note 52, at 10-11. Professor Schmitt's statement includes attacks on the critical national infrastructure as constituting a use of armed force.
[57] For a (very brief) contrary view, see Evans & Lanchantin, supra note 51, at 68.

VI. Cyber Attacks Are Armed Attacks

United Nations Charter Article 51 and customary law specify that only an armed attack justifies armed response in self-defense by the victim state. If the attacker's use of force does not amount to an armed attack, the victim state may bring the matter before the Security Council, or it may employ non-forcible countermeasures. "But it cannot use counterforce in self-defense."[58]

An attack mounted without actual physical force of arms may give rise to lawful self-defense by a victim state, whether the attack be kinetic or electronic. It is "unreasonable to argue that because a [computer network attack] does not physically destroy the object of attack in the traditional sense, it can never amount to a use of force or an armed attack."[59] Moreover, "[t]he choice of arms by the attacking State is immaterial."[60] Cyber attacks are singular in their ability to kill and wound, and to destroy or damage civilian and military objects without the use of a traditional kinetic weapon. That includes attacks on the critical national infrastructure.

> The mere manipulation of a banking system or other manipulation of critical infrastructure, even if it leads to serious economic loss, would probably stretch the concept of armed force. . . . But the disruption of such vital infrastructure as electricity or water supply systems, which would inevitably lead to severe hardship for the population if it lasted over a certain period, even if not to death or injury, might well have to be considered as armed force . . . . [T]hey are precisely the kind of severe consequences from which IHL seeks to protect the civilian population.[61]

"The right of self-defence may be triggered by an armed attack or a clear threat of an impending attack," Professor Yoram Dinstein notes,

---

[58] Dinstein, *Concluding Remarks*, *supra* note 1, at 276, 278.
[59] Eric Talbot Jensen, *Computer Attacks on Critical National Infrastructure: A Use of Force Invoking the Right of Self-defense*, 38 STAN. J. INT'L L. 207, 222 (2002).
[60] Yoram Dinstein, *War, Aggression and Self-Defence* 196 (Cambridge Univ. Press, 4th ed., 2005).
[61] Droege, *supra* note 6, at 548. Executive Order 13,010, specifically includes banking and finance systems in its definition of critical infrastructure. *See supra* note 37.

> [W]henever a lethal result to human beings, or serious destruction to property, is engendered by an illegal use of force by State A against State B, that use of force will qualify as an armed attack. The right to employ counter-force in self-defense against State A can then be invoked by State B . . . .[62]

Dinstein continues,

> From a legal perspective, there is no reason to differentiate between kinetic and electronic means of attack. A premeditated destructive [CNA] can qualify as an armed attack just as much as a kinetic attack bringing about the same . . . results. The crux of the matter is not the medium at hand (a computer server in lieu of, say, an artillery battery), but the violent consequences of the action taken.[63]

A traditional physical assault by force of arms is not required for the act to constitute an armed attack. For example, during a period of peace, a surprise attack employing biological or chemical weapons would be viewed as an armed attack and constitute the initiation of an armed conflict. The 9-11 attacks on the United States by al Qaeda initiated an armed conflict, even though a traditional armed enemy force was not involved. A cyber attack that kills, wounds, or destroys constitutes an armed attack, just as kinetic weapons causing the same results, would be considered an armed attack.

VII. Cyber Attacks and the Initiation of Armed Conflict

International norms guiding state behavior apply equally in cyberspace. The International Criminal Tribunal for the Former Yugoslavia (ICTY) has held that "an armed conflict exists whenever there is a resort to armed force between States, or protracted armed violence between governmental authorities and organized armed

---

[62] Yoram Dinstein, *Computer Network Attacks and Self-Defense*, *in* Michael N. Schmitt & Brian T. O'Donnell, eds., *International Law Studies*, 76 COMPUTER NETWORK ATTACK & INT'L L. 99, 100 (Naval War C. 2002).
[63] *Id.* at 103.

groups."[64] Cyber attacks may accordingly initiate either international or non-international armed conflicts.

> [International] humanitarian law principles apply whenever computer network attacks can be ascribed to a State . . . and are either intended to cause injury, death, damage or destruction . . . or such consequences are foreseeable . . . By this standard, a computer network attack on a large airport's traffic control system by agents of another State would implicate humanitarian law. So too would an attack intended to destroy oil pipelines by surging oil through them after taking control of computers governing flow . . . or using computers to trigger a release of toxic chemicals from production and storage facilities.[65]

De minimus damage or destruction, as might be caused by an attack by an armed opposition group unsupported by a sponsoring state, probably could not meet the threshold of destruction required to initiate armed conflict. Presume an intended cyber attack by a Redland armed opposition group targeting Blueland submarine navigation systems. The group's intent is to destroy the subs' ability to navigate while submerged, causing their destruction. Instead, the submarines simply surface, bypass their damaged navigation systems patching their function into alternate systems. Yes, it was a cyber attack: a trans-border offensive cyber operation, expected to cause the destruction of significant military objects. The effect, however, was (arguably) *de minimus*, causing the inconsequential surfacing of submarines to deal with the damage. Applying an effects test, the intended cyber attack would not be sufficient to initiate a non-international armed conflict. Were the attacker the state of Redland, rather than an armed opposition group, the *de minimus* result would be the same: insufficient to initiate an international armed conflict.

---

[64] Prosecutor v. Tadić, Case No. IT-94-1-A, Decision on Defense Motion for Interlocutory Appeal on Jurisdiction, ¶ 70 (Int'l Crim. Trib. for the Former Yugoslavia Oct. 12, 1995).

[65] Sean Watts, *Combatant Status and Computer Network Attack*, 50-2 VA. J. OF INT'L L. 391, 394 (2010) (emphasis in original). *See also* SCHMITT, *supra* note 46, Rule 30, at 106–07 ("The crux of the notion lies in the effects that are caused . . . For instance, a cyber operation that alters the running of a SCADA [supervisory control and data acquisition] system controlling an electrical grid and results in a fire qualifies. Since the consequences are destructive, the operation is an attack.").

Can a CNA trigger an international armed conflict in the absence of a kinetic use of force? The ICRC cautiously responds, "The answer depends on whether a computer network attack is (1) attributable to the state and (2) amounts to a resort to armed force, a term that is not defined under [international humanitarian law]."[66] Although not squarely responsive to the question, the ICRC's response highlights that a CNA initiated by non-affiliated non-state actors cannot initiate an international armed conflict. It is clear, however, that a state-initiated CNA, even without a kinetic element, may initiate an international armed conflict.

VIII. Cyber Attacks and Non-State Actors

From whom must a cyber attack emanate in order to trigger a state's right of self-defense? Cyberspace affords "the individual the same ability to deliver effects that a nation state possesses. As a result, the applicability of LOAC may be questionable if an act is attributable to an individual, potentially making the act illegal but not an act of war, or if the nation state claims the offender was operating outside the cognizance of the government."[67] Attacks by a state's armed forces are of course within the purview of UN Charter Article 51 relating to self-defense. That is also true if similar acts by non-state actors are attributable to a sponsoring state, although attribution can be a difficult cyber issue, in part because "geography is irrelevant to the issue of attribution. Non-State actors may, and likely often will, launch a cyber operation from outside territory controlled by the State to which the conduct is attributable."[68]

A question raised by the ICJ is whether non-state cyber actors, or an armed opposition group acting without state sponsorship or control, can initiate a cyber attack that raises a victim state's right to armed self-defense, even though nothing in Article 51 limits self-defense to armed attacks by a state, or by state-sponsored groups. The ICJ has twice ruled that self-defense is limited to instances of states attacked by other states. In its 2004 *Palestinian Wall* advisory opinion, self-defense against other than an attacking state is dismissed by the court in a single paragraph:

---

[66] Droege, *supra* note 6, at 543.
[67] Evans & Lanchantin, *supra* note 51, at 68.
[68] Michael N. Schmitt, *Below the "Threshold Cyber Operations: The Countermeasures Response Option and International Law*, 54 VA. OF INT'L L. (forthcoming 2014).

> Article 51 . . . recognizes the existence of an inherent right of self-defense in the case of armed attack by one State against another State. However, Israel does not claim that the attacks against it [emanating from the Occupied Palestinian Territories] are imputable to a foreign State . . . and therefore Israel could not in any case invoke those [post-9/11 UN Security Council] resolutions in support of its claim to be exercising a right of self-defense.[69]

A year later, the ICJ again rejected self-defense in response to attacks by non-state actors[70] and reaffirmed the restrictive state-centric approach enunciated in its pre-Taliban, pre-al Qaeda, 1984 *Nicaragua* opinion. That decision requires that an armed opposition group's actions be attributable to a sponsoring state before another state's right to self-defense arises. Absent such attribution, the group's war-like acts cannot form a valid basis for victim-state armed self-defense. These two opinions, although criticized,[71] hold that the self-defense provisions of UN Charter Article 51 are of "no relevance" to attacks by non-state actors because that provision applies only "in the case of armed attack by one State against another State . . . ."[72]

Through its two decisions, "the Court circumscribed the applicability of the international legal order to certain actors, leaving others unregulated despite their actual participation in activities that affect world public order."[73] The two holdings were soon questioned, however. "[A] majority of scholars accept that a strict insistence on State imputability is no longer tenable."[74] Another commentator declared, "the Court's restrictive approach is increasingly out of touch with state

---

[69] Legal Consequences of the Construction of a Wall in the Occupied Palestine Territory, The Wall Advisory Opinion, 2004 I.C.J. 136, ¶ 139 (July 9).

[70] Armed Activities on the Territory of the Congo (Democratic Republic of the Congo v. Uganda), 2005 I.C.J. 116–20, ¶¶ 132, 146, 147 (Dec. 19).

[71] *See, e.g.*, Sean D. Murphy, *Self-Defense and the Israeli Wall Advisory Opinion: An* Ipse Dixit *from the ICJ?* 99-1 AM. J. INT'L L. 62, 64 (Jan. 2005) ("First, nothing in . . . Article 51 . . . requires the exercise of self-defense to turn on whether an armed attack was committed directly by, or can be imputed to, another state . . . [and] the Security Council has repeatedly found that the conduct of nonstate actors can be a threat to international peace and security.").

[72] *Legal Consequences of the Construction of a Wall*, *supra* note 68, ¶ 139.

[73] Jacob Katz Cogan, *Current Developments: The 2010 Judicial Activity of the International Court of Justice*, 105–03 AM. J. INT'L L. 477, 486 (July 2011).

[74] RUYS, *supra* note 43, at 487.

practice."[75] Professor Laurie Blank adds, "State practice in the aftermath of the 9/11 attacks provides firm support for the existence of a right of self-defense against non-State actors, even if unrelated to any State."[76] Today, the Court's view of limited applicability is essentially disregarded.

A non-state cyber attacker would be an unprivileged belligerent, a civilian taking a direct part in hostilities.[77] "Some examples of cyber acts that could constitute direct participation in hostilities include writing and executing malicious code, launching distributed denial of service attacks, providing malware or other cyber tools to a party to the conflict . . . ."[78]

What if attacking non-state actors are not state-sponsored, and the group lacks the necessary organizational character to constitute an armed opposition group? Or if a single unaffiliated actor were to initiate a cyber attack? What if the attacking non-state actor(s) lack, in the words of the ICTY, a "headquarters, designated zones of operation, and the ability to procure, transport, and distribute arms"[79] 'or, in the case of cyber attackers, the ability to formulate and distribute electronic instructions and orders, or control the electronic means of attack? What if the hackers are no more than an unorganized aggregate, affiliated only in philosophy, united only in their determination to cripple or destroy government institutions? Lacking the organization to constitute an armed opposition group, they could not be a party and there can be no armed conflict in the sense of either common Article 2 or 3. "Cyber operations conducted by individuals or by unorganized groups of 'hackers,' no matter how intense . . . cannot qualify as a non-international armed conflict."[80] The attackers would be criminals to be captured and prosecuted under the domestic law of the state wherein their attack originated.

---

[75] Theresa Reinold, *State Weakness, Irregular Warfare, and the Right to Self-Defense Post 9/11*, 105-2 AM. J. INT'L L. 244, 261 (Apr. 2011).
[76] Blank, *supra* note 45, at 413.
[77], Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflicts art. 51.3, June 8, 1977, U.N. Doc. A/32/144 [hereinafter Protocol I]; Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of Non-International Armed Conflicts art. 13.3, U.N. Doc. A/32/144 [hereinafter Protocol II]
[78] Blank, *supra* note 45, at 430.
[79] Prosecutor v. Limaj, et al., Case No. IT-03-66-T, Judgment, ¶ 90 (In't' Crim. Trib. for the Former Yugslovia Nov, 30, 2005).
[80] Schmitt, *supra* note 52, at 19.

Any counter-attack against non-state actors, or armed opposition groups, would have to satisfy the requirements of distinction, military necessity, and proportionality, discussed, below, in a cyber context.

IX. Not All Cyber Intrusions Are Cyber Attacks

Some cyber intrusions, such as those initiated for purposes of cyber theft, intelligence gathering, espionage, or periodic disruptions or denials of nonessential cyber services,[81] may be mistakenly viewed as attacks. "[I]t is essential to differentiate between actors with 'war' intentions and those with malicious or criminal intentions, especially when assessing the appropriate response."[82]

> Absent a conventional attack component, manipulation or intrusion by itself does not automatically indicate hostile intent. A[n] intrusion into the communications network could be just an intelligence probe for future operations . . . . In the case of a CNA with only network effects, the consequences, although degrading a particular computer network, may not place [a military] force in imminent danger or be evidence of an impending attack. . . . This situation would be analogous to tolerating an aircraft tracking radar, but not a locked on fire control radar.[83]

Espionage—using spies to collect information about what another government is doing, or plans to do—is not a LOAC violation.[84] Covert actions against a state *in time of peace*, however, are generally considered violations,[85] as well as domestic law violations.[86] "[T]he

---

[81] *Id.* at 11.
[82] Blank, *supra*, note 45, at 436.
[83] Vice Admiral James H. Doyle, Jr., U.S. Navy, *Computer Networks, Proportionality, and Military Operations*, *in* Schmitt & O'Donnell, *supra* note 62, at 147, 152, 153–54.
[84] Hague Convention IV Respecting the Laws and Customs of War on Land, art. 24, Oct. 18,1907, 36 Stat. 2277 [hereinafter Hague Convention IV]. No customary law or treaty forbids the practice, although the domestic laws of all nations criminalize espionage, e.g., in American law, 18 U.S.C. §§ 793, 794 (2014).
[85] UK MINISTRY OF DEFENSE, MANUAL OF THE LAW OF ARMED CONFLICT, ¶¶ 4.9.3 –.4, at 45–46 (Oxford Univ. Press 2004).
[86] *See, e.g.*, 50 U.S.C. § 413b(e) (2014). The Computer Fraud and Abuse Act, 18 U.S.C. § 1030(a)(5)(A) (1), is also on point. Neither law explicitly criminalizes covert acts, however.

utilization of cyber networks in carrying out collection activities likely entails a measure of conceptual overlap with covert action."[87] But, as the word "likely" suggests, when considering cyber operations, the status of covert acts remains unclear in LOAC and in international law.

X. Cyber Attacks on Civilian Critical National Infrastructure

Cyber attacks are not limited to military targets. The core principle of distinction prohibits attacks on civilians and civilian objects, which includes attacks on civilian computers. But would a cyber operation targeting the U.S. civilian aviation air control computer system, which the United States considers an element of its critical national infrastructure,[88] be a cyber attack raising the right to self-defense? Such an intrusion would likely result in the death of civilians in crashing aircraft, and the destruction of aviation-related objects, meeting the U.S. definition of a cyber attack justifying acts in armed self-defense, even though the target was a civilian computer system.

What if the intrusion was an Estonia-type series of intrusions that shut down America's banking system, closed Wall Street financial markets, silenced cell phone towers, and seriously disrupted interstate communications? Professor Schmitt is surely correct when he writes that it depends:

> Given the pervasive importance of cyber activities, an interpretation that limits the notion of attacks to acts generating physical effects cannot possibly survive . . . . Perhaps the likeliest prospect is eventual expansion of the notion of attack to include interference with essential civilian functions. The difficulty with such an approach is that the notion of attack does not currently contain a severity of consequences component other than the exclusion of *de minimus* damage or injury. Rather, it focuses on the nature of the harm—damage, destruction, injury, or death . . . . A more plausible prospect is that

[87] Williams, *supra* note 49, at 1166–67.

[88] Executive Order No. 13,010 (2006) (describing critical national infrastructure as including "telecommunications, electrical power systems, gas and oil storage and transportation, banking and finance, transportation, water supply systems, emergency services . . . and continuity of government").

> States will simply begin to treat operations against essential civilian services and data as attacks . . . creating the State practice upon which the evolution in meaning can be based . . . . Some activities, like banking and operation of critical civilian infrastructure, are self-evidently essential. Beyond that . . . only State practice will definitively pinpoint those civilian activities and data that qualify as essential.[89]

For now, if no one is killed or injured, if property is not physically destroyed or materially damaged, LOAC is uncertain on the subject and the question is left open, to be determined by state practice and *opinio juris*.

Nevertheless, the direction Schmitt suggests is already indicated in U.S. government documents relating to national cyber security.

> In 1998, the U.S. government officially made critical infrastructure protection a national goal and set out a strategy for cooperation between the government and the private sector to protect systems essential to the nation's security. Sadly, fifteen years later [in 2013], implementation of a plan to defend critical infrastructure is still pending."[90]

In the 2011 *Department of Defense Strategy for Operating in Cyberspac*e the United States warns, "The Department will . . . oppose those who would seek to disrupt networks and systems, dissuade and deter malicious actors, and reserves the right to defend these vital national assets as necessary and appropriate."[91] An Executive Order issued a month after the 9/11 attacks, also suggests counter-force, should the critical national infrastructure be attacked: "It is the policy of the United States to protect against disruption of the operation of information systems for critical infrastructure and thereby help to protect the people, economy, essential human and government services, and national

---

[89] Schmitt, *supra* note 52, at 21.

[90] Brown, *supra* note 46, at 215 (citing Presidential Decision Directive/NSC 63, Critical Infrastructure Protection (May 22, 1998)).

[91] U.S. DEP'T OF DEFENSE STRATEGY FOR OPERATING IN CYBERSPACE (July 2011), *available at* http://www. slideshare.net/DepartmentofDefense/department-of-defense-strategy-for-operating-in-cyberspace.

security . . . ."[92] Presidential Policy Directive 20, of October 2012, states that "the United States Government shall retain DCEO [Defensive Cyber Effects Operations], including anticipatory action against imminent threats [to critical national infrastructure] . . . as an option to protect such infrastructure."[93] If one were to put key terms from those documents in a single sentence, it is U.S. "policy" to "oppose" through "Defensive Cyber . . . Operations" attacks on the critical national infrastructure. One may apparently surmise that a decision to defend the critical national infrastructure, as well as military objectives, has already been made by the United States.

XI. Cyber War Conflict Classification

Conflict classification, the first step in a LOAC analysis of any armed conflict, can be complex when a cyber attack is involved. Customary factors to determine conflict classification apply in cyber warfare: if two or more states oppose each other in an armed conflict, or non-state fighters are under the overall control of a state not directly involved in the conflict, it is an international armed conflict.[94] Similarly, if a state is engaged in armed conflict, not with another state, but with an armed opposition group, or groups, it may be a non-international armed conflict.[95]

An international armed conflict must by definition be "armed" and must be "international." The "armed" criterion has been discussed. In considering the "international" aspect of a common Article 2 conflict, if

---

[92] Executive Order 13,231, *available at* www.dhs.gov/xlibrary/assets/executive-order-13231-dated-2001-10--16-initial.pdf.

[93] PRESIDENTIAL POLICY DIRECTIVE/PPD-20, U.S. CYBER OPERATIONS POLICY 8 (Oct. 2012) [hereinafter PPD-20]. At the date of this writing, PPD-20 ostensibly is a classified document. It is in the public domain, however, available at numerous Internet sites, including Wikipedia.

[94] Geneva Convention for the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field, art. 2, Aug. 12, 1949, 6 U.S.T. 3114, 75 U.N.T.S. 31 [hereinafter GC I]; Geneva Convention for the Amelioration of the Condition of the Wounded, Sick, and Shipwrecked Members of Armed Forces at Sea, art. 2 Aug. 12, 1949, 6. U.S.T. 3217, 75 U.N.T.S. 31 [hereafter GC II]; Geneva Convention Relative to the Treatment of Prisoners of War, art. 2, Aug. 12, 1949, 6. U.S.T. 3316, 75 U.N.T.S. 135 [hereinafter GC III]; Geneva Convention Relative to the Protection of Civilians in Time of War, art. 2, Aug. 12, 1949, 6. U.S.T. 3516, 75 U.N.T.S. 286 [hereinafter GC IV].

[95] *Id.* GCs I, II, III, and IV, art. 3; UK MOD, MANUAL OF THE LAW OF ARMED CONFLICT, *supra* note 85, ¶¶ 3.5-3.10, at 31-33; SCHMITT, *supra* note 45, Rule 23, at 84.

a cyber attack were launched from Blueland against Redland by an individual, or a group of individuals acting on their own initiative, should a resulting conflict be viewed as "international"? Only if Blueland exercised overall control of the individual or group,[96] or otherwise endorsed or encouraged the attack. Otherwise, the attack would be the unlawful act of an individual subject to domestic law enforcement of the state from which the attack was launched. "States are required to take all necessary measures to ensure that their territories are not used by other States or non-State actors for purposes of armed activities, including planning, threatening, perpetrating or providing material support for armed attacks against other States and their interests."[97]

Might the same attack, launched by the same state-unaffiliated individuals be considered a non-international conflict? A cyber-initiated non-international conflict would require the participation of an organized armed group, or individuals, and protracted armed violence of a certain level of intensity.[98] Organization would require that the group act in a coordinated manner, with a headquarters, command structure, issuance of orders, including disciplinary orders, and an ability to enforce LOAC compliance.[99] An individual cyber attacker is unlikely to meet such criteria, nor can most groups, particularly those who "organize" on-line without a physical connection between members. These inabilities "would preclude virtually organized armed groups for the purpose of classifying a conflict as non-international."[100] Nor would cyber attacks initiated by an individual or group of individuals be likely to meet the non-international armed conflict criteria of intensity of violence, or its requisite protracted character.

In combination, these impediments raise a high bar that would hinder most cyber operations launched by individuals or groups from rising to

---

[96] Prosecutor v. Tadić, Case No. IT-94-1-A, Judgment, ¶ 145 (Int'l Crim. Trib. for the Former Yugoslavia July 15, 1999).

[97] U.N. Secretary-General, *Developments in the Field of Information and Telecommunications in the Context of International Security*, U.N. Doc. A/66/152, at 19 (20 July 2010).

[98] Prosecutor v. Haradinaj, Case No. IT-04-84 T, Judgment, ¶ 49 (Int'l Crim. Trib. for the Former Yugoslavia Apr. 3, 2008)

[99] Prosecutor v. Limaj, et al., Case No. IT-03-66-T, Judgment, ¶¶ 90, 94–129 (Int'l Crim. Trib. for the Former Yugslovia Nov. 30, 2005); Prosecutor v. Boškoski, Case No. IT-04-82-T, Judgment, ¶¶ 190, 196–97, 199–03 (Int'l Crim. Trib. for the Former Yugoslavia July 10, 2008).

[100] Michael N. Schmitt, *Classification of Cyber Conflict*, 17 J. OF CONFLICT & SECURITY L. 245, 248 (2012).

non-international armed conflict status. Instead, their acts would likely be left to domestic law enforcement agencies, guided by human rights norms.

The resolution of conflict status classification issues, many of which are un-agreed upon in LOAC/IHL, will continue to evolve through state practice.

XII. Cyber Self-Defense

"Clearly, cyber will be an element of almost any crisis we're going to see in the future," according to the incoming commander of Cyber Command and the National Security Agency when he testified before the Senate Armed Services Committee in March 2014.[101] Largely unnoticed, cyber has become one more weapon to be employed as a matter of course in defense of the nation; our nation and the enemy's nation. "[W]hen exercised against a cyber armed attack, self-defense need not be circumscribed to 'cyber-on-cyber' warfare. Once a State is at war . . . it can use all the military assets available to it . . . whether they are kinetic or cyber."[102] "For targets of value," however, "cyber weapons are difficult to engineer, and delivery is difficult to orchestrate. These targets are often military or government systems that are highly secure . . . ."[103]

Presume that a state being cyber attacked knows it is being attacked—not always a safe presumption. "In fact, in most cases, the attack will already be over and the damage done by the time it is identified."[104] Once aware of an attack, however, a possible response is a counter-attack. Counter-strikes raise new and difficult LOAC issues, such as "the problems of identifying the perpetrators, determining their intent, affixing responsibility, and applying appropriate sanctions."[105]

---

[101] David E. Sanger, *N.S.A. Nominee Promotes Cyberwar Units*, N.Y. TIMES, Mar. 12, 2014, at A18.
[102] Dinstein, *Concluding Remarks*, *supra* note 1, at 280.
[103] Evans & Lanchantin, *supra* note 51, at 689.
[104] Major Jeffrey K. Souder, *Information Operations in Homeland Computer-Network Defense*, J. OF ELECTRONIC DEF., Oct. 1, 2001.
[105] Jensen, *supra* note 59, at 213 (citations omitted).

Those calculations involve painstaking investigation, making an immediate counter-attack impractical, if not impossible.[106]

The principle of distinction remains applicable in cyber counter-attacks. "Not only are civilians and the civilian population protected from direct attack, but [measures] . . . must also be taken to reduce as much as possible the incidental effects on civilians and civilian property of attacks."[107] An immediate counter-attack against a presumed source, without significant prior trace-back efforts, or requests for investigative assistance from the state from where the attack originated, would very likely violate the principle of distinction.

To escape identification—attribution—and incidentally frustrate distinction, cyber attackers route their strikes through zombies, botnets, and networks, masked by multiple routers and hosts, making immediate identification of the state from which the attack was mounted, let alone attributing the attack to an individual or group, most difficult.

> Attribution is one of the most difficult issues in cyberattacks. Rarely is it possible . . . to determine who launched a given attack. The reasons for this are both legal and technical. Virtually every nation has statutes that forbid the unauthorized access into personal computers and internet service providers' servers, actions that would be necessary to trace-back (hack back) the attack to its origins. The process to seek judicial authorization is time consuming and burdensome; by the time it is granted the evidence is gone. And this presumes that this action is even possible.[108]

---

[106] A group of individuals, angered by PayPal's decision to no longer process donations for WikiLeaks, orchestrated a series of denial-of-service attack on PayPal's computer system, for example. All involved were U.S.-based, used their own personal computers, and employed no "foreign" routers, networks or hosts to disguise their cyber tracks. Some did not bother to obscure their Internet Protocol addresses. Law enforcement officials took weeks to identify and apprehend those involved. Somini Sengupta, *For Suspected Hackers, a Sense of Social Protest*, N.Y. TIMES, July 26, 2011, at B-1. A foreign-based CNA would be a harder nut to crack.

[107] UK MOD, MANUAL OF THE LAW OF ARMED CONFLICT, *supra* note 85, para. 5.20.1, at 66.

[108] Richard Pregent, *Cyber Defense and Counterintelligence*, NATO LEGAL GAZETTE, no. 26, Sept. 19, 2011, at 13, 16. Mr. Pregent is NATO Headquarters' Legal Advisor for Allied Command Counterintelligence.

Often, with or without the cooperation of the state from which the attack originated, sophisticated computer-driven trace-back techniques can zero in on an attacker's computer.[109]

> [B]ut eventually you will probably get to a server that does not cooperate. You could, at that point, file a diplomatic note requesting that the law enforcement authorities in the country get a warrant, go around to the server, and pull its records as part of international cooperation in investigating a crime. That could take days, and the records might be destroyed by then. Or the country in question may not want to help you. When trace-back stops working, you do have the option of "hack back," breaking into the server and checking its records. Of course, that is illegal for U.S. citizens to do, unless they are U.S. intelligence officers.[110]

"[T]his appears to be potentially the most serious problem, i.e., aiming accurately at what the intended target is and, even if one manages to strike it with precision, not at the same time creating a host of unforeseen and unforeseeable effects."[111] If, one *can* aim accurately, however, a counter-attacker will have a target-rich environment because, "in cyber warfare . . . the physical infrastructure through which the cyber weapons (malicious codes) travel qualify as military objectives . . . . Disabling the major cables, nodes, routers, or satellites that these systems rely on will almost always be justifiable by the fact that these routes are used to transmit military information and therefore qualify as military objectives."[112] Indeed, at some point in cyber warfare, the principle of distinction could become almost meaningless in protecting civilian cyber infrastructure.

---

[109] Adnan Aijaz, Syed Raza Mohsin & Mof Assir-ul-Haque, IP Trace Back Techniques to Ferret out Denial of Service Attack Sources, Sixth World Scientific & Engineering Academy & Society Int'l Conf. on Information Security and Privacy, Tenerife, Spain, 14–16 Dec. 2007 (2007). This brief paper by students of Pakistan's Military College of Signals, outlines the three most common trace back techniques (on file with author and available on Internet).

[110] CLARKE & KNAKE, *supra* note 13, at 214.

[111] Schmitt & Doswald-Beck, *Thoughts on Computer Network Attack*, *in* Schmitt & O'Donnell, *supra* note 62 at 169.

[112] Droege, *supra* note 6, at 564.

Military necessity justifies measures not forbidden by international law and that are indispensible for defeating the enemy. In observing military necessity, an attacked state must first make good-faith efforts to determine whether the state from which the attack was launched (presuming the state itself was not involved) will take action to identify and apprehend the attacker. Military "necessity addresses whether there are adequate non-forceful options to deter or defeat the attack, such as diplomatic avenues, defensive measures to halt any further attacks, or reparations for injuries caused."[113] Should those efforts fail, the need to assure the safety of the attacked armed forces and the critical national infrastructure from further attack is apparent. A counter-attack to, for example, disable an attacking computer network could be considered a military necessity—the defeat of the enemy by lawful means.[114]

A final pre-counter-attack hurdle is proportionality—whether the envisioned counterforce is proportionate to the attack suffered, and the need to repel or deter further attacks. Proportionality does not require a counter-strike to be equivalent in force or effect to that of the attack. In fact, the counter-strike may be significantly greater in force than that of the attack and still be proportional.

Once distinction, military necessity, and proportionality issues are sorted out, the specifics of a counter-attack may be considered. Satisfying these core requirements narrows a victim state's options. Can a counter-attack oriented on an attacker's reverse azimuth, routed through civilian computer networks, servers, and routers, ever avoid catastrophic damage to a civilian computer network, raising potential violations of distinction and proportionality despite efforts toward their satisfaction? Or, is the damage to the civilian network proportional and lawful collateral damage? If a counter-attack is not considered politically feasible and militarily possible, a means other than a cyber counter-attack may be required.

---

[113] Blank, *supra* note 45, at 418.
[114] United States v. Wilhelm List, et al. ("The Hostage Case"), (1948), XI TWC 1253–54. *See also* Jensen, *supra* note 59, at 218.

XIII. A Possible Response to Cyber Attack in International Armed Conflicts

U.S. Standing Rules of Engagement allow a military response to a cyber attack based simply on the target of the attack.[115] Hostile intent may be inferred from the destruction of, or significant damage to, a computer system linked to critical national infrastructure, or to a secure military network. If the cyber attack killed, wounded, or destroyed military or civilian objects, it constitutes an armed attack and armed response may be lawful.

A responsive option to a confirmed unlawful cyber attack—one carried out as a surprise attack that opens hostilities, for example—is a belligerent reprisal. If the cyber attack was lawful, a reprisal would be an unlawful response. A reprisal is a specific violation of the law of armed conflict, undertaken in the course of an armed conflict, to encourage an enemy who has violated the law of armed conflict, to refrain from continuing their unlawful conduct.[116] Reprisals are limited to international armed conflicts.[117] "Reprisal amounts to an argument that crimes are justifiable as a proportionate response to criminal acts committed by the other party. In a sense, it is the most ancient means of enforcement of the law."[118] There are four requirements for a reprisal:

> 1. It must be a response to a prior violation of international law which is imputable to the state against which the reprisal is directed;
>
> 2. It must be reasonably proportionate;
>
> 3. It must be undertaken for the purpose of putting an end to the enemy's unlawful conduct and preventing further illegalities and not for mere revenge; and

---

[115] CHAIRMAN, JOINT CHIEFS OF STAFF, INSTR. 3121.01A, STANDING RULES OF ENGAGEMENT FOR U.S. FORCES paras. 5, 7 (15 Jan. 2000).
[116] JEAN PICTET, I COMMENTARY, GENEVA CONVENTION 1949, at 341–42 (1952).
[117] 1 JEAN-MARIE HENCKAERTS & LOUISE DOSWALD-BECK, CUSTOMARY HUMANITARIAN LAW, RULES Rule 148, at 526 (Cambridge Univ. Press, 2005).
[118] WILLIAM A. SCHABAS, THE INTERNATIONAL CRIMINAL COURT: A COMMENTARY ON THE ROME STATUTE 496 (Oxford Univ. Press 2010).

> 4. Since reprisals are a subsidiary means of redress, no other effective means of redress must be available.[119]
>
> Reprisals must be based on reasonable notice . . ., must be publicized (presumably to facilitate their deterrent effects), authorized only 'at the highest level of government (presumably to exclude emotive acts of personal revenge), and must be discontinued after the enemy eschews [its] egregious conduct . . . .[120]

Professor Dinstein writes, "On the whole, the most effective modality of self-defense against an armed attack in the shape of a CNA is recourse to defensive armed reprisals, to wit, forcible counter-measures undertaken at a different time and place."[121] Judge George Aldrich, Head of the U.S. delegation to the Geneva conferences that produced the 1977 Protocols, adds that "despite the 'limitations, risks, and unfairness of reprisals,' they may be the only remedial measure the victim State can take to coerce the enemy into respecting the law."[122]

A reprisal need not be immediate, giving a victim state time to positively identify the attacker and minimize issues of distinction, and it can be calibrated to meet proportionality requirements.[123] While the period between an attack and a reprisal may not be excessive, it may be sufficiently lengthy to seek the assistance of the state from which the attack originated. Although an unfriendly state is unlikely to meet its obligations to assist in identifying and apprehending cyber attackers

---

[119] Christopher Greenwood, *The Twilight of Belligerent Reprisals*, 20 NETH. YEARBOOK OF INT'L L. 35 (1989).

[120] Michael A. Newton, *Reconsidering Reprisals*, 20 DUKE J. OF COMPARATIVE & INT'L L. 361, 375 (2010) (citing U.K. MOD, MANUAL OF THE LAW OF ARMED CONFLICT, *supra* note 85, § 16.17, at 419)).

[121] Dinstein, *Computer Network Attack*, *in* Schmitt & O'Donnell, *supra* note 62, at 107. A reprisal is not the same as self-defense. "The main difference between them is that in case of self-defense force is used to directly rebut an attack or counter some other form of prejudicial conduct, while reprisals are designed to force the adversary to change its conduct." SANDOZ, *supra* note 41, ¶ 3431, at 983.

[122] THEODOR MERON, THE HUMANIZATION OF INTERNATIONAL LAW 12–13 (LEIDEN: MARTINUS NIJHOFF, 2006) (citing George Aldrich, *Compliance with International Humanitarian Law*, 282 INT'L REV. RED CROSS 301 (May–June 1991)).

[123] Philip Sutter, *The Continuing Role for Belligerent Reprisals*, 13-1 J. CONFLICT & SECURITY L. 93, 100–01 (Spring 2008). Sutter notes two theories of proportionality in reprisals. The predominant view is that reprisals must be proportionate to the initial violation. The second theory, that reprisals may be disproportionate in order to achieve the desired goal, the enforcement of LOAC, is generally rejected.

within its borders, perhaps because the state was itself involved, the attempt to gain cooperation must be made.[124]

Belligerent reprisals, that is, reprisals taken by belligerents in the course of an armed conflict, as opposed to peacetime reprisals,[125] have a long and disreputable history. Their widespread abuse in World War II, when they were permitted by the law of war, led to their prohibition in many circumstances. Today, reprisals against prisoners of war, civilians, civilian objects, cultural objects, medical and religious personnel, places of worship, works containing dangerous forces, and the natural environment, among other target categories, are prohibited in the 1949 Geneva Conventions.[126] (Notably, the United States does not consider Additional Protocol I's prohibition on reprisals against civilians to be customary law, viewing it as binding only on states ratifying that Protocol.) Reprisals are considered unlawful in peacetime.[127] Some view them as unlawful even in time of armed conflict. Although the line is often faint, "[a] reprisal is not revenge or retribution, but an act of compliance with the law of war. . . ."[128] An ICTY opinion authored by Presiding Judge Antonio Cassese suggests that reprisal may be a violation of customary law,[129] a view that does not reflect customary law.[130] The ICRC suggests that *ad hoc* tribunals are an adequate substitute for reprisals, rendering reprisals unlawful. A trial by tribunal, however, cannot be assured, and is a questionable deterrent to cyber violations.[131]

---

[124] *See* Protocol I, *supra* note 77, art. 85.1, .2.

[125] A post-Additional Protocol I non-belligerent reprisal was, for example, European Community Regulation 1901/98 (7 Sept. 1998), prohibiting Yugoslavian airline flights between the Federal Republic of Yugoslavia and European Community nations. The financial reprisal was in response to continued Yugoslav *jus cogens* violations.

[126] *See* GC I, *supra* note 94, art. 46; GC II, *supra* note 94, art. 47; GC III, *supra* note 94, art. 13; GC II, art. 33; Protocol I, *supra* note 77, arts. 20, 51.6, 52.1, 53(c), 54.4, 55.2, and 56.4.

[127] *Legal Threat or Use of Nuclear Weapons*, *supra* note 2, ¶ 39.

[128] SCHABAS, *supra* note 118, at 95.

[129] Prosecutor v. Kupreškić, Case No. IT-95-16-T, Judgment, ¶¶ 527–36 (Int'l Crim. Trib. for the Former Yugoslovia Jan. 14, 2000).

[130] *See, e.g.*, Theodor Meron, *The Humanization of Humanitarian Law*, 94-2 AM. J. INT'L L. 239, 250 (Apr. 2000); Frits Kalshoven, *Reprisals and the Protection of Civilians: Two Recent Decisions of the Yugoslavia Tribunal*, *in* LAL C. VOHRAH ET AL., EDS., MAN'S INHUMANITY TO MAN: ESSAYS IN HONOUR OF ANTONIO CASSESE 481, 510 (The Hague, Kluwer Law Int'l 2003); UK MOD, MANUAL OF THE LAW OF ARMED CONFLICT, *supra* note 85, ¶ 16.19.2 n.62, at 421: "[T]he assertion that there is prohibition [against reprisals] in customary law flies in the face of most of the state practice that exists."

[131] Sutter, *supra* note 123, at 119.

The guiding Statutes of the ICTY, the International Criminal Tribunal for Rwanda, and the Rome Statute for the International Criminal Court, not only do not criminalize reprisal; they do not mention them at all. The ICRC's *Customary International Law Study* concludes that "it is difficult to conclude that there has yet crystallized a customary rule specifically prohibiting reprisals during the conduct of hostilities."[132] Interestingly, the ICRC *Study* also finds that there is "insufficient evidence that the very concept of lawful reprisal in *non*-international armed conflict has ever materialized in international law."[133]

The law of neutrality is not applicable in non-international armed conflicts. In international armed conflicts, however, neutrality would be a complex and delicate issue in conducting a belligerent reprisal, for it is universally accepted that "[n]eutral states must refrain from allowing their territory to be used by belligerent states for the purposes of military operations."[134] Military aircraft, for example, may not lawfully enter the airspace of another state without that state's permission.[135] A belligerent electronic reprisal routed through the cyberspace of another state on its way to its ultimate target in a third state would require the permission of the traversed state. A neutral state that knowingly permitted another state's reprisal access to its cyber network would be allowing a violation of its non-involvement in the conflict, potentially drawing the formerly neutral state into the armed conflict on the side of the reprising state.

Although not all commentators agree,[136] in international armed conflicts, reprisal appears to be a viable response to cyberattack. Frits Kalshoven, author of the leading text on reprisals, writes, "Belligerent reprisals, though by now [the year 2005] prohibited in important fields of the law of war, have not so far come under a total prohibition."[137] Lawful and unlawful belligerents on the battlefield, and command and control elements of a violating combatant force, remain lawful reprisal targets. It is fairly clear that, "in some circumstances a defense of

---

[132] 1 HENCKAERTS & DOSWALD-BECK, *supra* note 117, at 523.
[133] *Id.* at 527 (emphasis added)
[134] UK MOD, MANUAL OF THE LAW OF ARMED CONFLICT, *supra* note 85, ¶ 1.43, at 20.
[135] U.S. DEPT. OF ARMY, FIELD MANUAL, FM 27-10, THE LAW OF LAND WARFARE 520 (July 1956) ("Should the neutral State . . . fail for any reason, to prevent violations of its neutrality by the troops of one belligerent entering or passing through its territory, the other belligerent may be justified in attacking the enemy forces on this territory.").
[136] Richard B. Lillich, *Forcible Self-Help Under International Law*, *in* JOHN NORTON MOORE & ROBERT F. TURNER, NATIONAL SECURITY LAW 113, 114 (2d ed. 2005).
[137] FRITS KALSHOVEN, BELLIGERENT REPRISALS 375 (republished ed. 2005) (Neither the cover nor the title page indicate it is a republication of the original 1971 edition.).

'reprisal' will be allowed if the violation [i.e., the reprisal] was a proportionate response to a violation committed by the opposing side."[138] And "exact equivalence between the target of the attack and the response has never been a requirement of belligerent reprisals."[139] As the 1977 Additional Protocol I *Commentary* notes, "Although such measures [reprisals] are in principle against the law, they are considered lawful by those who take them . . . i.e., in response to a breach committed by the adversary."[140] Their precise form, and how they might be delivered, will be dictated by the political and tactical situations at the time.

Belligerent reprisal is a possible response to an *unlawful* cyber attack in the course of an international armed conflict, not to every cyber attack. If a state Party were cyber attacked by an opposing state Party in an on-going international armed conflict, reprisal would not be a lawful option because the initial cyber attack would simply be another form of attack in the course of the armed conflict.

XIV. A Possible Response to Cyber Intrusions in International Armed Conflicts

If belligerent reprisal is a possible response to a cyber attack, how might a state lawfully respond to a cyber intrusion that does not rise to an attack? A category of responses offering lawful options is "countermeasures." In the early twentieth century, countermeasures were referred to as "peacetime reprisals." Essentially, they are reprisals without the use or threat of force. Possible countermeasures are varied, each tailored to the situation giving rise to their use.

The authoritative but non-binding Articles of State Responsibility describe countermeasures as "State actions, or omissions, directed at another State that would otherwise violate an obligation owed to that State and that are conducted by the former in order to compel or convince the latter to desist in its own internationally wrongful acts or omissions."[141] Like reprisals, countermeasures may be unlawful acts or

---

[138] Sean D. Murphy, *Progress and Jurisprudence of the International Criminal Tribunal for the Former Yugoslavia*, 93-1 AM. J. INT'L L.57, 89 (Jan. 1999).
[139] JUDITH GARDAM, *NECESSITY*, PROPORTIONALITY AND THE USE OF FORCE BY STATES 79 (Cambridge Univ. Press, 2004).
[140] SANDOZ, *supra* note 41, ¶ 3426, at 982.
[141] Schmitt, *supra* note 68. Schmitt notes that the articles of *Responsibility of States for Internationally Wrongful Acts*, including Article 22, are not a treaty and therefore are

omissions undertaken by a victim state in response to an internationally wrongful act committed by or attributable to another state. They may be taken solely to induce, convince, or compel the other state to return a situation to lawfulness.

For instance, if wrongful Redland cyber operations are ongoing against Blueland's banking system, Blueland may respond with cyber countermeasures blocking Redland's access to its own state bank accounts, a limited pinpoint intrusion into the offending state's banking system that would not constitute a cyber attack. To block access to all Redland bank accounts, however, would affect non-state accounts and be a violation of distinction.

Countermeasures, like reprisals, must be preceded by a request that the responsible state remedy its wrongful act. Like reprisals, they may only be taken to induce compliance with international law after an earlier international wrong attributable to a state, they must be proportionate,[142] and they must be ended when the responsible state returns to compliance with its obligations. Also like reprisals, countermeasures to internationally wrongful cyber activity may be cyber or non-cyber in character, and they may not involve the threat or use of force.

Because countermeasures involve acts that are otherwise unlawful, they differ from acts in retorsion, which "refers to the taking of measures that are lawful, but 'unfriendly.' A State may, for example, block certain cyber transactions emanating from another State because the former enjoys sovereignty over cyber infrastructure on its territory."[143]

In September 1998, Electronic Disturbance Theater (EDT), a small group of individuals located in California, launched a pre-announced distributed-denial-of-service program against a Pentagon website. Notably, EDT referred to its cyber program as a virtual sit-in, and as

---

non-binding. They nevertheless are authoritative, having been developed by the International Law Commission and commended to governments by the UN General Assembly in 2001. They are generally, although not universally, accepted as customary international law. Countermeasures are discussed in Part 3, Chapter II of the Draft Articles. *See generally* OMAR YOUSIF ELAGAB, THE LEGALITY ON NON-FORCIBLE COUNTER-MEASURES IN INTERNATIONAL LAW (Clarendon Press 1988).

[142] Countermeasures proportionality differs from the more familiar proportionality in LOAC/IHL. In gauging countermeasures proportionality the focus is on the injury suffered by the victim state, rather than limiting defensive measures to those required to defeat the armed attack of another state.

[143] Schmitt, *supra* note 68 (footnote omitted).

performance art. Their denial of service program, called "FloodNet," entered and searched the Pentagon website's search engine every nine seconds, effectively shutting it down. Having been forewarned, the Defense Information Systems Agency (DISA, now co-located and associated with CyberComm, at Fort Meade, Maryland) responded with a denial of service intrusion of its own and crashed the browsers being used by EDT.[144]

Was EDT's denial of service a cyber attack, a cyber intrusion, or an unlawful hack? There was no death, injury, destruction, or damage, nor was it trans-border; thus, it was not an attack. It was small-scale and targeted a specific computer system, the penetration of which was of some value, which describes a cyber intrusion. Taking place within the borders of the United States, it also was unlawful as a violation of the federal Computer Fraud and Abuse Act.[145] Was DISA's hack-back a countermeasure, or a retorsion? It was neither, because another state was not involved and there was no apparent violation by EDT of international law. What was DISA's countermeasure, then?

XV. Cyber Attacks and Intrusions in Non-International Armed Conflicts

Reprisals and countermeasures are limited to employment by states engaged in international armed conflicts. Cyber attacks and intrusions initiated by non-state actors and opposition groups not attributable to a state are criminal acts to be investigated, prosecuted, and punished by domestic authorities of the state from where the event emanated. Such cyber intrusions occur thousands of times every day. As Professor Schmitt notes, "in light of the imminent advent of 'cyber terrorism,' a State's obligation to control cyber activities taking place on its territory looms especially large."[146]

XVI. U.S. Cyber Practice

The United States was aware of cyberwarfare's threat well before the last century ended but took few defensive measures until well into the twenty-first century. In 2008, the President signed National Security

---

[144] Winn Schwartau, *Cyber-Civil Disobedience*, NETWORK WORLD, Jan. 11, 1999.
[145] 18 U.S.C. § 1030 (a)(3) (2014).
[146] Schmitt, *supra* note 68.

Presidential Directive 54 (NSPD-54), *Comprehensive National Cybersecurity Initiative*[147] which was kept secret until 2010, discusses U.S. cybersecurity goals which, at the time, were rudimentary and predictable. NSPD-54's notable result, one that will have lasting effect, was construction of America's principal cyber data collection center at Bluffdale, Utah, near Salt Lake City.[148]

The 2011 *Department of Defense Strategy for Operating in Cyberspace* (*DoD Strategy*) notes in its Introduction that "[o]ur reliance on cyberspace stands in stark contrast to the inadequacy of our cybersecurity."[149] It goes on to explain that U.S. military cyber strategy centers on a five-point program that calls for the cooperation of the entire defense establishment, including civilian defense corporations, agencies, and individuals.

The *DoD Strategy* lays out each of the five "strategic initiatives." First, cyberspace is to be considered a distinct domain, allowing the "DoD to organize, train, and equip for cyberspace as we do in air, land, maritime, and space to support national security interests."[150] Future exercises and war games are directed to include cyber red (i.e., enemy) teams, as well as the development of a "National Cyber Range,"[151] apparently an electronic version of a live-fire rifle range. Second, the DoD will employ new defense operating concepts to protect networks and systems, including sensor, software, and intelligence defenses against insider threats, as well as outside intrusions into DoD networks and systems, including cloud computing. The *Strategy* next requires the DoD to act with other government departments and agencies, and the private (i.e., defense contractor) sector, to generate an overarching government-wide cybersecurity. Note that the *Strategy* is intended to protect DoD cyber operations and networks, not the United States as a whole, although through this third initiative, civilian organizations and

---

[147] NATIONAL SECURITY PRESIDENTIAL DIRECTIVE 54 (8 Jan. 2008) ("The Comprehensive National Cybersecurity Initiative").

[148] Completed in late 2013, the $1.5-billion Community Comprehensive National Cybersecurity Initiative Data Center was the Pentagon's largest construction project in the United States to date. Operated by the NSA, the data collection center can intercept, capture, and store exabytes of a wide variety of electronic data, including foreign signals intelligence, U.S. domestic telephone, Internet, credit card usage data, and parking receipts. James Bamford, *The NSA Is Building the Country's Biggest Spy Center (Watch What You Say)*, WIRED MAG., Mar. 2012.

[149] DOD STRATEGY FOR CYBERSPACE, *supra* note 91.

[150] *Id.* at 5.

[151] *Id.* at 12.

corporations supplying defense technologies, weapons, and personnel are encompassed. The *Strategy* notes in a hopeful tone, "Public-private partnerships will necessarily require a balance between regulation and volunteerism . . . ."[152] Fourth, the DoD is directed to partner with allies and international partners to strengthen cybersecurity. "By sharing timely indicators about cyber events, threat signatures of malicious code, and information about emerging actors and threats, allies and international partners can increase collective cyber defense."[153] Finally, a high quality cyber workforce, capable of rapid technological advancement, is mandated. . . ."[154]

The American news media, anticipating release of the *DoD Strategy*, wrote that the Pentagon would consider cyber attacks to be "acts of war,"[155] The *Strategy* does not go that far, but it does announce that the "[DoD] will . . . oppose those who would seek to disrupt networks and systems, dissuade and deter malicious actors, and reserves the right to defend these vital national assets as necessary and appropriate."[156] Does "networks and systems" indicate that the DoD assumes responsibility for protecting civilian systems such as the critical national infrastructure? Former Secretary of Defense Robert Gates writes, "There was a deep division within the government—in both the executive branch and Congress—over who should be in charge of our domestic cyber defense: government or business, the Defense Department's National Security Agency, the Department of Homeland Security, or some other entity . . . . The result was paralysis."[157] Any paralysis in U.S. practice was soon cured, however.

Executive Order 13,231, *Critical Infrastructure Protection in the Information Age* (16 October 2001), issued a month after the 9-11 attacks, suggests unspecified retaliation, should the critical national infrastructure be attacked: "It is the policy of the United States to protect against disruption of the operation of information systems for critical infrastructure and thereby help to protect the people, economy, essential

---

[152] *Id.* at 9.
[153] *Id.*
[154] *Id.* at 10.
[155] David E. Sanger & Elizabeth Bumiller, *Pentagon to Consider Cyberattacks Act of War*, WASH. POST, June 1, 2011, at A10. The article does not specify the document it refers to. It is possible there is a separate unannounced document denominating cyber attacks as acts of war.
[156] DOD STRATEGY FOR OPERATING IN CYBERSPACE, *supra* note 91, at 10.
[157] GATES, *supra* note 25, at 449.

human and government services, and national security. . .” Any covert cyber act initiated by the government, however, including DoD, and presumably the Central Intelligence Agency, requires a presidential finding, as well as notification of both the House and Senate intelligence committees.

In May 2011, two months before issuing the *DoD Strategy for Operating in Cyberspace*, the United States published its *International Strategy for Operating in Cyberspace*. The *International Strategy* is oriented less toward defense, instead promoting “an open, interoperable, secure, and reliable information and communications infrastructure that supports international trade and commerce. . . .”[158] Surprisingly, it is more direct than the *DoD Strategy* in asserting America’s response to cyber attack:

> 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 . . . . 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.[159]

A report released by the Government Accounting Agency days after release of the 2011 *DoD Strategy* noted the lack of a joint doctrine for cyber operations: “[T]here is still a lack of clarity over whether the uniformed services should report to Cyber Command or the geographic combatant commands in cyber operations . . . .”[160] Military doctrine shaping operations on land, sea, air, and outer space have been in place for decades. Cyber warfare doctrine at the same level of detail and sophistication is evolving, but is not yet in place.[161]

U.S. Cyber Command (“CyberCom”) was established in May 2010. It is a subordinate unit of U.S. Strategic Command. Its creation should establish clearer command relationships and will shape military cyber

---

[158] *International Strategy for Cyberspace*, *supra* note 3.
[159] *Id.* at 14.
[160] Ellen Nakashima, *GAO Faults Pentagon’s Cyber Efforts, Lack of Clarity*, WASH. POST, July 26, 2011, at A5.
[161] Thom Shanker, *U.S. Weighs Its Strategy on Warfare in Cyberspace*, N.Y. TIMES, Oct. 19, 2011, at A12.

doctrine. CyberCom is co-located with a major National Security Agency (NSA) facility, NSA's Threat Operations Center, at Fort Meade, Maryland. Significantly, CyberCom and NSA are commanded by the same four-star general, a circumstance objected to, reviewed, and confirmed by Congress in 2014. Co-locating Cyber Command and NSA allows both to leverage the expertise of the other, "obviating the need for reinventing many wheels."[162] CyberCom includes multi-service elements intermixed with civilian cyber experts. Its mission is to plan, coordinate, integrate, and conduct activities to direct the operations and defense of DoD information networks, to prepare and conduct military cyberspace operations, and to deny adversaries freedom of action in cyberspace.[163] This logically includes offensive, as well as defensive, cyber operations. Indeed, in 2010, the United States deployed an expeditionary cyber-support element to the Afghanistan combat zone.[164]

The 2008 *Comprehensive National Cybersecurity Initiative* and the 2011 *International Strategy for Operating in Cyberspace* are vague in regard to a U.S. response to cyber attacks.

> Neither defines a hostile act in cyberspace, nor is there language explicitly stating when, how, and to what extent the United States will respond to such acts . . . . The United States is better served in the long run by not establishing such thresholds. . . . If red lines are established, we will be compelled to respond to each threat that crosses the line, which is unrealistic . . . . [N]ot doing so allows government leaders the latitude to tailor response options. . . . [R]ed lines that automatically result in a response could escalate an already volatile situation.[165]

Since the establishment of CyberCom, however, the United States has been anything but vague in announcing its intended cyber practice. In 2013, CyberCom's commanding general revealed the establishment of

---

[162] CLARKE & KNAKE, *supra* note 13, at 39.

[163] U.S. Cyber Command Fact Sheet, *available at* http://www.stratcom.mil/factsheets/cyber_command/.

[164] *U.S. Cyber-Command: Organizing for Cyberspace Operations, Before the House Armed Servs. Comm.* (statement of General Keith B. Alexander, Commanding General designate, U.S. Cyber Command, 111th Cong. (Sept. 2010).

[165] Lieutenant Commander John A. Mowchan, *Don't Draw the (Red) Line*, U.S. NAVAL INST. PROCEEDINGS, Oct. 13, 2013, at 10, 19–20.

forty cyber teams; thirteen of them programming teams to formulate and execute offensive cyber counterattacks in response to cyber attacks on the United States. "I would like to be clear that this team, this defend-the-nation team, is not a defensive team," the general testified at a House Armed Services Committee hearing. (The general apparently missed the irony of specifying that the "defend-the-nation team" is not defensive.) He continued, "This is an offensive team . . . to defend the nation if it were attacked in cyberspace. Thirteen of the teams that we're creating are for that mission alone."[166] The other twenty-seven teams, he said, focus on training and surveillance. Six months later, in September 2013, CyberCom activated a Cyber Mission Force, composed of National Mission Teams, Combat Mission Teams, and Cyber Protection Teams.[167] Although the teams' missions were unannounced, their titles suggest their direction.

In Tehran, in October 2013, Mojtaba Ahmadi, an Islamic Revolutionary Guards officer who commanded Iran's Cyber War Headquarters, was shot and killed by unknown assailants on his way to work.[168] Since 1977, five Iranian nuclear scientists have been murdered, as well. There is no accusation of U.S. involvement, but cyber warfare may have entered a dangerous stage extending the boundaries of LOAC/IHL.

> The Pentagon has developed a list of cyber-weapons and -tools, including viruses that can sabotage an adversary's critical networks . . . . [T]he military needs presidential authorization to penetrate a foreign computer network and leave a cyber-virus that can be activated later. The military does not need such approval, however, to penetrate foreign networks for a variety of other activities. These include studying the cyber-capabilities of adversaries or examining how power plants or other networks operate. Military cyber-warriors can also, without presidential authorization, leave beacons to mark spots for later targeting by viruses. . . . [T]he United States need not respond to a cyberattack in kind

---

[166] Mark Mazzetti & David E. Sanger, *Security Chief Says Cyberattacks Will Meet With Retaliation*, N.Y. TIMES, Mar. 13, 2013, at A4.
[167] Admiral James Stavridis & David Weinstein, *Time for a U.S. Cyber Force*, U.S. NAVAL INST. PROCEEDINGS, Jan. 2014, at 40, 41.
[168] Caroline Byrne, *Iranian Cyber Warfare Commander Shot Dean in Suspected Assassination*, THE LONDON TELEGRAPH (25 Nov. 2013).

> but may use traditional force instead as long as it is proportional . . . . [T]he use of any cyber-weapon outside an area of hostility or when the United States is not at war . . . requires presidential approval . . . .[169]

In November 2012, President Obama signed Presidential Policy Directive 20 (PPD-20), *U.S. Cyber Operations Policy*, revealing new U.S. cyber policies and initiatives; PPD-20 directs that the U.S. government shall conduct neither offensive or defensive cyber operations "that are intended or likely to produce cyber effects within the United States unless approved by the President."[170] A less sanguine section of PPD-20 directs that:

> The United States Government . . . shall make all reasonable efforts . . . to identify the adversary and the ownership and geographic location of the targets and related infrastructure where DCEO [defensive cyber effects operations] or OCEO [offensive cyber effects operations] will be conducted or cyber effects are expected to occur, and to identify the people and entities, including U.S. persons, that could be affected by proposed DCEO or OCEO.[171]

Another section discusses the critical national infrastructure, saying, "the United States Government shall retain DCEO, including anticipatory action taken against imminent threats . . . as an option to protect such infrastructure."[172] While specifying a protective interest in the critical infrastructure, the PPD does not announce how it will be defended before an attack, other than to say its protection shall be coordinated with the Department of Homeland Security.[173] Nevertheless, PPD-20 authorizes the Secretary of Defense to conduct "Emergency Cyber Actions necessary to mitigate an imminent threat or ongoing attack using DCEO if circumstances at the time do not permit obtaining prior Presidential approval . . . ."[174] The PPD suggests a strong U.S. offensive capability, along with an awareness of need for that capability's high-level control.

---

[169] Ellen Nakashima, *Defense Dept. Develops List of Cyber-weapons*, WASH. POST, June 1, 2011, at A3.
[170] PPD-20, CYBER OPERATIONS POLICY, *supra* note 93, at 6.
[171] *Id.* at 7.
[172] *Id.* at 8.
[173] *Id.*
[174] *Id.* at 10.

It also illustrates that for cyber defense and responsive actions to be effective they must be predetermined and coordinated with Armed Service cyber security units, civilian law enforcement agencies, the Department of State, and international police agencies.

One might well ask whether, in U.S. practice, there is any *law* regarding cyber operations; any binding, codified regulation of cyber warfare activity. Although domestic laws and multistate treaties are sure to come, apparently there is none as of this writing. The publicly known guidance is a 2001 Executive Order protecting critical infrastructure, a 2008 Presidential Directive on national cybersecurity, a 2011 DoD strategy guidance, a similar executive-issued international strategy, and a 2012 PPD on cyber operations; an order, two directives, and two strategies. None have the force of law, but they authorize a broad range of U.S. cyber warfare practices.

XVII. Stuxnet[175]

Enriched uranium is critical to the manufacture of nuclear weapons. Uranium is enriched in high-speed centrifuges. Centrifuges depend on computerized operating directions and controls. Few companies have the technical ability to build such complex machines or their controlling electronic systems. Centrifuges, and millions of other mechanical devices that play vital roles in everyday life, are essentially controlled by small plastic boxes the size of a cigarette pack called programmable-logic controllers. "These controllers, or P.L.C.s, perform the critical scut work of modern life. They open and shut valves in water pipes, speed and slow the spinning of uranium centrifuges, mete out the dollop of cream in each Oreo cookie, and time the change of traffic lights from red to green."[176]

On June 17, 2010, a computer in Iran would not stop rebooting. Within a few days, a virus was found to be infecting the computer's Microsoft Windows operating system. The virus was a worm that replicated through infected e-mail, or when an infected flash drive was plugged into the computer. Leaving no sign of its presence, the virus

---

[175] Except where indicated, this section is based on Michael Joseph Gross, *A Declaration of Cyber-War*, *Vanity Fair* (Apr. 2011) magazine, and the internet version of the same article, which differs slightly.

[176] *Id.* p. 1 of internet version.

uploaded two files: a "rootkit dropper," giving the worm administrator status in the computer's operating system, and a payload injector of encrypted malicious code. "The most unsettling thing about the virus was that its components hid themselves as soon as they got into the host."[177] Later, it was determined that the first Stuxnet infection occurred in June 2009.[178]

Within a few days, a German security analyst decrypted most of the infected payload and discovered that its target was P.L.C.s. Specifically, P.L.C.s in certain gas centrifuge models made by the German engineering conglomerate, Siemens.[179] On July 16, 2009, Microsoft issued the first of a series of patches, defenses against the virus, which had been found in only a few American and European sites. Thousands of infections were reported in India, Indonesia, and Iran. A Microsoft researcher named the virus "Stuxnet," for an anagram of letters from two sections of its code.

The digital code that allowed Stuxnet to pass from computer to computer was quickly revoked, but a new Stuxnet version, with a new digital pass code, immediately appeared and the worm continued to spread the virus. When it, too, was revoked, a third version appeared. When the third code was revoked no new digital pass code version arose, but the virus continued to spread from computers already infected.

It was apparent to researchers that a national government must have written the complex and lengthy (said to be a half-megabyte[180]) virus that exploited Windows' source code. Symantec became a major analyst of Stuxnet and "[a] Symantec strategist estimated that as many as 30 different people helped write it . . . [taking] at least six months."[181] Nor were the writers ordinary hackers.

When Stuxnet entered a host computer, it attempted to spread to all computers on that network, specifically searching for Siemens software. When found, the virus determined if the host computer was connected to

---

[177] *Id.* at 2.
[178] John Markoff, *Malware Aimed at Iran Hit Five Sites, Report Says*, N.Y. TIMES, Feb. 13, 2011, at A12.
[179] Other sources cite another target: frequency converters, which apparently are P.L.C.-based power sources that control the speed of motors by changing the frequency converter's output frequency.
[180] Richard A. Falkenrath, *From Bullets to Megabytes*, N.Y. TIMES, Jan. 27, 2011, at A27.
[181] Gross, *supra* note 175, at 4.

a P.L.C. If so, the virus searched for a particular model of Siemens machine that the P.L.C. controlled, and inquired if the machine was operating under a specific range of conditions. If it was running within that range, Stuxnet injected the rogue code into the P.L.C. to vary the machine's operation. The variation radically varied the speed of the centrifuge's rotors, causing them to destroy themselves.[182] "In a spooky flourish . . . the worm ends the attack with a command to restore the current to the perfect operating frequency for the centrifuges . . . ."[183]

> [E]ven as it sabotages its target system, it fools the machine's digital safety system into reading as if everything were normal . . . . Stuxnet is like a self-directed stealth drone: the first known virus that, released into the wild, can seek out a specific target, sabotage it, and hide both its existence and its effects until after the damage is done.[184]

This is the course taken by Stuxnet in three waves of attacks on Iran's centrifuges at Natanz, the desert site of Iran's nuclear enrichment facility, where the Bushehr nuclear power plant is located.[185] The first attack was in late 2009, the other two in 2010.[186]

What damage did Stuxnet inflict on Iran's centrifuges, and its nuclear program? Reports vary, some reports being suspect. The *New York Times* wrote that Stuxnet involved Siemens' initial cooperation with the United States (almost surely incorrect), and that Stuxnet "appears to have wiped out roughly a fifth of Iran's nuclear centrifuges."[187] That would be as many as a thousand centrifuges. A *Times* security analyst source said, "The attackers took great care to make sure that only their designated targets were hit . . . It was a marksman's job."[188] Such care

---

[182] William J. Broad & David E. Sanger, *Worm in Iran Was Perfect for Sabotaging Nuclear Centrifuges*, N.Y. TIMES, Nov. 19, 2010, at A1.
[183] *Id.*
[184] Gross, *supra* note 175, at 5.
[185] Markoff, *supra* note 178. Other sources assert there were two waves.
[186] Joby Warrick, *Iran Recovered Swiftly in Wake of Cyberattack*, WASH. POST, Feb. 16, 2011, at A1.
[187] William J. Broad, John Markoff & David E. Sanger, *Israel Tests Called Crucial In Iran Nuclear Setback*, N.Y. TIMES, Jan. 16, 2011, at A1.
[188] *Id.*

suggests someone concerned with distinction and proportionality.[189] "No independent hacker or criminal would bother with such niceties."[190]

> Stuxnet's code telegraphs the inherent caution of its makers in yet another way: it has a "fail-safe" feature to limit its propagation. The USB-spreading code, for instance, limits the number of devices that each infected device can itself infect. (The limit is three, enough to create a moderate chain reaction, but not so many that its effects would rage out of control.) Most dramatically, on June 24, 2012, the worm will self-destruct altogether; erase itself from every infected machine and simply disappear.[191]

In November 2010, Mahmoud Ahmadinejad, Iran's president, announced that a cyber attack had caused "minor problems with some of our centrifuges,"[192] and the UN's International Atomic Energy Agency reported that nearly 1,000 of Iran's Natanz centrifuges had been shut down for as long as a week. That is a period consistent with replacing all 4,800 centrifuges' operating software.[193] Despite the widespread damage, the Iranian enrichment process recovered in remarkably quick time, and "the net impact was relatively minor."[194]

To whom may the Stuxnet cyber attack be attributed? Most accounts credit it as a joint U.S.-Israeli project.[195] Although there is no proof of origin, media sources provide confirming details.[196] For example, details

---

[189] One source, Markoff, *supra* note 178, notes that, based on a Symantec analysis, Stuxnet infected 12,000 computers. Unless those computers were part of a network associated with Siemens centrifuges, however, the impact of the infections likely were imperceptible. The 2010 repeated re-booting of the computer that brought Stuxnet to light apparently was a one-off.

[190] Brown, *supra* note 46, at 218.

[191] Gross, *supra* note 175, at 7.

[192] Broad, Markoff & Sanger, *supra* note 187.

[193] Glenn Kessler, *Centrifuges in Iran Were Shut Down, IAEA Report Says*, WASH. POST, Nov. 24, 2010. Other reports indicate 9,000 centrifuges (e.g.,Warrick, *supra* note 186).

[194] Kessler, *supra* note 193; Warrick, *supra* note 186. To the same effect, Gross, *supra* note 175, at 10.

[195] Kessler, *supra* note 193.

[196] David E. Sanger, *Obama Order Sped Up Wave of Cyberattacks Against Iran*, N.Y. TIMES, June 1, 2012, at A1. A few months later, Sanger expanded on his detailed information in, *Confront and Conceal*, iv–xiii; 188–209 (Crown Publishers 2012); Ellen Nakishima, *Flame Virus Has Infected Computers, Iran Says*, WASH. POST, May 30, 2012, at A3.

that Stuxnet was designed by a small programmer cell, the Office of Tailored Access Operations at the Fort Meade, Maryland, headquarters of the National Security Agency, with improvements and new versions from Israel's NSA equivalent, Unit 8200.[197] Further confirming the origin of Stuxnet, "[retired Air Force General] Michael D. Hayden, the former chief of the CIA, [said], . . . 'This is the first attack of a major nature in which a cyberattack was used to effect physical destruction . . . . [Y]ou can't help but describe it as an attack on critical infrastructure.'[198] American and Israeli authorities have denied neither their role, nor reports that Stuxnet was part of what is called "Operation Olympic." Another virus, Duqu, was an earlier reconnaissance tool for Stuxnet that copied blueprints of Iran's nuclear program.[199] A third Operation Olympic virus was Flame, a data-mining virus confirmed by Iran to have stolen information from its computers.[200]

"One big question is why its creators let the software spread widely, giving up so many of its secrets in the process."[201] The answer, according to one writer, is that Stuxnet was aimed only at Natanz's centrifuges but a careless Iranian scientist "plugged his laptop into the [centrifuge] computer controllers and the worm had hopped aboard. When he later connected the same laptop to the Internet, the worm broke free and began replicating itself, a step its designers never anticipated."[202] Although it should have been foreseen, it was not intended that Stuxnet should spread beyond the targeted machines.

---

[197] *Id. See also* Sanger, *Confront and Conceal*, at 196. The Office of Tailored Access Operations (TAO) has additional units in San Antonio, Texas; Wahiawa, Hawaii; Fort Gordon, Georgia; Buckley Air Force Base, near Denver, Colorado; and a European liaison office in Darmstadt, Germany. The TAO's mission reportedly is "breaking into, manipulating and exploiting computer networks, making them hackers and civil servants in one." *Inside TAO: Documents Reveal Top NSA Hacking Unit*, 29 Dec. 2013, SPIEGEL ONLINE, *available at* http://www.sott.net/article/271802-Inside-TAO-Documents-reveal-top-NSA-hacking-unit.

[198] Sanger, *Confront and Conceal*, *supra* note 196, at 200.

[199] Nicole Perlroth, *Researchers Find Clues In Malware*, N.Y. TIMES, May 31, 2012, at B1.

[200] *Id.*; Thomas Erdbrink, *Iran Confirms Attack by Virus That Collects Information*, N.Y. TIMES, May 30, 2012, at A4; Hayley Tsukayama, *Malware is linked to Stuxnet, Flame*, WASH. POST, Aug. 10, 2012, at A3. Flame, first encountered in December 2007, first reported on in May 2012, reportedly can steal computer screen images, record e-mail and chats, monitor keystrokes, remotely turn on microphones, and take screen shots.

[201] John Markoff, *A Silent Attack, But Not A Subtle One*, N.Y. TIMES, Sept. 27, 2010, at A6.

[202] Sanger, *Confront and Conceal*, *supra* note 196, at xii.

Was Stuxnet a cyber attack? Is attribution satisfied? General Michael Hayden, former head of the National Security Agency (NSA), and before that the Central Intelligence Agency (CIA), says it was an attack on Iran by America. It resulted in the destruction of military or civilian objects. If similar results resulted from a kinetic strike, would it be an attack? Would self-defense have been justified under IHL? "Stuxnet was the first time a cyber activity could indisputably be labeled a cyber attack . . ."[203] The United States will find it difficult to complain, should another state mounts a similar attack against similar American targets.

"One big question is why its creators let the software spread widely, giving up so many of its secrets in the process."[204] The question is significant because "Stuxnet is now a model code for all to copy and modify to attack other industrial facilities."[205]

"In the end, the most important thing now publically known about Stuxnet is that Stuxnet is now publicly known."[206]

XVIII. Summary

If there is a circumstance in armed conflict that was unforeseen (and unforeseeable) by the 1949 Geneva Conventions, it is cyber warfare. Still, cyber warfare can be dealt with using traditional law of war tools, even though today's *jus ad bellum* cyber war questions can instantly ripen into *jus in bello* issues. Cyber attacks are not *per se* LOAC/IHL violations. They are simply another strategy or tactic of warfare, like armed drones and artillery barrages. When considering their effect or use, in many respects they may be thought of as if they were kinetic weapons.

How does one distinguish a hacker's cyber intrusion from an enemy state's cyber attack? The United States employs a results test. If the intrusion results in death or wounding, or the destruction or significant

---

[203] Brown, *supra* note 46, at 218.
[204] Markoff, *supra* note 201.
[205] Warrick, *supra* note 186. In late 2011 a "new program [to steal digital information] was written by programmers who must have had access to Stuxnet's source code, the original programming instructions." John Markoff, *New Worm by Creators of Stuxnet is Suspected*, N.Y. TIMES, Oct. 19, 2011, at B6.
[206] Gross, *supra* note 175, at 11.

damage of military or civilian objects, including data, an attack may be presumed, just as if the event involved kinetic weapons. Death, wounding, or destruction may be neither presumed nor potential; they must be actual. Similarly, at least in U.S. policy, an attack apparently may be presumed if a CNA targets any part of the critical national infrastructure, or a civilian computer network closely associated with the military, such as that of a major defense contractor's classified network—as long as death, wounding, or physical destruction follow. Although there is no international agreement to the U.S. position, such consequences, the United States considers, may be deemed an attack with armed force, giving rise to self-defense under UN Charter Article 51. Whether a CNA or a bombing attack, an attacker's choice of arms is immaterial.

Non-state armed opposition groups, such as al Qaeda and its off-shoots, are not known to have engaged in cyber attacks, yet. If past is prelude, a cyber attack will more likely be initiated by another state, or an individual or group whose actions will be attributable to a state; an international armed conflict in which the 1949 Geneva Conventions, in their entirety, and Additional Protocol I, will apply, along with customary international law. Should a non-state armed opposition group without state sponsorship mount an attack the circumstances would be examined to determine if it was an effort to initiate of an armed conflict, or "merely" a criminal act. In either case, the attack should be a matter for domestic law enforcement authorities. A cyber attack by non-state actors, difficult as that might be to carry out, would open the door to a common Article 3 conflict, with possible Additional Protocol II, and customary law, application, in addition to common Article 3 itself.

Responding to a confirmed cyber attack raises difficult issues. Immediate counter-attacks will likely consist of pre-programed automated cyber operations. "Such 'hack-backs' simply target the computers from which the intrusion originates."[207] But, to whom, or to what entity, should the attack be attributed? How can the requirement for distinction be satisfied by a counter-attacker at each stop on the attacker's electronic back-trail? How may a counter-strike be made proportional? In an international armed conflict a possible answer is belligerent reprisal. Because a reprisal need not be immediate, there can be a reasonable period of time to calibrate a response and assure the identity and lawfulness of the target. Reprisals are not problem-free, nor

[207] Droege, *supra* note 6, at 574.

are they universally agreed upon as a tactic. They are, however, a possible means of responding to a cyber attack that can avoid the most obvious pitfalls associated with an immediate response, electronic or kinetic.

Meanwhile, all states continue to strengthen their cyber defenses. For the United States, that includes presidential findings and policy directives, some no doubt secret, a *Defense Strategy* document, and CyberComm. China and Russia are most frequently portrayed as the dark knights of cyber warfare but the United States more than holds its own in regard to offensive cyber stratagems.

Are U.S. defensive capabilities equally well advanced? Numerous attacks against U.S. networks involve computer hardware compromised at point of manufacture.

> Software is most of the problem. We have to find a way to write software which has many fewer errors and which is more secure . . . . Hackers get in where they don't belong, most often because they have obtained 'root' or administrator status, through a glitch they have discovered in the software.[208]

Threats from within, personnel with legitimate access to secrets, government workers like Edward Snowden, willing to provide information to a nation's enemies, will always be a threat to cyber secrets.

Still, so far, no one is known to have died from a cyber attack anywhere in the world. A long-time cyber expert in the military and civilian communities writes:

> The most meaningful cyber conflicts rarely occur at the "speed of light" or "network speed. . . . ." [Cyber] conflicts are typically campaigns that encompass weeks, months, or years of hostile contact between adversaries, just as in traditional warfare . . . . While some attacks are technically difficult to attribute, it is usually a straightforward matter to determine the nation responsible, since the conflict takes place during an on-

[208] CLARKE & KNAKE, *supra* note 13, at 173.

> going geo-political crisis . . . . Despite early fears that nations would strike at each other using surprise . . . there is no evidence that such conflicts have occurred. Nations seem to be willing to launch significant cyber assaults during larger crises, but not out of the blue . . . .[209]

Reassuring words. There need be but one cyber Pearl Harbor to prove them wrong, however. In any event, much will have occurred between the writing of these words and their reading to materially change the terrain of cyber warfare.

[209] Healey, *supra* note 15, at 21–23.