Pace International Law Review

Volume 28
Issue 1 *Spring 2016*

Article 6

April 2016

Anonymous Armies: Modern "Cyber-Combatants" and Their Prospective Rights Under International Humanitarian Law

Jake B. Sher
Pace University School of Law

COMMENT
ANONYMOUS ARMIES: MODERN "CYBER-COMBATANTS" AND THEIR PROSPECTIVE RIGHTS UNDER INTERNATIONAL HUMANITARIAN LAW

Jake B. Sher*

* J.D. Candidate, Pace University School of Law. I am indebted to Professors Alexander Greenawalt, Thomas McDonnell, and Peter Widulski for their thoughtful insights and suggestions, and to the Articles Editors and Associates of the Pace International Law Review (classes of 2016 and 2017), who tirelessly applied both Bluebook and practical knowledge to perfecting this work. My teammates in the 2016 Jessup International Moot Court Competition (Katherine Ehrlich, Wilfredo Lopez, and Michael Pesin-Virovets), which dealt with some of the issues of international law encompassed in this work, also have my unabashed thanks for permitting me the honor of joining their ranks.

I. Introduction

"Subtle and insubstantial, the expert leaves no trace; divinely mysterious, he is inaudible. Thus he is master of his enemy's fate." [1]

In the theater of war, the "Internet Age" has shifted the scenery. The advent and global expansion of this new medium may prove to be the fastest and most powerful technological revolution in humanity's history.[2] It has created a global atmosphere in flux, "characterized by interdependence, uncertainty, complexity, and continual change."[3] Because cyberspace passes electronically through geopolitical and natural boundaries, electronic payloads 'launched' into cyberspace enjoy instantaneous deployment.[4] Moreover, the threats posed by world conflicts in cyberspace are an imminent reality; with the advent of "the internet of things," hackers can remotely control connected devices, including motor vehicles traveling at full speed.[5] It is plausible that a state or group engaged in a cyber

---

[1] SUN TZU, THE ART OF WAR 97 (Samuel B. Griffith trans., 1971).

[2] *See* Nils Melzer, *Cyberwarfare and International Law* 3 (UNIDIR Resources 2011), http://www.unidir.org/files/publications/pdfs/cyberwarfare-and-international-law-382.pdf ("[T]he advent and global expansion of the Internet may prove to become the fastest and most powerful technological revolution in the history of mankind.").

[3] U.S. DEP'T OF DEF., THE NATIONAL MILITARY STRATEGY FOR CYBERSPACE OPERATIONS 1 (2006).

[4] *See* Melzer, *supra* note 2, at 5.

[5] *See* Mark Pesce, *The Internet of things is great until it blows up your house*, THE REGISTER (Apr. 17, 2015), http://www.theregister.co.uk/2015/04/17/the_internet_of_things_is_great_until_it_blows_up_your_house/ (noting that with 33 billion connected devices projected by 2020, a hacked connected device can be problematic, because "*33 billion connected devices means 33 billion attack surfaces*, each with their own exploits, zero day attacks, weaknesses and vulnerabilities."); *see also* Andy Greenberg, *Hackers Remotely Kill a Jeep on the Highway—With Me in* it, WIRED (Jul. 21, 2015, 6:00 AM), http://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/ (reporting on a test performed by hackers near St. Louis on a motor vehicle traveling at 70 m.p.h.: "As the two hackers remotely toyed with the air-conditioning, radio, and windshield wipers, I mentally congratulated myself on my courage under pressure. That's when they cut the transmission."). Some experts suggest that any number of otherwise benign devices are susceptible to hacking. *See*, *e.g.*, Brian Wheeler, *Toys*

conflict could remotely light up tens of thousands of ovens or furnaces in a military base or an urban center, effectively destroying a target without firing a missile or mobilizing a warplane.[6] In now-declassified documents, the United States military has characterized a new dimension in warfare: "The Cyberspace Domain," which may likely extend into outer space.[7] The U.S. military defines this domain as "[c]haracterized by the use of electronics and the electromagnetic spectrum to store, modify, and exchange data via networked systems and associated physical infrastructures."[8]

A recently suggested definition of a "cyber-attack" refers to it as "[a]ny action taken to undermine the functions of a computer network for a political or national security purpose."[9] The definition is hardly a settled one, however; many States and scholars have defined "cyber-attack" more broadly or narrowly.[10]

---

could be used as spying devices, MPs told, BBC News (Dec. 9, 2015), http://www.bbc.com/news/uk-politics-35043521 (noting experts' concerns about "smart toys" given that "anything that connected to the internet could 'in theory' be hacked into," including driverless cars or household appliances).

[6] *See* Pesce, *supra* note 5 (noting that "when you go away on a fortnight's holidays, and someone hacks into your oven, turns the gas on, waits 36 hours, then lights the pilot, well, then you've got a problem. A much worse problem if you happen to be at home at the time. Your oven could gas you in your sleep.").

[7] *See* Melzer, *supra* note 2, at 3 (positing the existence of the "Cyberspace Domain"); Chris Bowlby, *Could a war in space really happen?*, BBC NEWS (Dec. 19, 2015), http://www.bbc.com/news/magazine-35130478 (noting that "[c]yber attacks on military satellites are another concern" and that "[t]here are now more incentives for a potential adversary, such as China, to attack satellites or disable them as part of a conventional conflict … they know full well that space capabilities are at the core of the US's ability to project power.").

[8] *Id.*

[9] Oona A. Hathaway et al., *The Law of Cyber-Attack*, 100 CALIF. L. REV. 817, 826 (2012).

[10] *See, e.g.*, Reese Nguyen, Comment, *Navigating Jus Ad Bellum in the Age of Cyber Warfare*, 101 CAL. L. REV. 1079, 1088 (2013) ("rather than defining 'cyber attack' by the *object* of attack, it makes more sense to define the term by the *instrument* of attack. Under this reading, the term 'cyber attack' may describe the use of cyber operations as a weapon or form of attack, with the word 'cyber' characterizing the mode of assault. Just as an 'air assault' denotes a military attack using aircraft, or as an 'amphibious assault' denotes an assault by land and sea executed on a hostile shore, a 'cyber attack' can denote an attack executed by means of a computer or computer network. Here, a cyber attack is an *instrument* or *method* of attack, a *weapon* or *capa-*

While "the notion of 'armed attack' necessarily implies the use of a weapon,"[11] the members of armed forces seldom effectuate cyber-attacks exclusively in cyber operations.[12] In October of 2014, hackers thought to be working for the Russian government breached White House computer networks, resulting in temporary service disruptions.[13] Earlier in 2014, a group using the moniker "Lizard Squad" launched a series of denial-of-service attacks against the Vatican and several online gaming sites;[14] their acts culminated in the 'tweeting' of a false bomb threat, resulting in the diversion of American Airlines Flight 362, traveling from Dallas to San Diego.[15] Shortly thereafter, the group claimed that it took its actions in support

bility that is used to effectuate a particular objective."); Phillip Pool, *War of the Cyber World: The Law of Cyber Warfare*, 47 INT'L LAW. 299, 309 (2013) (noting the broad definition proffered in the Shanghai Cooperation, an agreement signed by Russia, China, and other central Asian countries, defining cyber warfare more expansively by including "information war," meaning a "mass psychological brainwashing to destabilize society and state, as well as to force the state to take decisions in the interest of an opposing party."); Erki Kodar, *Applying the Law of Armed Conflict to Cyber Attacks: From the Martens Clause to Additional Protocol I*, 15 ENDC PROCEEDINGS 107, 107-08 (2012), http://www.ksk.edu.ee/wp-content/uploads/2012/12/KVUOA_Toimetised_15_5_Kodar.pdf (noting the U.S. Department of Defense's narrower definition, "actions taken through the use of computer networks to disrupt, deny, degrade or destroy information resident in computers and computer networks, or the computers and the networks themselves.").

[11] Melzer, *supra* note 2, at 13.

[12] Kodar, *supra* note 10, at 124.

[13] Ellen Nakashima, *Hackers breach some White House computers*, WASH. POST (Oct. 28, 2014), http://www.washingtonpost.com/world/national-security/hackers-breach-some-white-house-computers/2014/10/28/2ddf2fa0-5ef7-11e4-91f7-5d89b5e8c251_story.html?utm_source=Sailthru&utm_medium=email&utm_term=*Morning%20Brief&utm_campaign=2014_MorningBrief-%20RD%20PROMO10.29.14 (noting, in addition, a previous operation termed "Buckshot Yankee," allegedly perpetrated by the Russian intelligence service, that breached U.S. military classified networks in 2008).

[14] Alyssa Newcomb, *Lizard Squad: Who Is the Group Claiming Responsibility for High Profile Hacks?* ABC NEWS (Aug. 26, 2014, 1:38 PM), http://abcnews.go.com/Technology/lizard-squad-group-claiming-responsibility-high-profile-hacks/story?id=25129458.

[15] Hayley Tsukayama, *Sony says no customer information was taken in online attack*, WASH. POST (Aug. 25, 2014), http://www.washingtonpost.com/blogs/the-switch/wp/2014/08/25/sony-says-no-customer-information-was-taken-in-online-attack/.

of the Islamic State in Iraq and Syria (ISIS or ISIL).[16] While any direct relationship between Lizard Squad and ISIL is highly unlikely,[17] their attack is not the only one to have planted the ISIL flag in cyberspace. In February of 2015, a group declaring support for ISIL jihadists hacked Newsweek's twitter account, releasing several military documents claimed to be of a classified nature.[18] Notably, ISIL regularly utilizes online platforms to recruit fighters,[19] and over time, cyber operations by the group or its supporters have gotten bolder. In 2015, a dedicated cyber unit identifying as the "CyberCaliphate" hacked the Twitter account of the United States Central Command.[20] Another group, the "ISIS Cyber Army," targeted fifty-one American websites, defacing them with the ISIL flag.[21]

In December of 2014, the North Korean government

---

[16] Lizard Squad (@Lizard Squad), TWITTER, (Aug. 24, 2014, 8:03 AM), https://twitter.com/LizardSquad/status/503558145784815619 (last visited Aug. 27, 2014, 7:01 pm) ("Today we planted the ISIS flag on @Sony's servers #ISIS #jihad") (Twitter has since suspended this particular Lizard Squad Account).

[17] *See* Nakashima, *supra* note 13 (noting, while unable to confirm Russia's responsibility for the attack, that sources suggested "the nature of the target is consistent with a state-sponsored campaign."); Tsukayama, *supra* note 15 (noting that "there was no official information" on whether a substantiated connection between Lizard Squad and ISIS existed). However, at least some Lizard Squad members likely have anti-western leanings in tandem with those espoused by ISIS. *See* Neha Singh, US officials start probe as hackers claim leaking data about FBI employees, ibtimes.co.in (Feb. 9, 2016 16:06 PM IST), http://m.ibtimes.co.in/us-officials-start-probe-hackers-claim-leaking-data-about-fbi-employees-666286 (noting that a former member of Lizard Squad is reported to have had involvement in the leaking of some 29,000 FBI and DHS employees' personal information; reporting also that "before allegedly hacking into the data of FBI and DHS employees, the hackers tweeted, 'When will the US government reali[z]e we won't stop until they cut relations with Israel.'").

[18] *Newsweek is latest victim of the 'Cybercaliphate'*, I24 NEWS (Feb. 10, 2015: 9:45 PM), http://www.i24news.tv/en/news/technology/60697-150210-newsweek-is-latest-victim-of-the-cybercaliphate.

[19] *See*, *e.g.*, *ISIS recruits fighters through powerful online campaign*, CBS NEWS (Aug. 29, 2014: 6:55 AM), http://www.cbsnews.com/news/isis-uses-social-media-to-recruit-western-allies/.

[20] Michael Martinez, *Cyberwar: CyberCaliphate targets U.S. military spouses; Anonymous hits ISIS*, CNN (last updated Feb. 11, 2015, 7:50 AM), http://www.cnn.com/2015/02/10/us/isis-cybercaliphate-attacks-cyber-battles/.

[21] *ISIS Cyber Unit Announces More Hacks*, ANTI-DEFAMATION LEAGUE BLOG (Mar. 26, 2015), http://blog.adl.org/international/isis-cyber-unit-announces-more-hacks.

matched these groups' opening salvo tenfold by hacking into Sony Pictures' networks as retaliation for the film company's intended release of *The Interview*,[22] a film depicting the killing of the North Korean leader Kim Jong-un.[23] The rogue state's hackers damaged Sony Pictures' network infrastructure so badly that Sony workers had to revert to using fax machines to communicate.[24] The White House's speedy attribution of the Sony Pictures hack to agents of the North Korean government was only possible due to metadata and other evidence gathered by the United States government beginning in 2010, when the National Security Agency used "early warning radar" software to monitor North Korea's activities.[25] The devastating effect on Sony Pictures from that relatively crude attack led the company's CEO to describe the hack as "the worst cyberattack in U.S. history."[26] While that claim may be dubious given the shortcomings of Sony's own network and the international standard for a cyber-attack, the operation was unprecedented in that a sovereign state leveraged the attack in order to achieve a very non-cyber aim, namely, the cancellation of a film release.[27] In response to this and other attacks like it in recent years, the Obama Administration announced the creation of a new agency, the Cyber Threat Intelligence Integration Center (CTIIC), modeled on the National Counterterrorism Center, at the Wilson Center in Washington.[28]

---

[22] THE INTERVIEW (Sony Pictures 2014).

[23] Michael Cieply, *'The Interview' Brings In $15 Million on Web*, N.Y. TIMES (Dec. 28, 2014), http://www.nytimes.com/2014/12/29/business/media/the-interview-comes-to-itunes-store.html.

[24] Aarti Shahani, *Is Sony Hack Really 'The Worst' In U.S. History, As CEO Claims?* NPR.ORG (Dec. 23, 2014, 5:05 AM), http://www.npr.org/blogs/alltechconsidered/2014/12/23/372603286/is-sony-hack-really-the-worst-in-u-s-history-as-ceo-claims.

[25] David E. Sanger & Martin Fackler, *N.S.A. Breached North Korean Networks Before Sony Attack, Officials Say*, N.Y. TIMES (Jan. 18, 2015), http://www.nytimes.com/2015/01/19/world/asia/nsa-tapped-into-north-korean-networks-before-sony-attack-officials-say.html.

[26] Shahani, *supra* note 24.

[27] Roy Isacowitz, *Despite all the publicity, the Sony hack was small-time; much worse is yet to come*, HAARETZ (Dec. 25, 2014, 8:24 PM), http://www.haaretz.com/news/world/.premium-1.633813.

[28] *Obama administration announces new cybersecurity agency*, FOX NEWS (Feb. 10, 2015), http://www.foxnews.com/politics/2015/02/10/obama-

Regardless of whether victims or independent observers successfully identify the source of a cyber-attack, the effects of such an attack are pervasive, insidious, and borderless. Those that perpetrate cyber-attacks may do so *from* virtually anywhere with Internet access, and may reach *to* virtually anywhere with Internet access. Belligerent states increasingly employ private contractors and civilian employees in a variety of functions, including cyber operations roles.[29] In such an environment, where the 'fog of war' pervades every bit and byte of the virtual battlefield, the international community must revisit the definition of 'combatant' as applied to cyber-attacks if it wishes to ensure continued global peace and security.

Cyber-attacks take many forms, only some of which are applicable to the law of war.[30] This Comment discusses only those attacks sponsored by a government or non-state entity that have the goal of affecting morale or gaining political advantage, or those attacks amounting to tactical strikes on state or civilian infrastructure. In that vein, this Comment proposes the adoption of a new legal framework for determining the threshold that marks a participant in such a cyber-attack as a "cyber-combatant" by adapting the framework set by the Geneva Conventions and existing custom. This definition should encompass cyber-attacks perpetrated by states, unrecognized states, and non-state groups. It should set the rules of engagement for cyber-attacks and operations conducted for political advantage, morale boost, and tactical purposes.

Whether they act on the orders or in support of States or non-state groups, those perpetrating cyber-attacks that have material effects upon the morale or infrastructure of a sovereign nation during armed conflict should be treated as "combatants" for purposes of international law, and the legality of

---

administration-to-announce-new-cybersecurity-agency/.

[29] Melzer, *supra* note 2, at 34.

[30] *See id.* at 22 ("[S]ecurity threats emanating from cyberspace which do not reach the threshold of armed conflict can be described as 'cyber crime', 'cyber operations,' 'cyber policing' or, where appropriate, as 'cyberterrorism' or 'cyber piracy', but should not be referred to with terminology inviting doubt and uncertainty as to the applicability of the law of armed conflict."). This Comment will approach issues of attacks related to cyber-warfare and, to a lesser extent, cyber-terrorism, as applied to legal issues in direct relation to international humanitarian law.

their actions should be defined. Because the standard governing what constitutes a lawful combatant under any reasonable reading of the Geneva Conventions[31] is muddled as applied to combatants in cyber-warfare as presently conducted, this paper takes the position that under present custom, cyber-combatants may likely be effectively considered illegal combatants under International Law.

Part II of this Comment provides a framework for defining "cyber-combatants," reviewing the traditionally accepted definition of "combatants" under the Geneva Conventions and customary international law as restated through the Tallinn Manual on the International Law Applicable to Cyber Warfare.[32] Part III explores the alleged cyber-operations of sovereign States, including Israel's C4i Cyber Warfare Unit and The United States' USCYBERCOM and its sister agencies, some or all of which may have been responsible for the Stuxnet attack on Iran; Russia's coordinated cyber-attacks perpetrated during its war with Georgia in 2008 and in the conflict in Ukraine in 2014 and 2015; and China's PLA Unit 61398. Part IV introduces the unique problem posed by cyber-attacks perpetrated by agents of unrecognized states and organized terrorist groups such as Al-Qaeda and ISIS. Finally, Part V concludes by proposing alternative definitions for cyber-attacks, and consequentially, cyber-combatants.

II. The present status of the Law of Cyber-Warfare

---

[31] Geneva Convention for the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field, Aug. 12, 1949, (entered into force Feb. 2, 1956) 6 U.S.T. 3114, T.I.A.S. No. 3362, 75 U.N.T.S. 31 [hereinafter First Geneva Convention]; Geneva Convention for the Amelioration of the Condition of the Wounded, Sick and Shipwrecked Members of Armed Forces at Sea, Aug. 12, 1949, (entered into force Feb. 2, 1956) 6 U.S.T 3217, T.I.A.S. No. 3363, 75 U.N.T.S. 31 [hereinafter Second Geneva Convention]; Geneva Convention (III) Relative to the Treatment of Prisoners of War, Aug. 12, 1949, (entered into force Feb. 2, 1956) 6 U.S.T. 3316, T.I.A.S. No. 3364, 75 U.N.T.S. 135, https://www.icrc.org/ihl/INTRO/375?OpenDocument [hereinafter Third Geneva Convention]; Geneva Convention Relative to the Protection of Civilian Persons in Time of War, Aug. 12, 1949, (entered into force Feb. 2, 1956) 6 U.S.T. 3516, T.I.A.S. No. 3365, 75 U.N.T.S. 287 [hereinafter Fourth Geneva Convention].

[32] TALLINN MANUAL ON THE INTERNATIONAL LAW APPLICABLE TO CYBER WARFARE (Michael N. Schmitt, ed., 2013).

International treaty and custom governing cyber-warfare are in a state of evolution.[33] At present, broad international dialogue on the interpretation and application of existing rules and principles of international law to cyber-warfare are virtually non-existent.[34] The activities that would define the nature and character of 'cyber-combatants' thus find their definition in existing international humanitarian law (*jus in bello*), which "sets forth the rules of the game; the rules under which hostilities can be carried out."[35] These rules derive primarily from the Hague Convention of 1907,[36] the four Geneva Conventions of 1949,[37] and the Additional Protocols to the Geneva Conventions of 1977.[38] These treaties, and the custom derived from them, supply the predominant body of provisions related to *jus in bello*.[39]

Because the Third Geneva Convention is now widely accepted as customary international law,[40] it defines the playing

---

[33] *See generally* Bradley Raboin, *Corresponding Evolution: International Law and the Emergence of Cyber Warfare*, 31 J. NAT'L ASS'N ADMIN. L. JUDICIARY 602 (2011).

[34] *See* Melzer, *supra* note 2, at 4.

[35] Thomas Michael McDonnell, *Sow What You Reap? Using Predator and Reaper Drones to Carry Out Assassinations or Targeted Killings of Suspected Islamic Terrorists*, 44 GEO. WASH. INT'L L. REV. 243, 270 (2012).

[36] Convention (IV) respecting the Laws and Customs of War on Land and its annex: Regulations concerning the Laws and Customs of War on Land, Convention with Respect to the Laws and Customs of War on Land (Hague Convention (IV)), Annex, art. 1, Oct. 18, 1907, 36 Stat. 2277, T.S. No. 539 [hereinafter Hague Regulations], https://www.icrc.org/ihl/INTRO/195.

[37] *See generally supra* note 31.

[38] Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflicts (Protocol I) art. 51(2), June 8, 1977, 1125 U.N.T.S. 3 [hereinafter A.P. I]; Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of Non-international Armed Conflicts (Protocol II), June 8, 1977, 1125 U.N.T.S. 609 [hereinafter A.P. II].

[39] *See* McDonnell, *supra* note 35, at 270; ICRC, *What Is International Humanitarian Law?*, at 1 (July 2004), https://www.icrc.org/eng/assets/files/other/what_is_ihl.pdf.

[40] *See* Third Geneva Convention, *supra* note 31 (encompassing 196 State Parties); *Kadic v. Karadzic*, 70 F.3d 232, 242 (2d Cir. 1995) (noting, at that time, that the four Geneva Conventions "have been ratified by more than 180 nations, including the United States."); *see also* Press Release, ICRC, Geneva Conventions of 1949 achieve universal acceptance, *ICRC Press Release* 06/96, (Aug. 21, 2006), (acknowledging that "[t]he recent accessions by the Republic of Nauru and the Republic of Montenegro to the 1949 Geneva Conventions," resulting in the universal acceptance of the conventions, and remind-

field for States in armed conflict involving two or more States.[41] Article 4 of that Convention defines "combatants" as follows:

1. Members of the armed forces of a Party to the conflict, as well as members of militias or volunteer corps forming part of such forces.
2. Members of other militias and members of other volunteer corps, including those of organized resistance movements, belonging to a Party to the conflict and operating in or outside their own territory, even if this territory is occupied provided that such militias or volunteer corps, including such organized resistance movements, fulfill the following conditions:
    a. that of being commanded by a person responsible for his subordinates;
    b. that of having a fixed distinctive sign recognizable at a distance;
    c. that of carrying arms openly;
    d. that of conducting their operations in accordance with the laws and customs of war.
3. Members of regular armed forces who profess allegiance to a government or an authority not recognized by the Detaining Power . . ."[42]

The Third Geneva Convention imposed these conditions as requirements for "militias and corps of volunteers not forming part of the regular armed forces, thus solving one of the most difficult questions—that of 'partisans.'[43] The drafting history of

---

ing "all belligerents of their obligation to abide by the laws of war"); Mike Sanderson, *The Syrian Crisis and the Principle of Non-Refoulement*, 89 INT'L L. STUD. 776, 796 (2013) (stating that "all four conventions are now widely accepted to have passed in their entirety into customary international law"); INTERNATIONAL LAW 814-16 (Malcolm D. Evans ed., 3d ed. 2010); Partial Award on Prisoners of War, Eritrea's Claim (Eri. v. Eth.) 42 I.L.M. 1056, 1083 (Eri.-Eth. Claims Comm'n 2003).

[41] *See* Third Geneva Convention, *supra* note 31, art. 2.

[42] *Id*. at art. 4.

[43] *See* Int'l Comm. of the Red Cross, Commentary, III Geneva Convention Relative to the Treatment of Prisoners of War of 12 August 1949, 60 (Jean Pictet, ed., 1960) [hereinafter Commentary on Third Geneva Convention] (noting that the drafters of Article 4 codified it to resolve the issue posed by partisan fighters: "During the Second World War, certain States refused to recognize as belligerents combatant units which professed allegiance to a Government or authority which these States did not recognize.").

the Convention further reveals the flexibility inherent in each of the requirements.[44] Section (a), which requires the condition of command, did not necessarily require a military officer to fill the role; the individual asserting command could be a civilian, though his competence would be assessed in the same way as that of a military commander.[45] The drafting history on Section (b), which requires "a fixed distinctive sign recognizable at a distance," specifies that its distinctive nature requires that "the sign must be the same for all the members of any one resistance organization, and must be used only by that organization," but is more nebulous with respect to the issue of recognizance at a distance, leaving it "open to interpretation."[46] Likewise, the language "carrying arms openly" in Section (c) acknowledged that the arms need not be visible and could take many forms.[47] Finally, the term "the laws and customs of war" in Section (d) was purposely kept vague by the Convention's drafters.[48] It is apparent from the flexibility of these terms that the drafters' intent was to allow for renewed teleological interpretation of the Geneva Conventions, because advances in technology and socio-political norms would necessarily change the nature and dynamics of the battlefield.[49]

---

[44] *See id.* at 59-61.

[45] *Id.* at 59.

[46] *Id.* at 60; *see also* TALLINN MANUAL ON THE INTERNATIONAL LAW APPLICABLE TO CYBER WARFARE, *supra* note 32, at 99 (noting conflict as to what would meet the standard of a 'fixed distinctive sign' in cyber warfare; some experts noted that "the requirement only applies in circumstances in which the failure to have a fixed distinctive sign might reasonably cause an attacker to be unable to distinguish between civilians and combatants, thus placing civilians at greater risk of mistaken attack").

[47] Commentary on Third Geneva Convention, *supra* note 43, at 61 (noting that "openly" does not mean "visibly" or "ostensibly," as "[s]urprise is a factor in any war operation . . ." In regards to weaponry, noting that "[t]he enemy must be able to recognize partisans as combatants in the same way as members of regular armed forces, whatever their weapons.").

[48] *Id.* (noting that "[T]he concept of the laws and customs of war is rather vague and subject to variation as the forms of war evolve.").

[49] *See* Neil McDonald & Scott Sullivan, *Rational Interpretation in Irrational Times: The Third Geneva Convention and the "War on Terror"*, 44 HARV. INT'L L.J. 301, 306 (2003) (advocating a teleological approach to the Third Geneva Convention in light of its drafting history: "[b]ecause such narrowing language was rejected, application of the provisions should be read broadly."); *id.* at 303 ("[A] state's freedom of interpretation within the Geneva Convention treaty regime is relatively broad, but is subject to general assent

With the flexibility of a teleological approach in mind, it is worthwhile to review emerging custom in the law of cyber-warfare. Because of its comprehensive nature, it is worthwhile to begin such a survey through the lens of NATO's Tallinn Manual on the International Law of Cyber Warfare.[50] The rules proffered in the Tallinn Manual "reflect consensus among . . . Experts as to the applicable *lex lata*, that is, the law currently governing cyber conflict."[51] The international legal scholars who published the Tallinn Manual did so to address concerns similar to those of the ICRC's Interpretive Guidance to the Geneva Conventions; in applying International Law to the Information Age, these scholars noted that many international customs developed prior to the advent of the computer.[52] Due to their intended status as an attempted 'restatement' of current custom in both the *jus ad bellum* and *jus in bello* of cyber warfare, however, the rules in the Tallinn Manual do not proffer to "set forth *lex ferenda*, best practice, or preferred policy."[53] Thus, while it acknowledges that "the scope and manner of international law's applicability to cyber operations . . . has remained unsettled since their advent,"[54] and that "publicly available expressions of *opinio juris*" surrounding the issue "are sparse,"[55] the Tallinn Manual may nevertheless provide as valuable an insight as any into the evolving custom that currently governs 'the Law of Cyber-War.'[56]

---

from the international community, which may hinge on considerations of both international law and politics."); Orna Ben-Naftali & Sean S. Gleichgevitch, *Missing in Legal Action: Lebanese Hostages in Israel*, 41 HARV. INT'L L.J. 185, 248 (2000) (advocating for a teleological approach to the Third Geneva Convention in the context of Lebanese guerilla combatants; arguing that the complementary nature of the Geneva Conventions "indicates the primary purpose of the Laws of War: to ensure that all people, combatants and civilians alike, who find themselves involved in an armed conflict, are not bereft of status and the protection their status bestows.").

[50] TALLINN MANUAL ON THE INTERNATIONAL LAW APPLICABLE TO CYBER WARFARE, *supra* note 32.

[51] *Id.* at 5.

[52] *See* Collin Allan, Note, *Direct Participation in Hostilities from Cyberspace*, 54 VA. J. INT'L L. 173, 175 (2013).

[53] TALLINN MANUAL ON THE INTERNATIONAL LAW APPLICABLE TO CYBER WARFARE, *supra* note 32, at 5.

[54] *Id.* at 3.

[55] *Id.* at 5.

[56] *See* Manny Halberstam, Note, *Hacking Back: Reevaluating the Legali-*

Rule 30 of the Tallinn Manual defines a "Cyber Attack" as "a cyber operation, whether offensive or defensive, that is reasonably expected to cause injury or death to persons or damage or destruction to objects."[57] Note 2 accompanying the definition narrows it, stating that "[n]on-violent operation, such as psychological cyber operations or cyber espionage, do not qualify as attacks."[58] Note 3 specifies further that generally, in determining whether a cyber operation is an 'attack,' the consequences of the operation are material to the determination; the nature of the operation, however, is not.[59] Note 8 further suggests that some attacks that do not cause any physical damage may constitute 'cyber attacks' under Rule 30 in narrow circumstances:

> Article 51(2) of Additional Protocol I [to the Geneva Conventions] prohibits 'acts or threats of violence the primary purpose of which is to spread terror among the civilian population.' Since terror is a psychological condition resulting in mental suffering, inclusion of such suffering in this Rule is supportable through analogy.[60]

In addition, intercepted attacks nevertheless qualify as 'cyber attacks' under the Rule "if, absent such defenses, it would have been likely to cause the requisite consequences."[61] Thus, a cyber attack need not be successful to be classified as such.

---

ty of Retaliatory Cyberattacks, 46 GEO. WASH. INT'L L. REV. 199, 205 n. 42 (2013) (noting that "[a]lthough the manual is not binding, its influence as a persuasive secondary source will be substantial."); Harry P. Koulos, Note, *Attacked by Our Own Government: Does the War Powers Resolution or the Law of Armed Conflict Limit Cyber Strikes Against Social Media Companies?*, 11 GEO. J.L. & PUB. POL'Y 705, 736 (2013) (acknowledging the existing difficulty in definitively concluding the existence of customary norms in cyber warfare, yet adamant that "the Tallinn Manual Experts were unanimous in their conclusion that the current law of armed conflict applies to cyber operations."); *see also* Michael N. Schmitt, *International Law in Cyberspace: The Koh Speech and Tallinn Manual Juxtaposed*, 54 HARV. INT'L L.J. 13, 15-16 (2012) (noting that the United States has taken "precisely the same position" as the Tallinn Manual on the applicability of the law of armed conflict to cyber operations).

[57] TALLINN MANUAL ON THE INTERNATIONAL LAW APPLICABLE TO CYBER WARFARE, *supra* note 32, at 106.

[58] *Id.*

[59] *Id.* at 107.

[60] *Id.* at 108.

[61] *Id.* at 110.

Rule 5 declares a State's responsibility for cyber infrastructure located within its territory or under its exclusive governmental control.[62] Rule 7 clarifies, however, that attribution of an attack to a State may not be predicated upon "[t]he mere fact" that a cyber operation's place of launch or origination is within "governmental cyber infrastructure."[63] Presumably, once an attack meets this high threshold required for proper attribution, Rule 9 permits the State injured by the intentionally wrongful act of another state to resort to "proportionate countermeasures, including cyber countermeasures, against the responsible State."[64] As in the Law of War from which it derives,[65] countermeasures taken in self-defense are "not limited to a State's own territory."[66]

Rule 20 provides that "[c]yber operations executed in the context of an armed conflict are subject to the law of armed conflict."[67] The characterization of either "hostilities" under Rule 22 or "protracted armed violence" under Rule 23 ". . . may include or be limited to cyber operations," as an international armed conflict.[68] In addition, such characterization may apply in a non-international armed conflict.[69] Under Note 16 to Rule 22, "so long as the armed and international criteria have been met, an international armed conflict exists."[70] As regards a non-international armed conflict under Rule 23, Note 11 states that "[f]or a non-international armed conflict to exist, there must be at least one non-State organized armed group involved

---

[62] TALLINN MANUAL ON THE INTERNATIONAL LAW APPLICABLE TO CYBER WARFARE, *supra* note 32, at 26.

[63] *Id.* at 34.

[64] *Id.* at 36.

[65] *See* U.N. Charter art. 51 ("Nothing in the present Charter shall impair the inherent right of individual or collective self-defen[s]e if an armed attack occurs against a Member of the United Nations, until the Security Council has taken measures necessary to maintain international peace and security.").

[66] TALLINN MANUAL ON THE INTERNATIONAL LAW APPLICABLE TO CYBER WARFARE, *supra* note 32, at 36.

[67] *Id.* at 75.

[68] *Id.* at 79; *see also id.* at 84 (explaining, at cmt. 15, that "The International Group of Experts unanimously concluded that cyber operations alone might have the potential to cross the threshold of international armed conflict.").

[69] *Id.* at 84.

[70] *Id.*

in the hostilities. Such a group is 'armed' if it has the capacity of undertaking cyber attacks" under Rule 30.[71] This standard appears to operate under a broad canon of construction, as a group's 'armed' nature may be predicated solely upon its possession of computer hardware and software sufficient to render it capable of executing a cyber-attack.[72] This means that the possession of firearms and other kinetic weaponry is not a predicate requirement for a group to be 'armed' under the Tallinn Manual, which has implications with respect to Article 4, section 2, subsection c of the Third Geneva Convention.[73] Note 3 to Rule 22 notes that the question of whether the actions of a non-state may be attributed to another state such that the conflict is international was explicitly addressed in *Prosecutor v. Tadic*:

> [c]ontrol by a State over subordinate armed forces or militias or paramilitary units may be of an overall character . . . This requirement, however, does not go so far as to include the issuing of specific orders by the state, or its direction of each individual operation. Under international law it is by no means necessary that the controlling authorities should plan all the operations of the units dependent on them, choose their targets, or give specific instructions concerning the conduct of military operations and any violations of international humanitarian law. The control required by international law may be deemed to exist when a State (or, in the context of an armed conflict, the Party to the conflict) has a role in organising, coordinating or planning the military actions of the military group, in addition to financing, training and equipping or providing operational support to that group.[74]

---

[71] *See* TALLINN MANUAL ON THE INTERNATIONAL LAW APPLICABLE TO CYBER WARFARE, *supra* note 32, at 88.

[72] *See* Steven G. Bradbury, *The Developing Legal Framework for Defensive and Offensive Cyber Operations*, 2 HARV. NAT'L SEC. J. 591, 607 (2011) (noting that under customary international law, "if the cyber intrusion inflicts significant physical destruction or loss of life by causing the failure of critical infrastructure, like a dam or water supply system, then it obviously would constitute an armed attack under the law of war and would justify a full military response if it could be attributed to a foreign power.").

[73] Third Geneva Convention, *supra* note 31, at art. 4(2)(c) ("that of carrying arms openly").

[74] *See* TALLINN MANUAL ON THE INTERNATIONAL LAW APPLICABLE TO CYBER WARFARE, *supra* note 32, at 80, citing *Prosecutor v. Tadic*, Case No. IT-94-1-A, Appeals Chamber Judgment, ¶ 137 (Appeals Chamber, ICTY, Jul. 15,

In addition, Rule 24 holds "[c]ommanders and other superiors" to be "criminally responsible for "ordering cyber operations that constitute war crimes,"[75] and "[m]ercenaries involved in cyber operations do not enjoy combatant immunity or prisoner of war status" under Rule 28.[76] These Rules clarify that international custom contemplates attacks initiated in cyberspace by state or non-state actors, and that such attacks have the potential to be 'armed' in nature.

There are further complications, however, because navigating bits and bytes in effectuating a cyber-attack can create similar collateral consequences to dropping a bomb, but the effects are different. While the intended target of a party dropping a bomb may generally be extrapolated from the fallout surrounding the intended target, the intent of a party making a keystroke may have unintended consequences that are far-reaching.[77] The result is that the intent of the perpetrator with respect to such unintended consequences can be less clear, particularly if the cyber-attack causes sporadic or unforeseen damage to civilian targets.[78] In such a situation, the principle of proportionality is likely to be of significant importance in determining whether a violation of the *jus in bello* has resulted.[79] "[P]roportionality applies to the effects of the weapons on both noncombatants and combatants alike," and enjoins combatants from directly attacking life and property of noncombatants, "although legal and moral attacks directed against proper targets may affect them."[80]

1999).

[75] TALLINN MANUAL ON THE INTERNATIONAL LAW APPLICABLE TO CYBER WARFARE, *supra* note 32, at 91.

[76] *Id.* at 103.

[77] *See* William J. Bayles, *The Ethics of Computer Network Attack*, 31 PARAMETERS 44 (2001) (noting the far-reaching nature of cyber-attacks, and that "the greater the connectivity (defined as both the amount of external communications as well as the number of potential or habitual connections the machine uses), the more likely it is that the attack will reach unintended targets.").

[78] *Cf.* Rome Statute of the International Criminal Court art. 8(2)(b)(ii), July 17, 1998, 2187 U.N.T.S. 90 [hereinafter Rome Statute] ("intentionally directing attacks against civilian objects, that is, objects which are not military objectives" constitutes a war crime in international armed conflicts.).

[79] Bayles, *supra* note 77.

[80] *Id.*

Participation in a cyber-conflict requires its own nuanced analysis. Rule 25 notes that no category of person is barred "from participating in cyber operations," though "the legal consequences of participation differ, based on the nature of the armed conflict and the category to which an individual belongs."[81] Rule 26, however, provides that members of the armed forces who are party to an international armed conflict "lose their entitlement to combatant immunity and prisoner of war status" upon failure to comply with the requirements of combatant status in cyber operations.[82] It follows that the majority of the International Group of Experts who composed the Tallinn Manual took the position under Note 6 to Rule 26 that cyber-combatants who fail to comply with the Third Geneva Convention in executing cyber-attacks in an international armed conflict would lose their combatant status under the Convention.[83] If the Third Geneva Convention applies, however, that also suggests that some terms that would be ambiguous in assessing a cyber-combatant under it (such as "having a fixed sign recognizable at a distance" and "carrying arms openly") must have some meaning with respect to cyberspace operations—though the precise meaning remains unclear.

It is clear, however, that if an international armed conflict exists under Rule 22, Note 16 of the Tallinn Manual, there must necessarily be combatants participating in that conflict. It is conceivable that a conflict solely involving cyber operations might potentially reach international armed conflict status under Rule 22, Note 15. Thus, Notes 15 and 16, read together, suggest that cyber units engaged in such activity may obtain 'combatant' status when Rule 22 is met. The question of the perpetrators' "lawful" status as combatants when executing a cyber-attack presently falls to the Geneva Conventions and

---

[81] TALLINN MANUAL ON THE INTERNATIONAL LAW APPLICABLE TO CYBER WARFARE, *supra* note 32, at 95.

[82] *Id*. at 96.

[83] *See id.* at 97-98 (noting in addition that "[i]f a person engaged in cyber operations during an armed conflict is a member of an organized armed group not belonging to a party to the conflict, it does not matter if the group and its members comply with the four criteria of combatancy. That person will not have combatant status and therefore not be entitled to combatant immunity or to be treated as a prisoner of war. Such a person would be an 'unprivileged belligerent.'").

surrounding principles of international law.

III. A survey of sovereign states' alleged cyber operations

At this time, roughly 30 nations employ offensive cyber programs.[84] Irrespective of whether the current state of customary international law considers such programs to rise to the level of cyber-attacks, states (and groups acting on their behalf) have assembled formidable arsenals capable of executing devastating and continuous cyber-operations in the field of cyberspace.[85] Units possessing significant cyber-capabilities include Israel's Unit 8200 / C4i, the United States' USCYBERCOM, Russia's APT28,[86] and China's PLA Unit 61398. While examples of state cyber-capabilities are certainly not limited in practice to those described herein, the states whose activities are

---

[84] Ralph Langner, *To Kill a Centrifuge: A Technical Analysis of What Stuxnet's Creators Tried to Achieve* 4 (Nov. 2013), http://www.langner.com/en/wp-content/uploads/2013/11/To-kill-a-centrifuge.pdf (noting that those nations include North Korea, Iran, Syria, and Tunisia).

[85] *See* Molly Bernhart Walker, *Cyberwarfare underway 'all of the time,' says former NATO supreme allied commander*, FIERCEGOVERNMENTIT (Oct. 13, 2014), http://www.fiercegovernmentit.com/story/cyberwarfare-underway-all-time-says-former-nato-supreme-allied-commander/2014-10-13 (quoting Gen. Wesley S. Clark (ret.), recounting a meeting in 1994 where "a guy [at the meeting] with a handcuff on his suitcase . . . open[ed] it up and sa[id] 'this is really, really, really secret, but we could destroy a country's electricity grid. Yes, without dropping a bomb'"); Adam Jourdan, *China-U.S. cyber spying row turns spotlight back on shadowy Unit 61398*, REUTERS (May 20, 2014), http://www.reuters.com/article/2014/05/20/us-cybercrime-usa-china-unit-idUSBREA4J08M20140520 (quoting an analyst from Mandiant, the U.S. cyber security firm who identified the location of PLA Unit 61398's operations in China, as stating the discovery was only "the tip of the iceberg:" "I believe there's an ongoing battle in the cyberspace. These countries are investing large amounts in cyber units that are able to create specific malware and have the ability to get into foreign networks and computers to steal trade secrets and intellectual properties.").

[86] *See Special Report: APT28: A Window Into Russia's Cyber Espionage Operations?*, FIREEYE 3 (2014), https://www2.fireeye.com/rs/fireye/images/rpt-apt28.pdf [hereinafter FireEye APT28 Report] (stating that the APT28's activities are "the work of a skilled team of developers and operators collecting intelligence on defense and geopolitical issues – intelligence that would only be useful to a government. We believe that this is an advanced persistent threat (APT) group engaged in espionage against political and military targets including the country of Georgia, Eastern European governments and militaries, and European security organizations since at least 2007.").

enumerated below have significantly shaped the cyber-battlefield.

A. Israel and Stuxnet

The base at Urim in the Negev Desert that has formed the central node of Unit 8200's operations remained invisible for decades, silently intercepting phone calls and e-mails passed on to other Israeli agencies, including the Army and the Mossad.[87] Nir Lempert, a reserve colonel and former deputy commander of Unit 8200, has outlined the unit's recruitment policies: the brightest teenagers in the country are hand-picked, then trained to solve problems in multidisciplinary teams, where they are encouraged to think outside the military model.[88]

In contrast to Unit 8200, Israel's C4i Corps is a relatively recent arrival.[89] Nevertheless, it has claimed to possess far-reaching capabilities on the battlefield, from disruptions to command and control systems to more classified non-kinetic weaponry.[90] C4i is a dynamic unit, and is currently in the process of upgrading the entire IDF network, allowing for seamless communication on the battlefront.[91]

---

[87] Nicky Hager, *Israel's Omnicient Ears*, LE MONDE DIPLOMATIQUE (Sept. 2010), http://mondediplo.com/2010/09/04israelbase.

[88] Matthew Kalman, *Israeli military intelligence unit drives country's hi-tech boom*, THE GUARDIAN (Aug. 12, 2013), http://www.theguardian.com/world/2013/aug/12/israel-military-intelligence-unit-tech-boom ("The central mission of the unit is to save lives, to prevent terror and other attacks," says Lempert. "We teach our people that the mission is so important that there is no possibility of failure.").

[89] Yaakov Lappin, *Military Affairs: The IDF's Secret Attack Force*, JERUSALEM POST (May 11, 2013), http://www.jpost.com/Features/Front-Lines/Military-Affairs-The-silent-attack-force-312716 (quoting a senior source within the Electronic Warfare Section of the Corps as stating "[C4i] began small, and became large over the past decade. Now, it's a monster . . ." and "The government instructed us to prepare and know how to operate [Electronic Warfare] in every operational arena.").

[90] *Id.* (quoting the same source: "This is not a kinetic attack. The mission is not to destroy a target, to damage, or neutralize it, but rather to disrupt. I'm aiming at the enemy's command and control. His management, organization and commanders are the target . . ." but also noting that some activities are classified).

[91] Yaakov Lappin, *Person of the Year in the IDF: The C4i Corps*, JERUSALEM POST (Dec. 29, 2013), http://www.jpost.com/Features/In-Thespotlight/Person-of-the-year-in-the-IDF-The-C4i-Corps-336472 ("The IDF's C4i Corps is at the heart of a dramatic technological upgrade aimed at

Israeli cyber units may have participated in the creation of the infamous worm Stuxnet.[92] An early version of the attack weapon manipulated valves on the centrifuges to increase the pressure inside them and damage the devices as well as the enrichment process.[93] The worm, which reportedly caused the failure of roughly a fifth of Iran's nuclear centrifuges by causing them to spin out of control,[94] manipulated computer systems designed by Siemens, a German firm, infecting computers belonging to five outside firms believed to be connected with Iran's nuclear program.[95] All of the companies did business in industrial control and processing, either by manufacturing products, assembling components, or installing industrial control systems.[96] While exactly how long it took Stuxnet to reach its target after infecting these corporate machines is unclear, between June and November of 2010, the number of centrifuges enriching uranium gas at the Natanz Nuclear Facility began to drop significantly.[97]

Unlike any other virus or worm released before it, Stuxnet caused a physical impact on tangible equipment controlled by the computers it infected.[98] While the attack by Stuxnet on Natanz was pinpointed and specific, its tactics and technology

---

achieving this vision. It has seen the IDF revolutionize its capabilities in a very short matter of time, and 2013 has been a key year for developments.").

[92] *See* John Markoff, *A Silent Attack, but Not a Subtle One*, N.Y. TIMES (Sept. 26, 2010), http://www.nytimes.com/2010/09/27/technology/27virus.html?_r=0 (quoting "[a] former member of the United States intelligence community" who claimed the attack "had been the work of Israel's equivalent of America's National Security Agency, known as Unit 8200.").

[93] *Id.*

[94] Michael B. Kelley, *The Stuxnet Attack On Iran's Nuclear Plant Was 'Far More Dangerous' Than Previously Thought*, BUS. INSIDER (Nov. 20, 2013), http://www.businessinsider.com/stuxnet-was-far-more-dangerous-than-previous-thought-2013-11.

[95] Kim Zetter, *An Unprecedented Look at Stuxnet, the World's First Digital Weapon*, WIRED (Nov. 3, 2014), http://www.wired.com/2014/11/countdown-to-zero-day-stuxnet/.

[96] *Id.*

[97] *Id.* (noting a decrease of 328 centrifuges between June and August of 2010, and a decrease of an additional 656 centrifuges between September and November, for a total decrease in 984 centrifuges; also noting that "although new machines were still being installed, none of them were being fed gas.").

[98] *See id.*; *see also* Langner, *supra* note 84, at 4 (styling Stuxnet's assault on Iranian nuclear centrifuges "a cyber-physical attack").

are generic; the three-layer methodology used in them, consisting of the worm's propagation through IT systems, its manipulation of Industrial Controls, and the requisite physical damage that results from such manipulation, has strong potential for use against other targets.[99]

The Stuxnet attack has accelerated the propagation of cyber-capabilities in the Middle East region; in early March of 2012, Ayatollah Ali Khamenei, Iran's Supreme Leader, publicly announced the creation of a "Supreme Council of Cyberspace" charged "to oversee the defense of the Islamic Republic's computer networks and develop new ways of infiltrating or attacking the computer networks of its enemies."[100] Simultaneously, Iran embarked on a $1 billion (USD) plan to develop technology and hire computer experts with the goal of boosting the Islamic Republic's offensive and defensive cyber-warfare capabilities.[101] The 0xOmar Trojan, whose designer claims to be from Saudi Arabia,[102] released the information of thousands of Israeli credit cards in January of 2012.[103] While the 0xOmar worm appears to be the product of a Wahhabi group rather than a governmental directive,[104] its origin is not confirmed. Moreover, it

---

[99] *See* Langner, *supra* note 84, at 4.

[100] Shane Harris, *Forget China: Iran's Hackers Are America's Newest Cyber Threat*, FOREIGN POLICY (Feb. 18, 2014), *http://foreignpolicy.com/2014/02/18/forget-china-irans-hackers-are-americas-newest-cyber-threat/*; *see also* Eric K. Shafa, *Iran's Emergence as a Cyber Power*, STRATEGIC STUDIES INST. (Aug. 20, 2014), http://www.strategicstudiesinstitute.army.mil/index.cfm/articles/Irans-emergence-as-cyber-power/2014/08/20.

[101] Yaakov Katz, *Iran embarks on $1b. cyber-warfare program*, JERUSALEM POST (Dec. 18, 2011), http://www.jpost.com/Defense/Iran-embarks-on-1b-cyber-warfare-program.

[102] AL ARABIYA, *'Saudi' hacker says Israel uncovered wrong person, vows deeper strikes* (Jan. 7, 2012), http://english.alarabiya.net/articles/2012/01/07/186810.html (reporting that the hacker, OxOmar, "vowed to send more files and more emails, adding that he was from Riyadh.").

[103] Yaakov Lappin, *Hackers post 1000s of Israeli credit card numbers*, JERUSALEM POST (Jan. 3, 2012), http://www.jpost.com/International/Hackers-post-1000s-of-Israeli-credit-card-numbers.

[104] Gianluca Mezzofiore, *Anonymous Saudi Hacker OxOmar Second Attack on Israeli Credit Cards*, INT'L BUS. TIMES (Jan. 6, 2012), http://www.ibtimes.co.uk/anonymous-hacker-oxomar-stages-second-attack-israeli-277469 (quoting a statement posted on an Israeli sports website: "Hi, it's OxOmar from group-xp, largest Wahhabi hacker group of Saudi Arabia . . . "We are anonymous Saudi Arabian hackers. We decided to release

highlights the widespread retaliatory response to Stuxnet in the Middle East.[105]

B. USCYBERCOM and related U.S. Agencies

The Army divisions that would integrate into what would ultimately become the United States Cyber Command have their roots in the U.S. Army Strategic Communications Command (STRATCOM).[106] By 1968, STRATCOM numbered some 49,000 personnel and provided "rapid, dependable, secure communications to military and civilian users around the world."[107] Ultimately, however, the systems managed by the heirs to STRATCOM (U.S. Army Communications Command in 1973, replaced by U.S. Army Information Systems Command in 1984) and their ultimate rededication to strategic signal services, resulted in the decentralization and deregulation of command, control, communications, and computer (hereinafter C4) systems among Army Major Commands, causing serious compatibility issues for the Army's IT/IS equipment and support networks.[108] The negative impacts resulting from this incompatibility compelled the U.S. Army to re-centralize its C4 systems starting in 2002.[109]

By September 2006, it became apparent that computer network operations had begun to evolve into a larger mission set — cyberspace operations — and the Army directed for greater integration, coordination, and synchronization in Army computer operations to address risks in cyberspace.[110] By July of 2008, the Army had activated its first provisional network

---

first part of our data about Israel.").

[105] *See generally* Manny Halberstam, Note, *Hacking Back: Reevaluating the Legality of Retaliatory Cyberattacks,* 46 GEO. WASH. INT'L L. REV. 199 (2013).

[106] Vince Breslin, *Network Enterprise Command evolved from Strategic Communications Command*, ARMY COMMUNICATOR (Summer 2010), http://www.thefreelibrary.com/Network+Enterprise+Command+evolved+from+Strategic+Communications. . .-a0246535606.

[107] *Id.*

[108] *Id.*

[109] *Id.*

[110] *Establishment of U.S. Army Cyber Command*, U.S. ARMY CYBER COMMAND, http://www.arcyber.army.mil/history_arcyber.html#N1 (last visited Apr. 19, 2015).

warfare battalion under the U.S. Army Intelligence and Security Command (INSCOM).[111]

In June of 2009, United States Secretary of Defense Robert Gates, commissioned the United States Cyber Command ("USCYBERCOM") with the stated goal "to coordinate Pentagon efforts in the emerging battlefield of cyberspace and computer-network security."[112] At the time, USCYBERCOM's director, Lt. Gen. Keith Alexander, claimed that "[the establishment of USCYBERCOM] is not about efforts to militarize cyberspace . . . [r]ather it's about safeguarding the integrity of our military system."[113]

While it is possible that USCYBERCOM's initial goals may have been almost entirely defensive in nature, Iran's development of its nuclear program may have changed those goals – unofficially if not officially. The New York Times reported on a covert U.S. program initiated by President George W. Bush and handed off to his successor, Barack Obama, after Israeli officials requested to fly over Iraq to reach Iran's nuclear plant at Natanz.[114] While 2010 saw a much subtler attack by Stuxnet taking much of Natanz out of commission,[115] both Israeli and

---

[111] *Id.*

[112] Thom Shanker, *New Military Command for Cyberspace*, N.Y. TIMES. (June 23, 2009), http://www.nytimes.com/2009/06/24/technology/24cyber.html.

[113] Mike Mount, *U.S. Won't Militarize Cyberspace, Nominee Says*, CNN (Apr. 16, 2010, 12:04 PM), http://www.cnn.com/2010/POLITICS/04/16/military.cyberspace/; s*ee also* Tod Leaven & Christopher Dodge, *The United States Cyber Command: International Restrictions vs. Manifest Destiny*, 12 N.C.J.L. & Tech. On. 1, 2 (2010); *cf. U.S. Cyber Command*, U.S. STRATEGIC COMMAND, http://www.stratcom.mil/factsheets/2/Cyber_Command/ (last visited Apr. 19, 2015) (proclaiming USCYBERCOM's stated mission, among other elements, is to ". . . prepare to, and, when directed, conduct full spectrum military cyberspace operations in order to enable actions in all domains, ensure US/Allied freedom of action in cyberspace and deny the same to our adversaries.").

[114] David E. Sanger, *U.S. Rejected Aid for Israeli Raid on Iranian Nuclear Site*, N.Y. TIMES Jan. 10, 2009, http://www.nytimes.com/2009/01/11/washington/11iran.html?scp=1&sq=january%202009%20sanger%20bush%20natanz&st=cse (reporting, somewhat cryptically, that "Several details of the covert effort have been omitted from this account, at the request of senior United States intelligence and administration officials, to avoid harming continuing operations.").

[115] *See* Zetter, *supra* note 95.

U.S. officials proclaimed an official denial of involvement in the Worm's dissemination.[116]

The evidence pointing to U.S. involvement in Stuxnet is circumstantial at best,[117] but there is much to suggest that the U.S. has developed strong offensive cyber-warfare capabilities. In October of 2012, President Obama issued Presidential Policy Directive 20, which lays out policies and procedures for "Offensive Cyber Effects Operations" (hereinafter OCEO).[118] The directive places OCEO into three distinct categories: "Cyber Operations with Significant Consequences," which require "[s]pecific Presidential approval;"[119] "Threat Response Operations," which provide a certain degree of departmental autonomy, but require that "[t]he United States Government shall reserve use of such responses to circumstances when network defense or law enforcement measures are insufficient or cannot be put in place in time to mitigate the malicious cyber activity" and cautions that "departments and agencies shall conduct . . . responses in a manner not reasonably likely to result in significant consequences."[120] In addition, the directive cautions departments to "use the minimum action required to mitigate the

---

[116] William J. Broad, John Markoff and David E. Sanger, *Israeli Test on Worm Called Crucial in Iran Nuclear Delay*, N.Y. TIMES, Jan. 15, 2011, at A1, http://www.nytimes.com/2011/01/16/world/middleeast/16stuxnet.html?pagewanted=1&_r=2&hp (reporting, in spite of the U.S. and Israeli denials, that "[b]y the accounts of a number of computer scientists, nuclear enrichment experts and former officials, the covert race to create Stuxnet was a joint project between the Americans and the Israelis, with some help, knowing or unknowing, from the Germans and the British.").

[117] Spencer Ackerman, *With Stuxnet, Did The U.S. And Israel Create a New Cyberwar Era?*, WIRED (Jan. 16, 2011), http://www.wired.com/2011/01/with-stuxnet-did-the-u-s-and-israel-create-a-new-cyberwar-era/ (acknowledging that "Stuxnet' s origin is unknown;" subsequently stating that "[t]he Stuxnet whodunit may be solved: it appears to be a joint U.S.-Israeli collaboration — and a cyberwarfare milestone. *The New York Times* doesn't have definitive proof, but it has fascinating circumstantial evidence . . .").

[118] Presidential Policy Directive 20, Subject: U.S. Cyber Operations Policy (U), (Oct. 16, 2012), http://www.theguardian.com/world/interactive/2013/jun/07/obama-cyber-directive-full-text; (June 7, 2013) (directing a new cyber operations policy; marked "Top Secret" and ordered to be declassified on Oct. 16, 2037).

[119] *Id.* at 9.

[120] *Id.* at 9-10.

activity."[121] "Emergency Cyber Actions" are to be conducted by either the Secretary of Defense or other department head authorized by the President, with several caveats, including that they be conducted only when "necessary in accordance with the United States inherent right of self-defense as recognized in international law to prevent imminent loss of life or significant damage" and "intended to be nonlethal in purpose, action, and consequence."[122]

U.S. military officials have acknowledged cyber-espionage, and cyber-attacks have heralded a revolutionary new era in military operations in which the United States cannot afford to be left behind.[123] Undoubtedly, U.S. forces are developing both the defensive and offensive capabilities necessary to build and maintain advantages to protect its domestic and foreign interests as regards this potential new war front.

C. Russia and APT28

If Israel and the United States in fact opened the war-front of cyber-warfare with the release of Stuxnet in 2013, it was Russia that fired the opening salvo five years earlier. Weeks before the attack on Georgia in 2008 began, a security researcher in Lexington, Massachusetts became aware of a stream of data directed at Georgian government sites containing the message "win+love+in+Rusia."[124] As early as July of

---

[121] *Id.* at 10.

[122] *Id.* at 10.

[123] Mike Milord, *Guard activates first cyber protection team, issues new shoulder sleeve insignia*, ARMY.MIL (Oct. 20, 2014), http://www.army.mil/article/136100/ (quoting a speech given by Army Maj. Gen. Judd H. Lyons during a ceremony on October 7, 2014, at which The Army National Guard's first cyber protection team received its new shoulder sleeve insignia) ("In 1775, the 'shot heard round the world' signaled the start of the American Revolutionary War . . . Today, 239 years later, we face a world in which the first shots of the next war may be fired in cyberspace. And unlike the shots fired in 1775, those shots may indeed be heard around the world, in a very real sense, as systems and components thousands of miles away are instantaneously disabled by a keystroke.") (Lyons stated further that) ("The billions of lines of code, massive server farms and cloud-based assets that govern our power, water, fuel, communications, transportation, and national defense must be protected.").

[124] John Markoff, *Before the Gunfire, Cyberattacks*, N.Y. TIMES, (Aug. 12, 2008), http://www.nytimes.com/2008/08/13/technology/13cyber.html.

2008, internet experts across the United States observed a relentless barrage of distributed denial-of-service attacks that effectively shut down numerous Georgian servers in a prelude to wave of attacks that followed once the war began in earnest, originating from hosting centers controlled by Russian telecommunications firms.[125] One of the first Georgian websites that was attacked was a popular hacker forum. In perpetrating such an attack, Russian-supported hacker "militias" appeared to perpetrate a preemptive strike, attempting to prevent or mitigate "returning fire" from Georgian hackers.[126] These massive digital attacks drove some of the government of Georgia's websites offline during the Russian invasion. The attacks were termed by many net security experts to be the first overt act of cyber-warfare.[127]

Naturally, Russia denied involvement in the computer-related attacks.[128] But the repeat use of similar measures in Russia's conflict with Ukraine suggests that Mother Russia protests too much."[129] With the advent of the Ukrainian conflict, dozens of computer networks in Ukraine were found to be infected by a cyber-espionage "tool kit" called "Ouroboros," or Snake, which bore uncanny similarity to a system that had attacked classified systems at the Pentagon years before.[130] This

---

[125] *Id.*

[126] David Hollis, *Cyberwar Case Study: Georgia 2008,* SMALL WARS J., (Jan. 6, 2011), http://smallwarsjournal.com/blog/journal/docs-temp/639-hollis.pdf.

[127] *See Cyber-attacks on Georgia Websites Tied to Mob, Russian Government*, L.A. TIMES: TECHNOLOGY (Aug. 13, 2008, 6:39 PM), http://latimesblogs.latimes.com/technology/2008/08/experts-debate.html; *see also* Michael Gervais, *Cyber-attacks and the Laws of War*, 30 BERKELEY J. INT'L L. 525, 579 (2012).

[128] Markoff, *supra* note 124.

[129] *See* William Shakespeare, *The Tragedie of Hamlet, Prince of Denmarke*, *in* THE APPLAUSE FIRST FOLIO OF SHAKESPEARE IN MODERN TYPE 742, 758 (2001) (Neil Freeman Ed.) ("The Lady doth protest too much methinks.").

[130] David E. Sanger and Steven Erlanger, *Suspicion Falls on Russia as 'Snake' Cyberattacks Target Ukraine's Government*, N.Y. TIMES, (Mar. 8, 2014), http://www.nytimes.com/2014/03/09/world/europe/suspicion-falls-on-russia-as-snake-cyberattacks-target-ukraines-government.html?; *see also* Fred Barbash, *Cyberattacks on Ukraine bear Russian hallmarks*, WASH. POST (Mar. 9, 2014), http://www.washingtonpost.com/news/morning-mix/wp/2014/03/09/the-snake-cyberrattacks-on-ukraine-said-likely-to-come-from-russia/ (describing the predecessor program to Ouroboros, called "Agent.Btz," as "the most serious breach of the U.S. military's classified com-

appeared to fit with the typical Russian *modus operandi*: as one senior U.S. Intelligence official noted, "[t]he usual Russian approach would be to design something that could both conduct surveillance and aid in an attack."[131] Ouroboros does exactly that: By targeting the Ukrainian government with Ouroboros, the Russians are able to effectively engage in an aggressive, kinetic act without actually declaring war, or other countries reacting like it is an act of war..[132] "Snake" perpetrated a massive DDoS-attack on communication channels for the National Security and Defense Council of Ukraine, the Ukrainian state-run news agency, the Ukrainian telecommunications system, and the mobile phones of members of the Ukrainian parliament.[133]

The cyber-security firm FireEye has traced the Russian-backed hacker group behind the attacks in Ukraine, dubbed APT28 (sometimes ATP28) by experts, to coordinated, sophisticated digital attacks against NATO and the European Union.[134] Ultimately, APT28 planted its flag on the White House; U.S. officials, alerted to the breach by an ally, were able to mitigate the group's activity, but not before the attack caused multiple service outages to unclassified White House networks and potentially resulted in significant data theft.[135] Nevertheless, no nation or organization has managed to directly attribute APT28 to the Russian government, much less reveal its true name or identity. The closest anyone has gotten — publicly, at least — is the identification of the group's regular activity in Moscow and St. Petersburg time zones, and the fact that its activities further Russian governmental interests.[136] The level of

puter systems . . . the Pentagon . . . discovered the rogue program infecting a classified network harboring some of the military's most important secrets.").

131 Sanger, *supra* note 130.

132 Alec Ross, *Russia's cyber weapons hit Ukraine: How to declare war without declaring war*, WORLD POST (Mar. 10, 2014), http://www.huffingtonpost.com/alec-ross/russias-cyber-war_b_4932475.html

133 Hillary Douglas, *Cyber attackers target Ukraine's government departments*, EXPRESS (Mar. 9, 2014), http://www.express.co.uk/news/world/463828/Cyber-attackers-target-Ukraine-s-government-departments.

134 FireEye APT28 Report, *supra* note 86, at 3-5.

135 *See* Nakashima, *supra* note 13.

136 *Special Report: APT28: A Window Into Russia's Cyber Espionage Operations?*, *supra* note 86.

coordination APT28 exercises, however, is strikingly similar to that of its counterparts in Israel and the United States. Even assuming APT28 were not a Russian military unit, it is likely that they are operating with support from the Russian government.

D. China and PLA Unit 61398

In February of 2013, Cyber Security firm Mandiant released a report identifying an "advanced persistent threat" in cyberspace and designating that threat "APT1."[137] Mandiant tracked APT1 down to a 130,663 square-foot compound at 208 Datong Road in Shanghai.[138] China would have been no stranger to cyber operations; "[i]n late August of 2011, a state television documentary aired on the government-run China Central Television [that] appeared to capture an in-progress distributed denial of service attack by China's military on a Falun Gong website based in Alabama."[139] Most commonly known by its Military Unit Cover Designator, PLA Unit 61398, APT1 is believed to have compromised 141 companies spanning 20 major industries, stealing vast amounts of intellectual property in the process.[140] According to Mandiant's report, Unit 61398 "requires its personnel to be trained in computer security and computer network operations and also requires its personnel to be proficient in the English language."[141] A 2004 notice on Zhejiang University's website "China's People's Liberation Army Unit 61398 Recruiting Graduate Students" [zh], stated that "Unit 61398 of China's People's Liberation

---

[137] *APT1: Exposing One of China's Cyber Espionage Units*, Mandiant 2 (2013), http://intelreport.mandiant.com/Mandiant_APT1_Report.pdf.

[138] Charles Riley, *The Cybercrime Economy: China's military denies hacking allegations*, CNNMONEY (Feb. 20, 2013, 3:52 AM), http://money.cnn.com/2013/02/20/technology/china-cyber-hacking-denial/index.html (last visited Nov. 5, 2015) (noting that a Chinese government spokesman has criticized the report as "groundless both in facts and legal basis" and "lacks technical proof" because it "relies too heavily on the tracking of IP addresses . . . that are stolen almost everyday").

[139] *See* Hathaway, *supra* note 9, at 820 (citing Ellen Nakashima & William Wan, China's Denials on Cyberattacks Undercut, WASH. POST, Aug. 24, 2011, at A12).

[140] *APT1: Exposing One of China's Cyber Espionage Units*, *supra* note 137, at 3.

[141] *Id.*

Army (located in Pudong District, Shanghai) seeks to recruit 2003-class computer science graduate students."[142] According to the NSA, "China may have the capability to remotely shut down computer systems [belonging to] U.S. utilities, aviation networks, and financial companies".[143]

Mandiant revealed three identifiable individuals perpetrating the attacks, two of whom it identified using the same shared infrastructure, including Fully Qualified Domain Names (FDQNs) and IP ranges identified as belonging to APT1.[144] The first persona, "UglyGorilla", has been active in computer network operations since October 2004, and authors malware used in APT1 campaigns,[145] when that persona registered the first domain name system (DNS) zone attributed to APT1 using both Shanghai and the "+86" international code in the registrant's information fields.[146] The second, "DOTA", "has registered dozens of email accounts used to conduct social engineering and spear phishing attacks in support of APT1 campaigns, us[ing] a Shanghai phone number [in] registering th[o]se accounts."[147] The third, "SuperHard," "discloses his location to be the Pudong New Area of Shanghai."[148] The file names in these hackers' own digital weaponry suggest that English is a second language for the programmers.[149] These and other APT1 personae appear to target emerging industries

---

[142] *PLA Unit 61398 Recruitment Notice Found*, CHINA DIGITAL TIMES (Feb. 20, 2013), http://chinadigitaltimes.net/2013/02/pla-unit-61398-recruitment-notice-found/ (noting that the link to the recruitment post was available at the time the article was written. The recruitment post is no longer available and redirects to a "not found" page as of Apr. 13, 2015).

[143] Edd Gent, *China could shutdown critical US infrastructure, says NSA chief*, E&T (Nov. 21, 2014), http://eandt.theiet.org/news/2014/nov/china-cyber-infrastructure.cfm.

[144] *APT1: Exposing One of China's Cyber Espionage Units*, *supra* note 137, at 5.

[145] *Id.* (noting that "UglyGorilla" publicly expressed his interest in China's "cyber troops" in Jan. 2004).

[146] *Id.* at 45-46.

[147] *Id.* at 5.

[148] *Id.*

[149] *APT1: Exposing One of China's Cyber Espionage Units, supra* note 137, at 38 (noting language such as "No Doubt to Hack You, Writed by UglyGorilla" and "you specify service name not in Svchost\netsvcs, must be one of following" in the malware code's tools).

identified in China's "12th Five Year Plan,"[150] including information technology, high-end equipment manufacturing, advanced materials, and biotechnology.[151]

Close to a year after Mandiant released its report, a grand jury in the Western District of Pennsylvania "indicted five Chinese military hackers for computer hacking" and related offenses "directed at six American victims in the U.S. nuclear power, metals, and solar products industries."[152] The indictment, which included "UglyGorilla" among its Defendants,[153] accused the defendants of hacking into several corporations with integral roles in U.S. infrastructure, including Westinghouse Electric Company, U.S. Steel, and Alcoa.[154] In response, China "summoned the U.S. ambassador in Beijing, and warned it would retaliate if the U.S. followed through with the charges," and suggesting that the proceedings would damage mutual trust.[155] There has been no further news since the indictment. Nevertheless, on April 1, 2015, President Obama signed an Executive Order allowing for the freezing of all property and interests in the United States linked to computer compromise at-

---

[150] *Id.* at 59.

[151] *See id.* at 24 (noting information technology, aerospace, satellites and telecommunications, scientific research, energy, transportation, construction and manufacturing, and high-tech electronics among those hardest hit by APT1); *see also* Stephen S. Roach, *China's 12th Five-Year Plan: Strategy vs. Tactics*, 5 (Apr. 2011), http://www.law.yale.edu/documents/pdf/cbl/China_12th_Five_Year_Plan.pdf (noting that China's Twelfth Five Year Plan "focuses on the development and expansion of seven strategic emerging industries (SEIs): New-generation information technology, high-end equipment manufacturing, advanced materials, alternative-fuel cars, energy conservation and environmental protection, alternative energy, and biotechnology.").

[152] U.S. Department of Justice, *U.S. Charges Five Chinese Military Hackers for Cyber Espionage Against U.S. Corporations and a Labor Organization for Commercial Advantage* (May 19, 2014), http://www.justice.gov/opa/pr/us-charges-five-chinese-military-hackers-cyber-espionage-against-us-corporations-and-labor.

[153] Indictment, United States v. Dong (2014) (No. 14-118), http://www.justice.gov/iso/opa/resources/5122014519132358461949.pdf (currently under seal) (designating "UglyGorilla" as the alias for "Wang Dong").

[154] *Id.* at ¶ 6.

[155] Adam Jourdan, *China-U.S. cyber spying row turns spotlight back on shadowy Unit 61398*, REUTERS (May 20, 2014), http://www.reuters.com/article/2014/05/20/us-cybercrime-usa-china-unit-idUSBREA4J08M20140520.

tacks, espionage, or other related disruptions.[156]

As with APT28, direct ties between APT1 and PLA Unit 61398 are tenuous and largely circumstantial.[157] Individual Chinese perpetrators of cyber-espionage, however, appear to have been less successful in hiding their identities than their Russian, American, and Israeli counterparts. On the other hand, attacks attributed to the Chinese appear to avoid choosing foreign sovereigns as targets, more content with attacks on corporations or private firms a step removed from direct contact with a sovereign state. Nevertheless, it would be wrong to conclude that China's trepidation in seeking out such direct contact means that its cyber unit or units would be any less capable in perpetrating a cyber-attack if it elected to pursue that option.[158]

E. Analysis of Sovereign States' Present Legal Liabilities

Cyber units created by sovereign States are a prelude to a new dimension to combat support tactics executed through cyber warfare. These sovereign States have envisioned both defensive and offensive means of utilizing this 'new front' in military operations. Certainly, they may possess the capability to execute cyber operations that would constitute "acts or threats of violence the primary purpose of which is to spread terror among the civilian population" as defined in Article 51(2) of Additional Protocol I to the Geneva Conventions.[159] Likewise, they appear capable of measures that are "reasonably expected to cause injury or death to persons or damage or de-

---

[156] Exec. Order No. 13694, 80 Fed. Reg. 18077 (Apr. 1, 2015) ("Blocking the Property of Certain Persons Engaging in Significant Malicious Cyber-Enabled Activities").

[157] Zeljka Zorz, *More (circumstantial) findings reinforce Mandiant's APT1 claims*, HELP NET SECURITY (Feb. 28, 2013), http://www.net-security.org/secworld.php?id=14522.

[158] *See* Ellen Nakashima, *China testing cyber-attack capabilities, report says*, WASH. POST (Mar. 8, 2012), https://www.washingtonpost.com/world/national-security/china-testing-cyber-attack-capabilities-report-says/2012/03/07/gIQAcJwDyR_story.html (noting Chinese cyber capabilities may rival those of the U.S.; reporting a statement by James A. Lewis, a cyber-policy expert with the Center for Strategic and International Studies: "if we get into any kind of a conflict with the PLA, cyber will be their opening move.").

[159] A.P. I, *supra* note 38.

struction to objects" under Rule 30 of the Tallinn Manual.[160] While the question of attribution is a difficult one that likely shields sovereign states from liability in most instances,[161] this paper's analysis is confined to circumstances in which the international community successfully attributes an attack to a state actor, and the "victim" state has captured the individuals perpetrating that attack.

In such circumstances, the captives could be divided into two broad categories: those who executed such attacks from an openly designated military complex under a command structure, and those who did not. In cases involving "uniformed armed forces," "militias," and "volunteer corps that form part of those forces,"[162] as is the case in some Israeli, American, and Chinese forces focused on defensive tactics, the calculus is, in theory, simple, provided members of those cyber-units are apprehended in uniform and at a designated military site.

The problem, however, is that cyber forces often operate out-of-uniform and from numerous discrete locations.[163] The

---

[160] TALLINN MANUAL ON THE INTERNATIONAL LAW APPLICABLE TO CYBER WARFARE, *supra* note 32, at 106.

[161] *See id.* at 34 (noting, at Rule 7, that "[t]he mere fact" that a cyber operation's place of launch or origination is within "governmental cyber infrastructure" is insufficient to meet the standard for attribution); *see also* Larry Greenemeier, *Seeking Address: Why Cyber Attacks Are So Difficult to Trace Back to Hackers*, SCI. AM. (June 11, 2011), http://www.scientificamerican.com/article/tracking-cyber-hackers/ ("The hardest problem in finding the source of [cyber] attacks is attribution."); Dimitar Kostadinov, *The Attribution Problem in Cyber Attacks*, Infosec Inst. (Feb. 1, 2013), http://resources.infosecinstitute.com/attribution-problem-in-cyber-attacks/ (noting the consequences in the event of a hacker's misidentification).

[162] Third Geneva Convention, *supra* note 31, at art. 4.

[163] *See, e.g.*, James Stavardis, *The New Triad*, FOREIGN POLICY (June 20, 2013), http://foreignpolicy.com/2013/06/20/the-new-triad/ ("A U.S. Cyber Force will require a large civilian component and will need to be instinctively oriented toward working with the interagency process and the private sector"); Christopher Paul, Isaac R. Porche III, and Elliot Axelband, THE OTHER QUIET PROFESSIONALS: LESSONS FOR FUTURE CYBER FORCES FROM THE EVOLUTION OF SPECIAL FORCES, Rand Corp., at 27 (2014), http://www.rand.org/content/dam/rand/pubs/research_reports/RR700/RR780/RAND_RR780.pdf (noting that cyber operations "are best satisfied with a force that includes both uniformed and civilian personnel to appropriately execute given authorities, and many CNO functions can (and should) be carried out from remote locations as part of reachback").

Geneva Conventions were meant to apply to partisan forces,[164] not to the anonymities of warfare conducted over the internet.[165] An issue more analogous to those conventions might more reasonably arise concerning a 'cyber-soldier' or a 'cyber-partisan' who perpetrates a cyber-attack while operating behind enemy lines in a war zone. Assuming that the individual is apprehended under the laws of war, the question would be whether the apprehended perpetrator is a lawful combatant under the Geneva Conventions. Certainly, the apprehending state would argue that such an individual would fail to comply with Article 4, Section 2 of the Third Geneva Convention if that individual were out of uniform. That is, of course, unless the individual operated in uniform and under orders while hiding out in a forest and hacking via a satellite internet connection or a local wi-fi signal. Under those circumstances, assuming the cyber-soldier executed the attack in compliance with the laws of war, in which case she might argue that her computer could effectively be construed as an "openly displayed" armament, particularly if she is otherwise unarmed. These unlikely circumstances, however, would constitute the only manner in which such a cyber-combatant might successfully argue for the applicability of the Geneva Conventions to her.

Even when operating within his own state, a cyber-combatant's rights under the Geneva Conventions are at best unclear. Attacks perpetrated by the Stuxnet Worm, APT1, and APT28 all appear to meet this model, at least in part. In these cases, Article 4 of the Third Geneva Convention poses serious problems if the individuals carrying out the cyber-attack act covertly, because such individuals might easily fall into the ambit of Article 4, Section 2. Under that section, even individuals following "the laws and customs of war" within a distinct command unit would have a difficult time proving that they possessed "a fixed distinctive sign recognizable at a distance," much less that they carried their arms openly; cyber-

---

[164] *See* Commentary on Third Geneva Convention, *supra* note 43, at 52 (noting that in the course of World War II, an "abnormal and chaotic situation" arose "in which relations under international law became inextricably confused").

[165] *See* Martin Libicki, *Sub Rosa Cyber War* 12-13 (noting marked differences between physical conflicts and those in cyberspace, particularly where cyber-combatants are "sheltered . . . in the anonymity of the Internet").

combatants thrive on anonymity, and code in cyberspace does not move through the battlefield with the openness of a kinetic assault, such as a missile launcher or an M-16. Moreover, if cyber units were to post their nation's flag on the computer screens of a hijacked site prior to an attack, they would lose the element of surprise central to the effectiveness of attacks such as that by Stuxnet on Natanz. The same would apply to cyber units posting their code (the closest thing to their "arms" that one can surmise in an electronic landscape) online prior to launching a barrage of bits and bytes; it would only serve to alert the enemy, which could then easily destroy that code or render it ineffective before launching a counterattack of their own against whatever sovereign nation had fired the opening salvo.

It is of note that Mandiant's data collection on PLA Unit 61398 managed to record aspects of the malicious code and to decipher its contents.[166] This assisted in determining the identities of the authors, sometimes as far back as 2004;[167] it did not assist in determining, under the standard required by the Geneva Conventions, whether the authors flew a flag, wore their military uniforms, or carried any form of "arms openly" while they did so. The same analysis should apply equally to the authors of Stuxnet or APT28's activities. For these reasons, the time is nigh for a new Protocol concerning cyber operations perpetrated by sovereign state actors and their agents.

IV. The unique problem posed by non-state cyber forces

State actors have generally remained within the bounds (if tenuously) of what reasonably constitutes cybercrime or cyber espionage, rarely overreaching into the outright perpetration of a cyber-attack.[168] Non-state cyber units, in contrast, are far

---

[166] *APT1: Exposing One of China's Cyber Espionage Units*, *supra* note 137, at 45-46 (attempting to identify PLA Unit 61398 hackers based on metadata and code written by them).

[167] *Id.* at 45.

[168] *See* Benjamin Zweifach, *Plugging the Gap: A Reconsideration of the U.N. Charter's Approach to Low-Gravity Warfare*, 8 INTERCULTURAL HUM. RTS. L. REV. 379, 420 (2013) ("[O]ne state's encouragement of a guerilla, non-state movement would rarely rise to the level of an easily demonstrable Article 2(4) violation, simply by virtue of its less than kinetic conspicuousness . . ."), *citing Case Concerning Military and Paramilitary Activities in and*

more likely to possess the incentive to perpetrate activities rising to the level of a cyber-attack under international legal standards.[169] These groups, often already rogue in nature, may not view themselves as bound by international law, or worse, may not care.[170] The most likely non-state actor to perpetrate such a cyber-attack is ISIL, whose foray into the realm of cyber warfare has resulted in several cognizable cyber operations against sovereign states, including France and the United States.[171]

Admittedly, whether one may successfully attribute a link between ISIL and many groups professing loyalty to it is a tenuous gambit at best.[172] Regardless, the dangers posed by ISIL may be more acute than other organizations because of its embrace of modern technology and its appeal to young, computer-literate foreigners, including known hackers.[173] At present, ISIL hackers might find targeted, Stuxnet-style attacks that bridge cyberspace and cause kinetic damage more challenging; such attacks require time and resources not currently available

---

Against Nicaragua (Nicar. v. U.S.), 1986 I.C.J. 14 (1986).

[169] *See* Laurie R. Blank, *International Law and Cyber Threats from Non-State Actors*, 89 INT'L L. STUD. 406, 407 ("The nature of today's globalized and interconnected world combined with the extensive reliance on technology, computer systems and Internet connectivity means that non-State actors, whether individuals or groups of some kind, can have a significant impact through cyber activity.").

[170] *See* Scott Jasper and Scott Moreland, *The Islamic State is a Hybrid Threat: Why Does That Matter?* SMALL WARS J. (Dec. 2, 2014), http://smallwarsjournal.com/jrnl/art/the-islamic-state-is-a-hybrid-threat-why-does-that-matter (noting ISIS' disregard for international law).

[171] *See, e.g.*, Lizard Squad Twitter Feed, *supra* note 16; *Newsweek is latest victim of the 'Cybercaliphate,' supra* note 18; Martinez, *supra* note 20; Bill Chappell, *French TV Network Hacked By 'Cyber Caliphate' Group*, NPR.org (Apr. 9, 2015, 7:47 AM), http://www.npr.org/blogs/thetwo-way/2015/04/09/398492643/french-network-tv5monde-is-hacked-by-cyber-caliphate-group (reporting that France's TV5Monde went blank, replaced by the message "Je suIS IS.").

[172] Nakashima, *supra* note 13; Chappell, *supra* note 170 ("It's not yet known what actual ties, if any, the [Cyber Caliphate] hackers might have to ISIS.").

[173] Emma Graham-Harrison, *Could Isis's 'cyber caliphate' unleash a deadly attack on key targets? Britain's new spy chief has warned that we are in a 'technology arms race' with terrorists recruiting an army of hackers to their cause*, THE GUARDIAN (Apr. 12, 2015), http://www.theguardian.com/world/2015/apr/12/isis-cyber-caliphate-hacking-technology-arms-race.

to the group.[174] Nevertheless, ISIL or another rogue fanatic group bearing a similar desire for sovereign statehood would find cyber warfare a tempting tactic for causing quick, high-profile damage to a stronger, more established adversary.[175] In the likely event that such an attack takes place in the future, there are several distinct possibilities: first, the perpetrators may be directly, indirectly, or loosely affiliated with the group or unrecognized actor claiming statehood. There may also be questions as to whether or not a conflict exists. International Law would operate differently depending upon the nature of the permutations outlined above.

A scenario that has the potential to cause widespread panic involves the internet of things. Take, for example, the aforementioned scenario involving a cyber-attack on a military base.[176] Suppose, in the above scenario, a cyber unit that has sworn allegiance to a group similar to ISIL infiltrates the ovens at several military bases operated by the same sovereign state, discharging the gas on each and turning on their pilot lights several minutes thereafter. In an alternative scenario, the cyber unit might simultaneously overheat all of the base's furnaces overnight. Either situation causes a fire at the base, killing several hundred people. The hackers claim responsibility after the attack two weeks later by placing a message and an animated .gif file of their flag on the website of the company that manufactures the devices.

The state invokes the right to self-defense,[177] then invades the region, capturing the hackers after tracking their IP addresses and internet footprint in a manner similar to that used in Mandiant's attempt to unmask PLA Unit 61398.[178] At the time of their capture, the hackers in the unit are operating in

---

[174] *Id.*

[175] *See* Oliver Rochford, *Cyberwar: Breaching the Kinetic Barrier*, SECURITYWEEK (Jan. 22, 2013), http://www.securityweek.com/cyberwar-breaching-kinetic-barrier. ("The risk of cyber-terrorism is of course far greater – religious and dogmatic fanatics and radicals may indeed wish to provoke such a conflict. But we have to try and differentiate between that, and actual nation-states taking potshots at another- activities with very little to gain in real strategic terms, but which could very quickly escalate.").

[176] *See* Pesce, *supra* note 5.

[177] U.N. Charter art. 51, *supra* note 65.

[178] *See APT1: Exposing One of China's Cyber Espionage Units*, *supra* note 137, at 45-46.

uniform out of an unmarked building in territory seized by the invading state. Aside from their computers, of course, they are unarmed at the time of their capture. The invading state detains them as "unlawful combatants" in a temporary military base in the occupied territory. The hacking unit's commanding officer claims that he and the members of his unit are properly subject to treatment under the Geneva Conventions.

The analysis under the Third Geneva Convention is likely to create more problems than solutions. For the purposes of the proposed hypothetical, it can reasonably be assumed that an attack on military bases would be permissible under the laws of war, and thus the fourth prong of Article 4, section 2 of the Third Geneva Convention is met. Since the hacking unit's detention occurred in territory within the group's direct or effective control, the members of the unit perpetrating the attack have a strong argument that they are "members of regular armed forces who profess allegiance to a government or an authority not recognized by the Detaining Power."[179]

The detaining state may attempt a counterargument, alleging that the manner in which the detained cyber-soldiers carried out their attack was sufficient to render it covert. Moreover, the detaining power may argue that the detainees would fail to meet the standards enumerated in Article 4, subsection 2 of the Third Geneva Convention; the attackers have not displayed any fixed signs recognizable at a distance, nor have they carried their arms openly in effectuating their attack.[180] The detainees may counter that recognizance at a distance is left "open to interpretation" and that posting their flag on a related website meets the standard in Article 4, subsection

---

[179] *See* Third Geneva Convention, *supra* note 31, at art. 4, sect. 3.

[180] *Id*. at sec. 2. What "carrying arms openly" entails with respect to a cyber-attack is anyone's guess. *See infra* Part II (noting the significant issues with respect to subsections (c) and (d) under Article 4, subsection 2 of the Third Geneva Convention); *but see* Milord, *supra* note 123 (noting a "new shoulder sleeve insignia" for a cyber protection unit). A physical insignia is unlikely to meet the requirements of a "fixed sign recognizable at a distance," however. And regardless of whether the cyber-attackers adhere to the Geneva Conventions, the *jus in bello* may afford them no protection. *See* TALLINN MANUAL ON THE INTERNATIONAL LAW APPLICABLE TO CYBER WARFARE, *supra* note 32, at 97-98 (suggesting such fighters would be considered "unprivileged belligerents" not subject to the Third Geneva Convention).

2.[181] The detaining state is likely to argue that the flag on the website is insufficient to meet that standard, to which the detainees might respond by quoting Comment 11 to Rule 26 of the Tallinn Manual, which states the opinion of some in the group of experts that "the requirement only applies in circumstances in which the failure to have a fixed distinctive sign might reasonably cause an attacker to be unable to distinguish between civilians and combatants, thus placing civilians at greater risk of mistaken attack."[182] Because the attack was perpetrated solely against military targets, the detainees could argue, they were justified in carrying it out, and thus a fixed distinctive sign requirement does not apply.[183]

There will also be a question as to whether the "carrying arms openly" standard is applicable to the detainees. The detainees may argue that their unit's computers were used to perpetrate the attack, and thus constitute "arms." They may refer to the Tallinn Manual, which states that the unit is effectively "'armed' if it has the capacity of undertaking cyberattacks" (Rule 30).[184] However, the detaining state will argue that the programs used in the cyber-attack are the "arms," not the computers, and it is thus impossible for the unit to have carried a computer program "openly." A question of prevailing custom could arise, but because few cyber operations rise to the level of a cyber-attack under international law, and there is no consensus as to how a cyber-attack should be defined,[185] neither side's arguments are likely to prove entirely persuasive. The detainees would argue that the element of surprise, at least, is covered under existing law, and thus the openness of the "arms" used in the cyber attack is subject to a figurative, rather than a literal, interpretation.[186] The detaining state could attempt to counter this argument by suggesting that due to the medium, the attackers were not reasonably recognizable

---

[181] *See* Commentary on Third Geneva Convention, *supra* note 43, at 60.

[182] TALLINN MANUAL ON THE INTERNATIONAL LAW APPLICABLE TO CYBER WARFARE, *supra* note 32, at 99.

[183] *See id*.

[184] *Id.* at 88.

[185] Pool, *supra* note 10, at 309; *see also* Kodar, *supra* note 10, at 124.

[186] Commentary on Third Geneva Convention, *supra* note 43, at 61 (noting that "openly" does not mean "visibly" or "ostensibly," as "[s]urprise is a factor in any war operation . . . ").

in cyberspace at the time of the attack itself, whatever the nature of their actual weaponry.[187] Regardless, the detainees may have a strong argument that their international legal status is in doubt. Thus, protection is warranted until a "competent tribunal" determines the detainees' status.[188] At that tribunal, a fact-specific analysis about the nature of the detainees' activities, the nature of their apprehension by the detaining power, and the nature of the conflict between the detaining power and the group to which the detainees belong is likely to become a factor in determining the detainees' ultimate classification.

In the above scenario, an indirectly or loosely affiliated actor would have a more difficult case. In such a scenario, the question will be whether the actor's affiliation with the detainee is strong enough to implicate that the detainee "belong[s] to a party to the conflict."[189] Proving a connection may require analysis under the standard in *Nicaragua v. United States*, which held mere encouragement of an indirectly affiliated actor insufficient to constitute a violation of the *jus ad bellum* on the part of an encouraging state.[190] On the other hand, "a role in organi[z]ing, coordinating or planning the military actions of the military group, in addition to financing, training and equipping or providing operational support to that group" is sufficient to result in that group's liability under *Prosecutor v. Tadic*.[191] Even under the Tallinn Manual's rules, loose affiliation may not be sufficient to shield the detainee from suffering under unlawful combatant status; depending upon the nature of their affiliation, the detaining power might term the detain-

---

[187] *Id.* ("The enemy must be able to recognize partisans as combatants in the same way as members of regular armed forces, whatever their weapons.").

[188] *Id.* at art. 5 ("Should any doubt arise as to whether persons, having committed a belligerent act and having fallen into the hands of the enemy, belong to any of the categories enumerated in Article 4, such persons shall enjoy the protection of the present Convention until such time as their status has been determined by a competent tribunal.").

[189] Third Geneva Convention, *supra* note 31, at art. 4, sec. 2.

[190] *Case Concerning Military and Paramilitary Activities in and Against Nicaragua* (Nicar. v. U.S.), *supra* note 168.

[191] *Prosecutor v. Tadic*, Case No. IT-94-1-A, Appeals Chamber Judgment, ¶ 137 (Appeals Chamber, ICTY, Jul. 15, 1999), http://www.icty.org/x/cases/tadic/acjug/en/tad-aj990715e.pdf.

ees mercenaries, to whom the Manual affords no protection.[192]

There a final wrinkle worth considering. Suppose that in effectuating their attack, the detainees 'accidentally' acquired a handful of IP addresses for ovens or furnaces that were civilian, not military, in nature.[193] Suppose further that the resulting fires from those appliances caused widespread destruction and civilian deaths in an urban center a thousand miles from any of the unit's military targets. The detaining state would argue that the detainees violated Article 57(2)(a) of A.P. I, which requires planners to "take all feasible precautions in the choice of means and methods of attack with a view to avoiding, and in any event to minimizing, incidental loss of civilian life, injury to civilians and damage to civilian objects."[194] Thus, in perpetrating this attack, the detainees violated the laws and customs of war by targeting a civilian population. The detainees might attempt to counter that they had no intent to do so, that any resulting damage was collateral in nature rather than intentional, and that while "intentionally directing attacks against civilian objects" constitutes a war crime in an international armed conflict, unintentional attacks do not.[195]

Here, the proportionality principle will likely apply. The question will be whether the proper rubric for analysis should be the proportional number of erroneously targeted IP addresses, or the proportional amount of damage caused to civilian structures as a result of those erroneously targeted IP addresses. This is precisely the problem that existing treaty or custom does not anticipate; it will likely be a matter of first impression absent the establishment of some agreement or consensus regarding the issue.

Irrespective of what the outcomes in these scenarios might be, the lack of governing law is troubling both for the detainees and for the detaining state. Neither can be certain as to

---

[192] TALLINN MANUAL ON THE INTERNATIONAL LAW APPLICABLE TO CYBER WARFARE, *supra* note 32, at 103.

[193] *See* Laurie Segall, *My hack stole your credit card*, CNNMONEY (Dec. 7, 2015, 3:38 PM ET), http://money.cnn.com/2015/12/06/technology/my-hack-stole-your-credit-card/ (Recording the statement of a "grey hat" hacker: "Sometimes when you compromise something, you have access to a lot of other things in that same IP address space.").

[194] A.P. I, *supra* note 38, at art. 57.

[195] Rome Statute, *supra* note 78, at art. 8(2)(b)(ii).

whether the Geneva Conventions will apply. This lack of a clear demarcation of rights and responsibilities is a direct consequence of the lack of treaty, custom, or other prevailing authorities governing cyber conflicts; most arguments under international humanitarian law are persuasive, not binding, upon the parties that first encounter each other in this new arena.

V. Forward Into Cyberspace

The time is ripe for a new convention on cyber warfare, because cyber operations are now the norm.[196] Without clear rules of engagement, the impact on international humanitarian law will be significant. Members of cyber units fighting on behalf of both state and non-state actors are equally unsafe, because what precisely their "arms" might be is presently unclear, much less whether such arms may be carried openly when they conduct their operations against other sovereign states. Moreover, what precisely would constitute affiliation with a state or non-state actor under the Geneva Conventions is a muddled question at best. A detaining state may argue that the individuals perpetrating the attack were "lone wolf" attackers, or only loosely affiliated; a detained cyber-soldier may wish to bolster or deny his argument for connection with the entity on whose behalf the detainee operated; and the entity who encouraged or ordered the cyber-attack may have strong reasons to distance itself and disavow any connection. The result is a potential loophole in international humanitarian law that detaining states may seek to use to their advantage.

At the time when the international community enacted the Geneva Conventions, it faced a similar conundrum: how to deal with the sorts of ragtag militias and partisan groups that resulted when previously sovereign states became occupied?[197] It

---

[196] *See* Jake Sher, *A New UN Convention to Govern a New War Front?* PACE INT'L L. REV. BLOG (Oct. 21, 2014), http://pilr.blogs.law.pace.edu/2014/10/21/a-new-un-convention-to-govern-a-new-war-front/; *see also* Walker, *supra* note 85 (quoting Atlantic Council Board Director General Wesley Clark) ("We're doing it all of the time. So is everybody else; because, I hate to say this, you can't wait 'til the next war to discover what the enemy's cyber vulnerabilities are and what his nodes are.").

[197] *See* Commentary on Third Geneva Convention, *supra* note 43, at 49.

chose to enact treaties that would protect those individuals, provided they met certain standards. The international community faces a similar challenge in cyberspace today. If, as the Third Geneva Convention's drafters intended,[198] it can use a teleological approach to clarify the proper means by which states must conduct cyber-attacks and operations, many of the problems that an armed cyber-conflict poses could be brought to easy resolution. To await the question is ill-advised.

The Tallinn Manual and most legal scholarship on the issue of humanitarian law in cyber-conflict have presented more of a restatement of the present law than a true resolution. However, the Tallinn Manual poses at least one potential solution to the issue of what carrying arms openly in cyber warfare could mean. Read together, Rules 22 and 26 suggest that members of the armed forces who are party to an "international armed conflict" rescind entitlements to combatant immunity and prisoner of war status when they fail to comply with the requirements of combatant status in cyber operations.[199] Thus, the key to one's status as a combatant may not be whether one is in uniform; it could turn, rather, on whether one adheres to the rules of engagement. Given the nature of cyber warfare, this makes more sense than the present arrangement. It is much easier to discern whether an individual has navigated within accepted rules of *jus in bello* in cyberspace, because their activities may be captured, tracked, or recorded using the patterns of data executed by their activities.[200]

This legal standard would provide a strong enough evidentiary requirement to protect those who follow the rules of engagement, and to punish those who fail to do so. More importantly, however, the modern theater of war requires a significant improvement to the convoluted analysis that would apply at present under the Geneva Conventions. Absent a new standard governing the law applicable to cyber-combatants, activities in the first cyber-conflict will likely be adjudicated in the same manner as those of partisans were in the wake of the

---

[198] *See id.* at 61.

[199] TALLINN MANUAL ON THE INTERNATIONAL LAW APPLICABLE TO CYBER WARFARE, *supra* note 32, at 79, 96.

[200] *See, e.g.*, Barbash, *supra* note 130 (noting the use of a predecessor program to track such data).

Second World War: retroactively.