Ilkogretim Online - Elementary Education Online, 2018; Vol 17 (Issue 3): pp. 1790-1803
http://ilkogretim-online.org

Cyber Warfare And Protection Of Civilian Under International Humanitarian Law

Mian Muhammad Sheraz Ph.D. Law Scholar, Department of Law, Faculty of Shariah & Law, International Islamic University Islamabad, Pakistan, Email Id: sheeji333@gmail.com

Fazli Dayan PhD, (Islamic Law & Jurisprudence), and Visiting Assistant Professor, Faculty of Shariah & Law, International Islamic University, Islamabad, Pakistan, Email Id:dayansherpao@gmail.com

Abstract

Cyberspace is shared by the people and military both, and cyber warfare is developing a fifth domain of warfare. The intricate cosmos of cyber warfare nurtures several queries regarding the meanings, variances with other warfare and compatibility with jus ad bellum and jus in bello. The solution of some queries lies in construal of existing law armed conflict and others remain open and without an obvious solution. In this paper we will shed some light on those queries whether current international legal regime can cope with the new form of warfare which has already developed as a fifth domain of warfare.

Keywords: cyber space, cyber warfare, jus ad bellum, jus in bello

I. Introduction

Certainly, in the present day Cyber security became main priority on the agenda of foreign policy makers of world. A recently published study by the United Nations Institute for Disarmament Research (UNIDR) tells "the measures taken by thirty-three states that have specifically included cyber warfare in their military planning and organization, and gives an overview of the cyber security approach of thirty-six other states".[1] A number of states are setting up specialized units in or outside of their armed forces to deal with cyber operations.[2] It has also been reported that twelve of the world's fifteen largest military forces are building cyber warfare programs.[3]There is no blinking in fact that in case of cyber-attack victim state is able to identify the origin of the attack

[1] Center for Strategic and International Studies, Cyber security and Cyber warfare– Preliminary Assessment of National Doctrine and Organization, UNIDIR Resources Paper, 2011, available at: http://www.unidir.org/files/publications/pdfs/cybersecurity-and-cyberwarfare-preliminary-assessment-of-national-doctrineandorganization-380.pdf; see also, EnekenTikk, Frameworks for International Cyber Security, CCD COE Publications, Tallinn, 2011.

[2] See, e.g., Ellen Nakashima, 'Pentagon to boost cyber security force', in The Washington Post, 27 January 2013; Gordon Corera, 'Anti-cyber threat centre launched', in BBC News, 27 March 2013.

[3]Scott Shane, 'Cyber warfare emerges from shadows of public discussion by US officials', in The New York Times, 26 September 2012, p. A10.

and also is in position to avail several remedies. Firstly, it could refer matter to the Security Council under Article 35 Para. 1 of the UN Charter[4] and the Security Council may adopt the methods to settle the dispute as mention in Article 36 Para 1.[5] If the Security Council is in opinion that the situation amounts to a threat or breach of peace or act of aggression, it may exercise its powers under Chapter VII (Article 39 to 51). Secondly remedy for victim state which might also be brought before an international tribunal (for instance, the ICJ) in order to obtain remedy for the violation of Article 2 Para 4 and the principle of non intervention.[6] If the Security Council is in opinion that a cyber attack as a threat to the peace, it will be able to adopt recommendations under Article 39,[7] measures to prevent the worsening of the crisis under Article 40 and measures involving or not involving the use of force under Arts 41 and 42. Other remedy under Article 51,[8] of the UN Charter or under customary international law right

[4]Article 35 "Any Member of the United Nations may bring any dispute, or any situation of the nature referred to in Article 34, (Article 34 The Security Council may investigate any dispute, or any situation which might lead to international friction or give rise to a dispute, in order to determine whether the continuance of the dispute or situation is likely to endanger the maintenance of international peace and security) to the attention of the Security Council or of the General Assembly."

[5] Article 36 "The Security Council may, at any stage of a dispute of the nature referred to in Article 33 (Article 33"the parties to any dispute, the continuance of which is likely to endanger the maintenance of international peace and security, shall, first of all, seek a solution by negotiation, enquiry, mediation, conciliation, arbitration, judicial settlement, resort to regional agencies or arrangements, or other peaceful means of their own choice".)The Security Council shall, when it deems necessary, call upon the parties to settle their dispute by such means. Or of a situation of like nature, recommend appropriate procedures or methods of adjustment".

[6] Article 2 "the Organization and its Members, in pursuit of the Purposes stated in Article 1, shall act in accordance with the following Principles. All Members shall settle their international disputes by peaceful means in such a manner that international peace and security, and justice, are not endangered. All Members shall refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any state, or in any other manner inconsistent with the Purposes of the United Nations.

[7] The Security Council shall determine the existence of any threat to the peace, breach of the peace, or act of aggression and shall make recommendations, or decide what measures shall be taken in accordance with Articles 41 and 42, to maintain or restore international peace and security. Article 40 "In order to prevent an aggravation of the situation, the Security Council may, before making the recommendations or deciding upon the measures provided for in Article 39, call upon the parties concerned to comply with such provisional measures as it deems necessary or desirable. Such provisional measures shall be without prejudice to the rights, claims, or position of the parties concerned. The Security Council shall duly take account of failure to comply with such provisional measures". Article 41 "The Security Council may decide what measures not involving the use of armed force are to be employed to give effect to its decisions, and it may call upon the Members of the United Nations to apply such measures. These may include complete or partial interruption of economic relations and of rail, sea, air, postal, telegraphic, radio, and other means of communication, and the severance of diplomatic relations".

[8] Article 51 "nothing in the present Charter shall impair the inherent right of individual or collective self-defence 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". "Measures taken by Members in the exercise of this right of self-defence shall be immediately reported to the Security Council and shall not in any way affect the authority and responsibility of the Security Council under the present Charter to take at any time such action as it deems necessary in order to maintain or restore international peace and security".

of self-defense is available to victim state if one should conclude that a cyber attack triggers the right to self-defense. A plane reading of article 2 (4) brings issues that why at time of drafting 'use of force' only in the specific article, as opposed to 'armed force', 'armed attack' or 'act of aggression', which are used in other parts of the Charter? Whether sanctions regarding economic and political establish a 'use of force'? And what is a 'use of force'? Does a cyber-force fall within this threshold?

An International Information Security Code of Conduct in September 2011proposed by Secretary-General of the United Nations (UN), China, the Russian Federation, regarding cyber conflict with wider scope than just for situations of armed conflict.[9]An agreement adopted in the framework of the Shanghai Cooperation Organization in 2009[10]where India, the Islamic Republic of Iran, Mongolia, and Pakistan participated as observers agreement shows that it appears to enlarge the concepts of 'war' and 'weapon' beyond their traditional meaning in international humanitarian law (IHL).[11]There is conflict among states whether international humanitarian law is applicable in cyber attack some states, like the US,[12] Australia,[13] the United Kingdom of Great Britain and Northern Ireland,[14] have stated that IHL applies to cyber warfare.[15] However, yet to determine detail about questions such as the threshold for armed conflicts, the definition of 'attacks' in IHL, or the implications of cyber warfare. Although, China does not accept the applicability of IHL to cyber warfare.[16]

II. China and Russian Footing Regarding Application of Humanitarian Law: An Overview

[9]Letter dated 12 September 2011 from the Permanent Representatives of China, the Russian Federation, Tajikistan, and Uzbekistan to the United Nations addressed to the Secretary-General, UN Doc. A/66/359 of 14 September 2011.

[10] Agreement between the Governments of the Member States of the Shanghai Cooperation Organisation on Cooperation in the Field of International Information Security.

[11] Available at: http://media.npr.org/assets/news/2010/09/23/cyber_treaty.pdf. Annex 1 defines 'information war' as a 'confrontation between two or more states in the information space aimed at damaging

[12] Harold Koh, 'International law in cyberspace', speech at the US Cyber Command Inter-Agency Legal Conference, 18 September 2012, available at: http://opiniojuris.org/2012/09/19/harold-koh-oninternationallaw-in-cyberspace/; Report of the Secretary-General on Developments in the field of information and telecommunication in the context of international security (hereinafter 'Report of the Secretary-General'), 15 July 2011, UN Doc. A/66/152, p. 19;

[13] Ibid. p 6

[14] Report of the Secretary-General, 23 June 2004, UN Doc. A/59/116, p. 11; Report of the Secretary-General,20 July 2010, UN Doc. A/65/154, p. 15.

[15] See also, the proposal by the High Representative of the European Union for Foreign Affairs and Security Policy, Joint Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions – Cyber Security Strategy of the European Union: an Open, Safe and Secure Cyberspace, Brussels, 7.2.2013, JOIN (2013) 1 final.

[16] See, e.g., Adam Segal, 'China, international law and cyber space', in Council on Foreign Relations,2 October 2012, available at: http://blogs.cfr.org/asia/2012/10/02/china-international-law-and-cyberspace/.

China's stance is that the world should enjoy the value of cyber space. Its view is that "the current UN Charter and the existing laws not only dealing armed conflict but also reflects basic principles of International Humanitarian Law because it relates to war and the use or threat of force so applicable to cyberspace – like 'no use of force' and 'peaceful settlement of international disputes' imperatives as well as the principles of distinction and proportionality in regards to the means and methods of warfare".[17]As far as can be seen, the Russian Federation has not taken an official stance on the applicability of IHL to cyber warfare.[18]

It is also fact that only in case of armed conflicts; the rules of IHL apply, imposing specific restrictions on the parties to the conflict.[19] The International Committee of the Red Cross' (ICRC) humanitarian concern in regard of cyber warfare focus on the impact on the civilian population, in particular because cyber operations could seriously affect civilian infrastructure because of increasingly pervasive reliance on computer systems, civilian infrastructure is highly vulnerable to computer network attacks. No doubt number of critical installations, such as dams, power plants, , distribution systems, oil refineries, gas and oil pipelines, nuclear plants, hospital systems, banking systems, railroads, and air traffic control rely on so-called supervisory control and data acquisition (or SCADA) systems and distributed control systems (DCS). These systems, which constitute

[17] Li Zhang, 'A Chinese perspective on cyber war', in this edition. In his speech to the First Committee in September 2011, China's Ambassador stated that China proposed that countries 'commit themselves to non-use of information and cyber technology to engage in hostile activities to the detriment of international peace and security, and to non-proliferation of information and cyber weapons' and 'work to keep information and cyber space from becoming a new battlefield'; there is no mention of IHL. See the statement on information and cyberspace security made by H. E. Ambassador Wang Qun to the First Committee during the 66th Session of the General Assembly, 'Work to build a peaceful, secure and equitable information and cyber space', New York, 20 October 2011, available at: http://www.fmprc.gov.cn/eng/wjdt/zyjh/t869580.htm.

[18] The reported military doctrine of the Russian Federation does not mention IHL with respect to information warfare; see 'The Military Doctrine of the Russian Federation Approved by Russian Federation Presidential Edict on 5 February 2010', available at: http://www.sras.org/military_doctrine_ russian_federation_2010; and neither does K. Giles, above note 7; Roland Heikerö, 'Emerging threats and Russian Views on information warfare and information operations', FOI Swedish Defence Research Agency, March 2010, p. 49, available at: http://www.highseclabs.com/Corporate/foir2970.pdf, reports that the Russian Federation has proposed the "application of humanitarian laws banning attacks on noncombatants and a ban on deception in cyberspace".

[19] For the International Committee of the Red Cross (ICRC), it is important to draw attention to the specific situation of cyber operations amounting to or conducted in the context of armed conflicts – that is, cyber warfare in a narrow sense. This is because the ICRC has a specific mandate under the 1949 Geneva Conventions to assist and protect the victims of armed conflicts. It is also mandated by the international community to work for the understanding and dissemination of IHL. See, e.g., GC III, Art. 126(5), GC IV,Art. 143(5), and Statutes of the International Red Cross and Red Crescent Movement, Art. 5(2)(g).

the link between the digital and the physical worlds, are extremely vulnerable to outside interference by almost any attacker.[20]

III. Understanding the Concept of Cyber Attack

There are several issues regarding Cyber attack firstly it is difficult to define cyber-crime, cyber-attack and cyber warfare secondly issue of attribution it may be from state, individual, or third party due to which application of international law is difficult. An online dictionary defines "cyber crime" as "a crime committed on a computer network".[21] Cyber-crime covers any criminal act dealing with computers and networks and also includes traditional crimes conducted through the Internet. For example; hate crimes, telemarketing and Internet fraud, identity theft, and credit card account thefts are considered to be cyber crimes when the illegal activities are committed through the use of a computer and the Internet.[22]There are numerous categories of cyber attack through virus that change in financial records or incapacitates the stock market,[23] to a false message that causes a nuclear reactor to shut off,[24] or a dam to open,[25] to a blackout of the air traffic control system that results in airplane crashes. It is very difficult to define these incidents as cyber-attacks. There are two approaches firstly by The U.S.A and secondly is adopted by The Shanghai Cooperation Organization. The U.S. National Research Council defines cyber-attack as "deliberate actions to alter, disrupt, deceive, degrade, or destroy computer systems or networks or the information and/or programs resident in or transiting these systems or networks".[26]The Congressional Research Service does provide an official definition but it is not particularly specific: Cyber-warfare is "warfare waged in cyberspace". It can include defending information and computer networks, deterring information attacks, as well as denying an adversary's ability to do the same. It can include offensive information operations mounted against an adversary, or even dominating information on the battlefield".[27] The Joint Chiefs of Staff USA have defined forms of warfare closely related to cyber-warfare. For example, the Joint Chiefs explain that

---

[20] Stefano Mele analyses likely scenarios of interference with different types of military and civilian systems and states that the manipulation of electrical grid management systems is probably the greatest threat at present. See Stefano Mele, 'Cyber warfare and its damaging effects on citizens', September 2010, available at: http://www.stefanomele.it/public/documenti/185DOC-937.pdf.

[21] Cybercrime-definitions from Dictionary.com, http://dictionary.reference.com/

[22] http://www.webopedia.com/TERM/C/cyber_crime.html

[23] Duncan B. Hollis, Why States Need an International Law for Information Operations, 11 LEWIS & CLARK L. REV. 1023, 1042 (2007).

[24] Vida Antolin-Jenkins, Defining the Parameters of Cyberwar Operations: Looking for Law in All the Wrong Places?, 51 NAVAL L. REV. 132, 140 (2008).

[25] Barton Gellman, Cyber Attacks by Al Qaeda Feared; Terrorists at Threshold of Using Internet as Tool of Bloodshed, Experts Say, WASH. POST, June 27, 2002, at A01. 12 General Accounting Office, Air Traffic Control: Weak Computer Security Practices Jeopardize Flight Safety (May 1998). 13 As distinct from cyber-crime. See Part I.B.

[26] comm. On offensive information warfare, et. Al., nat'l res. Council, technology, policy law and ethics regarding u.s. Acquisition and use of cyber attack capabilities (william a. Owens, et. Al. Eds., 2009) [hereinafter NRC REPORT].

[27] Steven A. Hildreth, *Cyberwarfare*, CONGRESSIONAL RESEARCH SERVICE, 16 (June 19, 2001).

"information warfare" includes operations "to influence, disrupt, corrupt, or usurp adversarial human and automated decision making while protecting one's own".[28]("CIA") Director Michael Hayden defines cyber-war as the "deliberate attempt to disable or destroy another country's computer networks".[29]

Former National Security Advisor and Central Intelligence Agency define attack as, the employment of Computer Network Operations (CNO) with the intent of denying adversaries the effective use of their computers, information systems, and networks, while ensuring the effective use of our own computers, information systems, and networks. These operations include Computer Network Attack (CNA), Computer Network Exploration (CNE), and Computer Network Defense (CND).[30]

Approaches taken by the USA departments do not explain difference between a simple cyber-crime and a cyber-attack. Similarly, the Shanghai Cooperation Organization—composed of China, Russia, and most of the former Soviet Central Asian republics, as well as observers including Iran, India, and Pakistan—has adopted a much more spacious means-based approach to cyber-attacks.[31] The Organization has "expressed concern about the threats posed by possible use of new information and communication technologies and means for the purposes incompatible with ensuring international security and stability in both civil and military spheres."It defines an "information war" as "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". Moreover, it identifies the dissemination of information harmful to "social and political, social and economic systems, as well as spiritual, moral and cultural".

With regard to the concept of Cyberspace; the Economist describes cyberspace as the "fifth domain of warfare, after land, sea, air and space".[32] US Department of Defense defines cyberspace as "a global domain within the information environment consisting of the interdependent network of information technology infrastructures, including the Internet, telecommunications

---

[28] JOINT CHIEFS OF STAFF, U.S. DEP'T OF DEF., JOINT PUB. 3-13, INFORMATION OPERATIONS, AT IX (FEB. 13, 2006). [HEREINAFTER JP 3-13]

[29] Tom Gjelten, *Extending the Law of War into Cyberspace*, NPR.COM (Sept. 22, 2010),http://www.npr.org/templates/story/story.php?storyId=130023318.

[30] Jefferey Carr, Inside Ccyber Warfare 176 (2010). Additionally, numerous commentators and scholars have offered their own similar definitions. Government security expert Richard A. Clarke defines cyber-war as "actions by a nation-state to penetrate another nation's computers or networks for the purposes of causing damage or disruption". Richard A. Clarke & Robert K. Knake, Cyber War: The Next Threat To National Security And What To Do About It 6 (2010).

[31] Agreement between the Governments of the Member States of the Shanghai Cooperation Organization on Cooperation in the Field of International Information Security, 61st plenary meeting (Dec. 2, 2008) [hereinafter Shanghai Cooperation Agreement].

[32] <http://www.economist.com/node/16478792> Also, N Solce, Battlefield of Cyberspace: The InevitableNew Military Branch: The Cyber Force, Albany Law Journal of Science & Technology, Vol. 18, Issue 1(2008), pp. 293-324

networks, computer systems, and embedded processors and controllers"[33] Richard Clarke, former US cyber security czar, "Cyberspace is all of the computer networks in the world and everything they connect and control. It's not just the Internet". Let's be clear about the difference. The Internet is an open network of networks. From any network on the Internet, you should be able to communicate with any computer connected to any of the Internet's networks. Cyberspace includes the Internet plus lots of other networks of computers that are not supposed to be accessible from the Internet"[34]

Questionably, at what stage cyber-crime converts into cyber-attack Computer crime, or cybercrime is any crime that involves a computer and a network.[35] The computer may have been used in the commission of a crime, or it may be the target.[36] Cyber-crime convert into cyber-attack when a non-state actor commits an illegal act by means of a computer network, undermines a computer network, and has a political or national security purpose. Take, for example, a hypothetical group of individuals who hacked into the U.S. government's State Department server and shut it down out of disdain for the U.S. government. This instance would fall within the overlap between cyber-crimes and cyber-attacks given that a non-state actor committed the act, for a political or national security purpose, and it undermined a computer network.

Cyber-warfare is distinctive among the three cyber-categories considered here in that cyber-warfare must also constitute a cyber-attack. The first type includes attacks carried out by any actor in the context of an armed conflict, provided those actions could not be considered cyber-crimes, either because they do not constitute war crimes, or do not employ computer-based means, or both. The second type includes attacks carried out by a state actor, which produce effects equivalent to those of a conventional armed attack. Note that this use of force may be either lawful or unlawful; because the actor is a state actor, even unlawful actions do not constitute "cyber-crime". So cyber-attack may be carried out by state or non-state actors, must involve active conduct, must aim to undermine the function of a computer network, and must have a political or national security purpose. Some cyber-attacks are also cyber-crimes, but not all cyber-crimes are cyber-attacks. Cyber-warfare, on the other hand, always meets the conditions of a cyber-attack. But not all cyber-attacks are cyber-warfare. Only cyber-attacks with effects equivalent to those of a conventional "armed attack," or occurring within the context of armed conflict, rise to the level of cyber-warfare.

---

[33] Dictionary of Military and Associated Terms,http://www.dtic.mil/doctrine/dod_dictionary/data/c/10160.html

[34] R Clarke, *Cyber War* (Harper Collins, 2010), chapter 3, available at http://www.richardaclarke.net/cyber_war.php#excerpts

[35] Moore, R. (2005) "Cyber crime: Investigating High-Technology Computer Crime", Cleveland, Mississippi: Anderson Publishing.

[36] Warren G. Kruse, Jay G. Heiser (2002). Computer forensics: incident response essentials. Addison-Wesley. p. 392

IV. Some Famous Cyber-Attacks Distributed Denial of Service Attacks (DDOS)

In April 2007, republic of Estonia suffered a DDOS attack[37] and such attacks often cause mere inconvenience, but this was life threatening consequences—the emergency line to call for an ambulance or a fire truck was out of service for an hour.[38]There was some suspect of Russia's involvement due to the sophistication and scale of the attack.[39] Similarly In 2008 Georgia, when the country found itself unable to communicate with the outside world over the Internet as Russian forces invaded South Ossetia.[40] Despite the early speculations that Russian government was behind the incident shows that the government may simply have been complicit as private hackers openly arranged the attack.[41] Russians are certainly not the only source of DDOS attacks. In July 2009, a number of government and commercial websites in the United States and South Korea were shut down by a DDOS attack. Although South Korea quickly blamed North Korea,[42]the United States was more circumspect.[43] There remain some questions about where the attack originated. This serves to illustrate a common problem for cyber-attacks in general and DDOS attack in particular: By enlisting unsuspecting computers from around the world, botnets spin a web of anonymity around the attacker or attackers, making accurate attribution uniquely difficult. Surreptitiously inputting inaccurate information in a computer system is another form of cyber-attack, known as a semantic attack. More sophisticated than the DDOS attack, a semantic attack causes the computer system to appear to operate normally, even as it fails.[44] In 1999, for example, the United States developed a plan to feed false target data into the Serbian air defense command network, inhibiting Serbia's ability to target NATO aircraft. This attack would have exploited the increasing reliance on computer networks that characterizes modern warfare. In the end, NATO forces abandoned the plan due to legal concerns about collateral damage.[45]

---

[37] Estonia has one of the highest network saturation rates in the world. Richard A. Clarke & Robert K. Knake, Cyber War: The Next Threat To National Security And What To Do About It 6 (2010), 13 (2010).

[38] *Newly Nasty*, THE ECONOMIST,May 24, 2007, *available at* http://www.economist.com/node/9228757?story_id=9228757.

[39] Jeffrey T.G. Kelsey, Note, *Hacking into International Humanitarian Law: The Principles of Distinction and Neutrality in the Age of Cyber Warfare*, 106 MICH. L. REV. 1427, 1429 (2008).

[40]*The Threat from the Internet: Cyberwar*, THE ECONOMIST, July 1, 2010, *available at* http://www.economist.com/node/16481504.

[41]Brian Krebs, *Report: Russian Hacker Forums Fueled Georgia Cyber Attacks*, WASH. POST SECURITY FIX BLOG (Oct. 16, 2008, 3:15 PM), http://voices.washingtonpost.com/securityfix/2008/10/report_russian_hacker_forums_f.html.

[42] Malcolm Moore, *North Korea Blamed for Cyber Attack on South Korea*, THE TELEGRAPH, July 8, 2009, *available at* http://www.telegraph.co.uk/news/worldnews/asia/southkorea/5778176/North-Korea-blamed-for-cyber-attack-on-South-Korea.html.

[43] Officials anonymously leaked qualified reports of U.S. suspicions that the attack emerged in North Korea. *U.S. Eyes N. Korea for "Massive' Cyber Attacks"*, MSNBC.COM (July 9, 2009, 3:31 AM), http://www.msnbc.msn.com/id/31789294/ns/technology_and_science-security.

[44] MARTIN C. LIBICKI,WHAT IS INFORMATION WARFARE? 77 (1995

[45] William M. Arkin, *The Cyber Bomb in Yugoslavia*, WASHINGTONPOST.COM (Oct. 25, 1999), http://www.washingtonpost.com/wp-srv/national/dotmil/arkin.htm.

The Israeli Air Force employed a similar strategy on September 6, 2007 during its air strike against a nuclear facility in Syria. Israeli planes arrived undetected at their targets because of an earlier cyber-attack that compromised the Syrian air-defense system. The exact method of attack is unknown, but Israel apparently fed false messages to the radars, causing them to show clear skies on the night of the strike.[46] Because these cyber-attacks frequently accompany, and facilitate, conventional attacks, attribution is less problematic. The difficulty here is in identifying when a cyber-attack has occurred, since the disruption remains hidden until its kinetic sequel. In 2003, shortly before the invasion of Iraq, the United States infiltrated the Iraqi Defense Ministry email system to contact Iraqi officers with instructions for a peaceful surrender. The messages apparently worked: American troops encountered abandoned military equipment arranged in accordance with the email. This cyber-attack was a "Command and Control Attack"—a term that includes any attack meant to interfere with the enemy's capacity to command and control its troops.

V. The Issue of Attacker-Attribution

In cyber attacks identification of the attacker can play an integral role in ascertaining the nature of an attack Attacker-attribution has historically been less problematic for war than for crime or terrorism. The laws of war require states launching an attack on another state to identify themselves, though this convention is apparently honored more in the breach than in its realization. [47] The location from which an attack is launched can be another clue. Since it is predicated on conduct in the real-world, this approach assumes that the perpetrator of an attack-a crime-was, and still is, physically in the local geographical area.[48] But basic issue is with cybercrimes, a "place" is ambiguous because while attacks may be routed through Internet servers located in China, this does not necessarily mean that they originated in China. It is common for online attackers to use "stepping stones"-computers the attacker controls but that are owned by innocent parties-in their assaults. These "stepping stone" computers can be located anywhere in the physical world because real space is irrelevant to activity in cyberspace. So, while use of the Chinese servers might mean the attacks came from China, it also might mean they did not come from China. Rather, the attacker might be in Russia/India etc it is to mislead the

[46] CLARKE & KNAKE, *supra* note 16, at 1-9.

[47] See Hague Convention No. III Relative to the Opening of Hostilities art. I, Oct. 18,1907, 36 Stat. 2259, 2271, T.S. 598, available at http://www.yale.edu/lawweb/avalon/lawofwar/hague03.htm; Yoram Dinstein, Comments on War, 27 HARV. J.L.
& PUB. POL'Y 877, 885-86 (2004); see also DINSTEIN, supra note 111, at 29-32 (declaration of war is not essential to establish state of war; armed attack suffices). A declaration of war "served the legal function of triggering international law governing neutral and belligerent states **....** William C. Peters, On Law, Wars and Mercenaries: The Case for Courts-
Martial Jurisdiction over Civilian Contractor Misconduct in Iraq, 2006 BYU L. REv. 367, 404 (quoting CURTIS A. BRADLEY & JACK L. GOLDSMITH, FOREIGN RELATIONS LAW 177, 178 (2003)). The United Nations Charter "abolished" war "as a category of international law," so declarations of war no longer serve any legal purpose. See Paul W. Kahn, War Powers and the Millennium, 34 Loy. L.A. L. REv. 11, 17 (2000).

[48] See Brenner, Toward a Criminal Law for Cyberspace, supra note 5, at 65-76.

investigators trying to identify him. Unless and until investigators reliably establish that the attacks originated in Chinese real-space, we cannot predicate attacker-attribution on inferences drawn from the place of attack origin. The problem, for the moment, is in determination of whether an attack is "mere" cyber crime or state-sponsored cybercrime, "mere" cyber terrorism or states sponsored cyber terrorism.

State sponsorship necessarily involves a level of state participation in a cyber attack, but identifying a nation-state's involvement in a less-than cyber warfare attack will surely be difficult. Point of attack origin is unlikely to be helpful in this effort, for at least two reasons.

VI. Whether Cyber Attack is an Armed Attack: an Intrinsic Concern

It is clear, however, that the critical question determining the lawfulness of self-defense is whether or not an armed attack has occurred. Many agree that a cyber-attack may rise to the level of an armed attack.[49] The term "armed attack" is linguistically distinct from and has been interpreted to be substantively narrower than several other related terms.

To the extent that cyber-attacks do not qualify as armed attacks triggering the right of self-defense, countermeasures could potentially take the form of responsive cyber-attacks (provided that they did not constitute a use of force in violation of treaty and customary international law and that the need to induce a return to compliance with international law still exists.[50]

VI.I. Ad Bellum Necessity and Proportionality

In addition to overcoming Article 2(4)'s prohibition on the use of force, a state's use of armed force in response to a cyber-attack must also comply with the jus ad bellum principles of necessity and proportionality under customary international law. The principle of necessity requires that force must be used only as a last resort, when peaceful means, such as a diplomatic settlement, cannot achieve the state's overall aim. Proportionality extends this logic, prohibiting force if the overall scope and intensity of force is excessive in relation to the state's actual or imminent danger.[51] The United States has acknowledged that these principles apply to military responses to cyber-attacks.[52]

---

[49] *See, e.g.*, WHITE HOUSE CYBERSPACE STRATEGY, *supra* note 54, at 14 ("When warranted, the United States will respond to hostile acts in cyberspace as we would to any other threat to our country. All states possess an inherent right to self-defense, and we recognize that certain hostile acts conducted through cyberspace could compel actions under the commitments we have with our military treaty partners.").

[50] *See* OFFICE OF GEN. COUNSEL, DEP'T OF DEF., AN ASSESSMENT OF INTERNATIONAL LEGAL ISSUES IN INFORMATION OPERATIONS (Nov. 1999), *reprinted in* COMPUTER NETWORK ATTACK AND INTERNATIONAL LAW, *supra* note 75, at 459, 484-85 [hereinafter DOD Memo] ("If the provocation is not considered to be an armed attack, a similar response will also presumably not be considered to be an armed attack").

[51] Robert D. Sloane, *The Cost of Conflation: Preserving the Dualism of Jus Ad Bellum and Jus in Bello in the Contemporary Law of War*, 34 YALE J. INT'L L. 47, 108-09 (2009) ("Ad bellum proportionality is . . . parasitic on ad bellum necessity . . . . An act is ad bellum disproportionate if the same ad bellum

VI.II. Jus in Bello

Although a cyber-attack has never instigated an armed conflict, cyber-attacks have been used in wars in response to traditional provocations.. Because cyber-attacks are often not immediately lethal or destructive and may cause only temporary incapacity of network systems, it may be hard to evaluate whether a cyber-attack is proportional. It can also be nearly impossible to distinguish between combatants, civilians directly participating in hostilities, civilians engaged in a continuous combat function, and protected civilians in the context of cyber-attacks. Finally, the ease of masking the source of a cyber-attack makes enforcement of neutrality duties complicated and expensive.

VI.II.I. In Bello Necessity

Although the necessity of a cyber-attack may be difficult to evaluate, this difficulty arises from line-drawing debates that did not originate in cyber-warfare and are not unique to in bello cyber-attack. In bello necessity relates to the concrete military advantage to be gained from a specific hostile act. An individual cyber-attack may be unnecessary if it does not advance the military's objective.

VI.II.II. In Bello Proportionality

The in bello proportionality requirement prohibits "[a]n attack which may be expected to cause incidental loss of civilian life, injury to civilians, damage to civilian objects, or a combination thereof, which would be excessive in relation to the concrete and direct military advantage anticipated"[53]. In cyber attack issue is It is difficult to evaluate whether an attack would be proportional according to the relevant categories of "loss of civilian life, injury to civilians, damage to civilian objects, or a combination thereof," as the typical direct effects of cyber-attacks may be non-lethal or temporary, yet severe.[54]Furthermore, how should the temporary incapacity of critical systems be evaluated?[55] For example, a

---

objective sought by force clearly could have been achieved by diplomacy or another nonviolent strategy at a roughly comparable, or even moderately greater, cost.").

[52]*See* WHITE HOUSE CYBERSPACE STRATEGY, *supra* note 54, at 14 ("[W]e will exhaust all options before military force whenever we can; will carefully weigh the costs and risks of action against the costs of inaction; and will act in a way that reflects our values and strengthens our legitimacy, seeking broad international support whenever possible").

[53] Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflicts (Protocol 1), art. 51(5)(b), June 8, 1977, 1125 U.N.T.S. 3 [hereinafter Protocol Additional I]; see also id. art. 85(3)(b). An indiscriminate attack, defined by excessive effect, is not to be confused with an attack that does not discriminate amongst civilian and military objectives, which is defined by objective, and is prohibited by art. 85(3)(a). See infra Part II.B.3. Some scholars argue that, given the ability to avoid civilian casualties or damage to property and achieve the same military advantage, a state must do so. See DIMITRIOS DELIBASIS, THE RIGHT TO NATIONAL SELF-DEFENSE IN INFORMATION WARFARE OPERATIONS 268 (2007)

[54] Protocol Additional I, supra note 120, art. 57(2)(a)(iii).

[55] Similar questions arise in debates around non-lethal deployments of biological and chemical weapons, such as riot agents. See James D. Fry, Gas Smells Awful: U.N. Forces, Riot-Control Agents, and the Chemical Weapons Convention, 31 MICH. J. INT'L L. 475 (2010); MirkoSossai, Drugs as Weapons: Disarmament Treaties Facing the Advances in Biochemistry and Non-Lethal Weapons Technology, 15 J. CONFLICT & SECURITY L. 5 (2010).

cyber-attack that effectively stops the transmission of information through the Internet might merely inconvenience the populace—or it might result in hospitals being unable to communicate vital information, leading to loss of life. An in bello proportionality analysis requires anticipating the probable consequences of an action, but that may be difficult, if not impossible, in the context of cyber-warfare. Just as cyber-attacks may change the understanding of an armed attack under Article 2(4).

VII. How does IHL Works?

IHL provisions do not specifically mention cyber operations. Because of this, and because the exploitation of cyber technology is relatively new and sometimes appears to introduce a complete qualitative change in the means and methods of warfare, it has occasionally been argued that IHL is ill adapted to the cyber realm and cannot be applied to cyber warfare.[56] However, the absence in IHL of specific references to cyber operations does not mean that such operations are not subject to the rules of IHL. New technologies of all kinds are being developed all the time and IHL is sufficiently broad to accommodate these developments.[57]

VII.I. Types of Armed Conflict under Existing IHL

Notably, under existing IHL, there are two – and only two – types of armed conflict: namely, International armed conflicts and non-international armed conflicts. Instead, some aspects that seem to raise particularly difficult questions with respect to cyber operations will be addressed. IHL prohibits or limits the use of certain weapons specifically (for instance, chemical or biological weapons, or anti-personnel mines). But it also regulates, through its general rules, all means and methods of warfare, including the use of all weapons. In particular, Article 36 of Protocol I additional to the Geneva Conventions provides that: in the study, development, acquisition or adoption of a new weapon, means or method of warfare, a High Contracting Party is under an obligation to determine whether its employment would, in some or all circumstances, be prohibited by this Protocol or by any other rule of international law applicable to the High Contracting Party.[58]

VII.II. The Concept of International Armed Conflicts

Under common Article 2 to the four Geneva Conventions of 1949, an international armed conflict is any 'declared war or any other armed conflict which may arise between two or more States even if the state of war is not recognized by one of them'. There is no further treaty definition of international

[56] Charles J. Dunlap Jr., 'Perspectives for cyber strategists on law for cyber war', in Strategic Studies Quarterly, Spring 2011, p. 81

[57] see Get off my cloud: cyber warfare, international humanitarian law, and the protection of civilians by CordulaDroege* CordulaDroege is the Head of the Operational Law Unit, Legal Division, International Committee of the Red Cross (ICRC). International Review Of Red Cross Volume 94 Number 886 Summer 2012 page 540

[58] See Get off my cloud: cyber warfare, international humanitarian law, and the protection of civilians by CordulaDroegeCordulaDroege is the Head of the Operational Law Unit, Legal Division, International Committee of the Red Cross (ICRC). International Review Of Red Cross Volume 94 Number 886 Summer 2012 page 540

armed conflicts and it is by now accepted that, in the words of the International Criminal Tribunal for the former Yugoslavia (ICTY), an international armed conflict arises 'whenever there is a resort to armed force between States'.[59] The application of IHL depends on the factual situation and not on the recognition of a state of armed conflict by the parties thereto.

The specific question that arises in cyber warfare is whether an international armed conflict can be triggered by a computer network attack in the absence of any other (kinetic) use of force. The answer depends on whether a computer network attack is attributable to the state and amounts to a resort to armed force – a term that is not defined under IHL. It is true that states cannot circumvent their obligations under IHL by their own designation of the act. The application of the law of international armed conflict was divorced from the need for official pronouncements many decades ago in order to avoid cases in which states could deny the protection of this body of rules. This is made clear by common Article 2, as the ICRC Commentary thereto suggests: A State can always pretend, when it commits a hostile act against another State, that it is not making war, but merely engaging in a police action, or acting in legitimate self-defense. The expression 'armed conflict' makes such arguments less easy.[60]

VII.III. The Question of Non-International Armed Conflicts

When it comes to non-international armed conflicts in the cyber realm, the main question is how to differentiate between criminal behavior and armed conflict. It is not rare to hear or read about the actions of hacker or other groups, including groups such as Anonymous or Wiki Leaks, being referred to as 'war'.[61] There are two types of non-international armed conflicts. All non-international armed conflicts are covered by common Article 3 to the Geneva Conventions; in addition, the provisions of Additional Protocol II apply to non-international armed conflicts 'which take place in the territory of a High Contracting Party between its armed forces and dissident armed forces or other organized armed groups which, under responsible command, exercise such control over a part of

[59] International Criminal Tribunal for the Former Yugoslavia (ICTY), Prosecutor v. Tadic, Case No. IT-94-1-A, Appeals Chamber Decision on the Defence Motion for Interlocutory Appeal on Jurisdiction, 2 October 1995, para. 70 (emphasis added). The situations foreseen in Article 1(4) AP I are also considered international armed conflicts for States Party to AP I.

[60] Jean Pictet (ed.), Commentary on the Geneva Convention for the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field, ICRC, Geneva, 1952, p. 32. This is a different question from that of animus belligerendi: isolated acts are sometimes not considered to amount to armed conflict, not because they do not reach a certain level of intensity, but rather because they lack animus belligerendi, for instance accidental border incursions; see UK Joint Service Manual of the Law of Armed Conflict, Joint Service Publication 383, 2004, para. 3.3.1, available at: http://www.mod.uk/NR/rdonlyres/82702E75-9A144EF5-B414-49B0D7A27816/0/JSP3832004Edition.pdf.

[61] See, e.g., Mark Townsend et al., 'Wiki Leaks backlash: The first global cyber war has begun, claim hackers', in The Observer, 11 September 2010, available at: http://www.guardian.co.uk/media/2010/dec/11/wikileaks-backlash-cyber-war; Timothy Karr, 'Anonymous declares cyber war against "the system"', in The Huffington Post, 3 June 2011, available at: http://www.huffingtonpost.com/timothy-karr/anonymousdeclares-cyberw_b_870757.html.

its territory as to enable them to carry out sustained and concerted military operations and to implement this Protocol' (AP II, Art. 1(1)).

VIII. Conclusion

A few States have publicly acknowledged with the help of cyber operations in armed conflicts, and an incrementing number is developing different capabilities for military cyber.[62] The international humanitarian law eventually applies to the cyber operations from a legal point of view and there not be any type of doubt that the respective existing principles apply to the new weapons and methods of warfare.[63] These are completely dependent on information and telecommunications technology. Few changes are needed to be made in the IHL, for ensuring that maximum effectiveness in being gained in the cyber operations for these international armed conflicts. It should include documentation of war crimes, only to be investigated by the international and States courts. The uncivilized acts are needed to be avoided in a cyber attack and international rules and regulations are to be followed effectively.

[62] Connell, Michael, and Sarah Vogler, "*Russia's Approach to Cyber Warfare",* (1Rev). No. DOP-2016-U-014231-1Rev. Center for Naval Analyses Arlington United States, (2017).

[63] Schmitt, Michael N. "*The law of cyber warfare: quo vadis",* Stan. L. & Pol'y Rev. 25 (2014), p.269.