BALTIC JOURNAL OF LAW & POLITICS
A Journal of Vytautas Magnus University
VOLUME 10, NUMBER 1 (2017)
ISSN 2029-0454

DE GRUYTER OPEN

Cit.: *Baltic Journal of Law & Politics* 10:1 (2017): 1–34
http://www.degruyter.com/view/j/bjlp
DOI: 10.1515/bjlp-2017-0001

THE IMPLICATIONS OF TRANSNATIONAL CYBER THREATS IN INTERNATIONAL HUMANITARIAN LAW: ANALYSING THE DISTINCTION BETWEEN CYBERCRIME, CYBER ATTACK, AND CYBER WARFARE IN THE 21ST CENTURY

Hemen Philip Faga

Senior Lecturer; LL.M.
Ebonyi State University, Faculty of Law (Nigeria)

Contact information
Address: Abakaliki, P.M.B. 053, Ebonyi State, Nigeria
Phone: +2348037702042
E-mail address: hemenfaga@gmail.com

Received: August 21, 2016; reviews: 2; accepted: April 6, 2017.

ABSTRACT

This paper is an attempt to draw distinctive lines between the concepts of cybercrime, cyber-attack, and cyber warfare in the current information age, in which it has become difficult to separate the activities of transnational criminals from acts of belligerents using cyberspace. The paper considers the implications of transnational cyber threats in international humanitarian law (IHL) with a particular focus on cyber-attacks by non-state actors, the principles of state responsibility, and the implications of targeting non-state perpetrators under IHL. It concludes that current international law constructs are inadequate to address the implications of transnational cyber threats; the author recommends consequential amendments to the laws of war in order to address the challenges posed by transnational cyber threats.

KEYWORDS

Transnational cyber threats, cybercrimes, cyber-attack, cyber warfare, 21st century

INTRODUCTION

The advent of the internet and its subsequent dominance in virtually all aspects of national and global affairs has created a new threat environment in the international arena. The entire modern way of life, ranging from national socio-economic systems, with the complex interconnectivity of financial institutions, transport, power and other essential infrastructures, to national security systems of most countries is almost entirely dependent on real-time internet connectivity, which is exposed to the vagaries of cyberspace.[1] The reality of global interconnectivity has, however, led to a flood of international security problems related to the use of the internet and the cyberspace.[2] These problems increasingly tend to conflate the different aspects of transnational cyber threats, including cybercrime, cyber-attack and cyber warfare. Therefore, a need arises to distill and distinguish among the three, especially as we move towards the third decade of the twenty-first century.

This need cannot be overemphasized in today's world particularly because of the difficulty of separating the activities of mere transnational criminals from acts of belligerents in the cyberspace. A clearer understanding of the different cyber threats is necessary to circumvent the danger of discordant global responses common among nations and avoid potentially catastrophic consequences of use of force in retaliation or self-defence. This paper, therefore, attempts to define the boundaries between the three concepts, and examine their interrelatedness from the prism of international humanitarian law. It will explore the legal implications of these cyber threats and the attendant state responses to them, as well as the application of principles of state responsibility and attribution of cyber-attacks by

[1] *See* US Department of Defense (DOD), "Strategy for Operating in Cyberspace" (July 2011): 1. *See* also US Department of Defense (DOD), "Quadrennial Defense Review" (2010) (explaining the role of the cyberspace in the control and command of US forces, intelligence, logistics and weapon technology); Melissa E. Hathaway and Alexander Klimburg, "Preliminary Considerations: On National Cyber Security": 1–4; in: Alexander Klimburg, ed., *National Cyber Security Framework Manual* (Tallinn: NATO Cooperative Cyber Defence Centre of Excellence, Estonia Publication 2012) (discussing the global impact of the internet on different aspects of national and global systems, including economy, tourism, health, education, transport, communication etc.).

[2] 'Cyberspace' is generally a global interactive virtual domain that is superimposed on and supersedes the constraints of physical reality but at the same time mimicking the characteristics of the physical domain. *See* Susan W. Brenner, "Is There Such a Thing as 'Virtual Crime'?" *Cal. Crim. L. Rev. 4* (2001): 11; Natasha Solce, "The Battlefield of Cyber Space: The Inevitable New Military Branch – The Cyber Force," *Alb. L.J. Sci. & Tech.* 18 (2008): 296–297. The US DOD Dictionary of Military and Associated Terms define cyberspace as a "global domain within the information environment consisting of the interdependent network of information technology infrastructures, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers". *See DOD Dictionary of Military and Associated Terms* (2001) // http://www.dtic.mil/doctrine/new_pubs/jp1_02.pdf; *see* also Julija Kalpokienė and Ignas Kalpokas, "Hostes Humani Generis: Cyberspace, The Sea, And Sovereign Control," *Baltic Journal of Law & Politics* 5:2 (2012): 137. *See* Peter Dombrowski and Chris C. Demchak, "Cyber War, Cybered Conflict, and the Maritime Domain," *Naval War College Review* 67(2) (2014): 75. *See* also Matt Murphy, "War in the Fifth Domain: Are the Mouse and Keyboard the New Weapons of Conflict?" *Economist* (July 1, 2010).

non-state actors to host states. In order to accomplish these objectives, the paper is divided into three additional sections. Section two analyses the concepts of cybercrime, cyber-attack and cyber warfare and attempts to differentiate and correlate them. Section three considers the various legal issues that arise from transnational cyber threats initiated by non-state actors, which bear directly on different aspects of public international and international humanitarian law such as attribution of responsibility to states and application of the principle of direct participation in hostilities by non-combatants. In section four the paper draws various findings from the discussions already made, and makes concluding remarks and recommendations.

1. DRAWING THE LINE BETWEEN CYBERCRIME, CYBER-ATTACK AND CYBER WARFARE

The terms 'cybercrime', 'cyber-attack', and 'cyber-warfare' have often been used interchangeably without much consideration given to their conceptual meanings, depth and scope. Indeed, the trio is interrelated. Since the beginning of this millennium, the line dividing these triad concepts has been stretched almost to a breaking point. This absence of clarity has so far hindered attempts to fashion out meaningful legal responses to transnational activities related to any one of them. A single cyber activity today may constitute any of these threats depending on who initiated the act, the targeted infrastructure and the intention of the perpetrator. For instance, cyber-attacks are most often initiated using processes that in different circumstances may constitute cybercrime. However, cyber warfare must be initiated by a prior cyber-attack. In fact, it is difficult to say for sure that a particular cyber threat is an attack that necessitates military response by way of self-defence or bilateral (multilateral) criminal investigation and cooperation to dislodge a transnational threat. To understand the interrelatedness of these concepts, it is necessary to consider them separately.

1.1. CYBER-ATTACK

Just as activities that constitute cyber-attack are spread across a wide spectrum of the threat environment known as cyberspace,[3] the definition of cyber-attack itself also varies depending on the perspective of the person defining it.[4]

[3] Julija Kalpokienė and Ignas Kalpokas, *supra* note 2; Peter Dombrowski and Chris C. Demchak, *supra* note 2.
[4] Matthew C. Waxman, "Cyber-Attacks and the Use of Force: Back to the Future of Article 2(4)," *Yale Journal of International Law* 36 (2011): 421–422.

According to the U.S. Army's Cyber Operations and Cyber Terrorism Handbook, a cyber-attack is:

> the premeditated use of disruptive activities, or the threat thereof, against computers and/or networks, with the intention to cause harm or to further social, ideological, religious, political or similar objectives, or to intimidate any person in furtherance of such objectives.[5]

Waxman defines cyber-attack as "efforts to alter, disrupt, or destroy computer systems or networks or the information or programs on them".[6] The German Cyber Security Strategy also defines cyber-attack to involve "an IT attack in cyberspace directed against one or several other IT systems and aimed at damaging IT security – confidentiality, integrity and availability – which may all or individually be compromised".[7] For their part, the UK, instead of defining the term, outlined four different methods of cyber-attack in its National Cyber Strategy, which include "electronic attack", "subversion of supply chain", "manipulation of radio spectrum" and "disruption of unprotected electronics using high power radio frequency".[8] Cyber-attacks aim to achieve four main objectives according to the U.S. Army Training and Doctrine Command Handbook:

> a) Loss of integrity, such that information could be modified improperly;
> b) Loss of availability, where mission critical information systems are rendered unavailable to authorized users;
> c) Loss of confidentiality, where critical information is disclosed to unauthorized users; and,
> d) Physical destruction, where information systems create actual physical harm through commands that cause deliberate malfunctions.[9]

However, after the US Cyber Command was established in 2011, the US Joint Chiefs of Staff published a lexicon in which they defined cyber-attack as:

> A hostile act using computer or related networks or systems, and intended to disrupt and/or destroy an adversary's critical cyber systems, assets, or functions. The intended effects of cyber-attack are not necessarily limited to the

[5] *US Army Training & Doctrine Command, DCSINT Handbook No. 1.02, Critical Infrastructure Threats and Terrorism: Cyber Operations and Cyber Terrorism Handbook* (2005), at VII-2 (hereinafter 'US Army Cyber Operations and Cyber Terrorism Handbook').
[6] Matthew C. Waxman, *supra* note 4. *See* also W.A. Owens, K.W. Dam, and H.S. Lin, eds., *Technology, Policy, Law, and Ethics Regarding US Acquisition and Use of Cyber-attack Capabilities* (National Research Council Report, 2009), 1 ('NRC Report') (which defined 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").
[7] German Federal Ministry of the Interior, *Cyber Security Strategy for Germany* (Berlin: Beauftragter der Bundesregierung für Informationstechnik, 2011), 14-15.
[8] UK Cabinet Office, *The UK Cyber Security Strategy: Protecting and Promoting the UK in a Digital World* (November 2011), 13-14 // https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/60961/uk-cyber-security-strategy-final.pdf.
[9] US Army Cyber Operations and Cyber Terrorism Handbook, *supra* note 5, p. II-1 and II-3.

> targeted computer systems or data themselves…A cyber-attack may use intermediate delivery vehicles including peripheral devices, electronic transmitters, embedded code, or human operators. The activation or effect of a cyber-attack may be widely separated temporally and geographically from the delivery.[10]

The major element in this definition is that the US Cyber Command considers a "cyber-attack" to be a hostile act not only intended to harm vital cyber systems but also other infrastructure related to the use of the cyber system. This definition focuses on the purpose of the attack,[11] and is substantiated by the Tallinn Manual, which defines cyber-attacks as "cyber operation, whether offensive or defensive, that is reasonably expected to cause injury or death to persons or damage or destruction to objects".[12] Following this definition, Hathaway *et al*. defined cyber-attack as consisting of "any action taken to undermine the functions of a computer network for a political or national security purpose".[13] The combined effect of these definitions is that the notion of cyber-attacks equals its conventional equivalent of 'armed attack', which requires some elements of violence against the integrity of the state (purpose) and the consequence of the attack (scale). The use of computer in the definition of cyber-attack is extended beyond the traditional perception of desktops and laptops, to include other devices of artificial intelligence such as devices that control traffic lights and elevators, pressure on water terminals, washing machines, televisions, as well as cell phones.[14]

The functions of a computer network may be undermined in several diverse ways. The two most probable routes are the syntactic and semantic methods. The former utilises worms, viruses, Trojan horses and other similar destructive programmes to undermine a computer's operating system, leading to malfunctioning of end use computers and the network itself.[15] The latter, on the other hand, compromises the programme language on the targeted computer system or network causing it to interpret commands differently thereby affecting the correctness of the information processed or reacted to by the operating

[10] US DOD, "Memorandum for Chiefs of the Military Services, Commanders of the Combatant Commands, Dirs. of the Joint Staff Directories – Joint Terminology for Cyberspace Operations" (November 2011): 5 // http://www.nsci-va.org/CyberReferenceLib/2010-11-joint%20Terminology%20for%20Cyberspace%20Operations.pdf (hereinafter 'DOD Joint Terminology for Cyberspace Operation').
[11] For an alternative view, *see* Steven A. Hildreth, "Cyber warfare," Cong. Research serv., CRS Report for Congress (2001): 16.
[12] See Rules 30 of the Tallinn Manual, Michael N. Schmitt, ed., *Tallinn Manual on the International Law Applicable to Cyber Warfare* (Cambridge: Cambridge University Press, 2013), 106.
[13] Oona Hathaway, *et al.*, "The Law of Cyber-Attack," *Calif. L. Rev. 100* (2012): 820.
[14] Richard A. Clarke and Robert K. Knake, *Cyber War: The Next Threat to National Security and What to do About it* (New York: Ecco, 2010), 70–74.
[15] Vida M. Antolin-Jenkins, "Defining the Parameters of Cyber War Operations: Looking for Law in All the Wrong Places?" *Naval Law. Rev*. 51 (2005): 139.

system.[16] A system under semantic attack may be perceived as operating correctly but "will generate answers at variance with reality".[17] Other methods of cyber-attacks also exist. Although less frequently used, these other methods are not less effective in achieving the objectives proposed in Hathaway's definition, which emphasizes the political or national security purpose of the attacks.[18] An example is the 2003 US cyber operation in Iraq, which constituted a cyber-attack, because it undermined the function of a secured e-mail system causing it to send an email from an unauthorised user.[19]

The 'political or national security purpose' serves to distinguish between mere cybercrimes and cyber-attacks, especially in circumstances where a cyber-activity initiated by a non-state actor would constitute cybercrime in all other respects, except that it is calculated to affect the political or national security objectives of a state. Therefore, the distinguishing feature between cybercrime and cyber-attack is the purpose of the cyber operation, not necessarily the nature of the actors. Non-state actors may very well constitute the victims or perpetrators of a cyber-attack the same way as the government of a state. The definitional element of 'political or national security purpose' signifies that cyber-attacks are operations of a public nature, which are directed essentially against state interests even if they are specifically targeted against private individuals or corporations.

1.2. CYBER CRIME

The term 'cybercrime' has also proven difficult to define,[20] although some features of the crime are widely acknowledged. For instance, cybercrime may only be committed by a non-state actor,[21] by means of a computer system and must have violated a state penal provision or international criminal law.[22] The crime does not seek to undermine the functions of a computer network, or possess a political or national security purpose.[23] Instead, cybercrime is defined simply as "any crime

[16] *Ibid*.: 140.
[17] Martin C. Libicki, "What is Information Warfare?" *Strategic Forum* No. 28 (1995): 2.
[18] Oona Hathaway, *et al.*, *supra* note 13.
[19] *See* Richard A. Clarke and Robert K. Knake, *supra* note 14, 9-10. *See* also Oona Hathaway, *et al.*, *supra* note 13, 839 (noting that the US cyber operation was a command and control cyber-attack, which interfered with the Iraqi capacity to command and control its troops. Shortly before the Iraqi invasion of 2003, the US penetrated the Iraqi Ministry of Defence email system and succeeded in sending email messages to Iraqi soldiers to surrender peacefully. When the invasion commenced, US troops encountered little resistance and they discovered that military equipment were abandoned in the manner instructed in the email).
[20] *See* Sarah Gordon and Richard Ford, "On the Definition and Classification of Cybercrime," *J. Computer Virology*, 1, (2006): 13; Debra Little, John Shinder, and Ed Tittel, *Scene of the Cybercrime: Computer Forensics Handbook* (MA: Syngress Publishing, Inc. Rockland, 2002), 16.
[21] *See* Marco Gercke, *Understanding Cybercrime: Phenomena, Challenges and Legal Response* (ITU: Telecommunication Development Bureau, 2012), 2-3.
[22] Oona Hathaway, *et al.*, *supra* note 13, 833.
[23] *Ibid*., 834.

that is facilitated or committed using a computer network or hardware device".[24] This means that the concept of cybercrime is very broad, covering all sorts of criminal activities perpetrated in cyberspace including, cyber-squatting, online privacy, storage, dissemination of child pornography and other related offences.

The open-ended scope of cybercrimes and especially the wide spectrum of criminal activities in the cyberspace leads to conceptual complications between cybercrime and, particularly, cyber-attacks. Examples of some of the complexities between these two concepts for instance is where a person commits a cybercrime by hacking into an important national database of a country, say a museum or social security system, with a national security or political objective, but fails to actually undermine the database in the process. A second situation is where a non-state actor commits an unlawful act through the use of computer network, which undermines the network but without a political or national security purpose. This can be presented in series of situations, such as where a person hacked a national database of a country, say a museum or national financial system, and in the process undermines the system in order to steal a precious national treasure and sell it for economic gain or steal credit cards. Another scenario could be where a non-state actor becomes involved in the online spreading of terrorist propaganda or distribution of child pornography without undermining the functions of the computer network, and not inspired by a political or national security purpose. These instances demonstrate the complexities and confusion that accompany an attempt to conceptually desegregate and distinguish between cyber-attack and cybercrime.

The Sony incident amply illustrates this difficulty. Sony Corporation in the US, a Japanese company with Headquarters in Tokyo, experienced an attack on its information technology systems on November 24, 2014, which destroyed data and workstations, and released internal emails and other materials. There were speculations that the attack was part of a "9/11-style" terrorist attack on theatres in the US scheduled to show the film 'The Interview', causing some theatres to cancel screenings and Sony to cancel its widespread release. The US Federal Bureau of Investigation (FBI) and the Director of National Intelligence (DNI) attributed the attacks on Sony's internet network and systems to the North Korean government, which denied any involvement, but praised a hacktivist group, called the "Guardians of Peace," for having done a "righteous deed". President Obama referred to the incident as an act of "cyber-vandalism," and publicly pledged to

[24] Sarah Gordon and Richard Ford, *supra* note 20: 14. In addition, some proposed definitions are broad enough to include not only all crimes committed by means of a computer, but also any crime in any way involving a computer as means or target. Debra Little, John Shinder, and Ed Tittel, *supra* note 20, 17 (referring to the Tenth United Nations Congress on the Prevention of Crime and Treatment of Offenders' broad definition of "computer-related crime," as compared to its narrower, means-based definition of "computer crime").

"respond proportionally" to North Korea's alleged cyber assault, "in a place, time and manner of our choosing". The President's categorization of the attack as cyber-vandalism and his pledge of appropriate response raised questions as to the nature of the attack (whether a mere crime, cyber-attack or cyber warfare), the considered 'proportional' response, as well as other issues regarding sovereignty and transboundary cyber-attacks and the motivation of non-state perpetrators of cyber-attacks.

1.3. CYBER WARFARE

The phrase 'cyber warfare' is virtually non-existent in official documents and it lacks international acceptability. In order to define it, the US Department of Defence relied heavily on the concept of computer network operations (CNO),[25] which includes the components of computer network attack (CNA), computer network defence (CND) and computer network exploitation (CNE). Computer Network Attack is defined as "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 networks themselves".[26] Computer Network Defence, on the other hand, is defined as "actions taken to protect, monitor, analyse, detect, and respond to unauthorised activity within the Department of Defence information systems and computer networks".[27] In the case of Computer Network Exploitation, it is defined as "enabling operations and intelligence collection capabilities conducted through the use of computer networks to gather data from target or adversary automated information systems or networks".[28] A combination of these computer network operations results in cyber warfare. Other definitions also support this understanding of cyber warfare. For instance, Billo and Chang define the concept as involving:

> units organized along nation-state boundaries, in offensive and defensive operations, using computers to attack other computers or networks through electronic means...The overall intent is to seek advantage over an adversary by compromising the integrity, confidentiality, or availability of a computing device.[29]

[25] DOD Joint Terminology for Cyberspace Operation, *supra* note 10: 2.
[26] *Ibid.*, 3.
[27] *Ibid.*, 6.
[28] *Ibid.*, 4.
[29] Charles G. Billo and Welton Chang, *Cyber Warfare: An Analysis of the Means and Motivations of Selected Nation States* (Institute for Security Technology Studies, 2004), 17. *See* also Susan W. Brenner and Leo L. Clarke, "Civilians in Cyber Warfare: Conscripts," *Vanderbilt Journal of Transnational Law* 43 (2010): 1028, 1031-1035 (explaining in detail the nature of combat in the cyberspace from both offensive and defensive positions).

Unfortunately, these notions of cyber warfare limit the concept of 'war' strictly within an information technology space at the level of the computer systems and networks.[30] However, a broader understanding of the concept expands its application considerably beyond cyberspace, to include the kinetic effects which may result from cyber operations and attacks on the victim state's critical infrastructure.[31] Thus, Theohary and Rollins defined cyber warfare as "state-on-state action equivalent to an armed attack or use of force in cyberspace that may trigger a military response with a proportional kinetic use of force".[32] The concept is also conceptualised as cyber-attack that causes physical injury or property damage comparable to a conventional armed attack.[33] In this sense, cyber-warfare is distinctive because it first consists of a cyber-attack, which then leads to physical injury or property damage comparable to conventional armed attack. An excerpt from a book by a cyber security expert paints a picture of a typical cyber warfare scenario to include:

> a catastrophic breakdown within 15 minutes. Computer bugs bring down military e-mail systems; oil refineries and pipelines explode; air traffic-control systems collapse; freight and metro trains derail; financial data are scrambled; the electrical grid goes down in the eastern United States; orbiting satellites spin out of control. Society soon breaks down as food becomes scarce and money runs out. Worst of all, the identity of the attacker may remain a mystery.[34]

A complex interrelationship actually exists between the concepts of cyber warfare, cyber-attack and cybercrime. While cyber warfare must first constitute a cyber-attack, the same cannot be said of cyber-crime, which may exist independently of either cyber-attack or cyber warfare. However, in certain

[30] *See*, e.g., Timothy Shimeall, *et al.*, "Countering Cyber War," *NATO Rev*. 49 (2001): 16, 17 ("In a limited cyber war, the information infrastructure is the medium, target and weapon of attack . . ."). See also Steven A. Hildreth, *supra* note 11: 11 (noting the Russian view that cyber warfare involves disrupting enemy computer systems).

[31] *See*, e.g., Arie J. Schaap, "Cyber Warfare Operations: Development and Use under International Law," *A.F. L. Rev*. 64 (2009): 133 (stating that Russia's cyber warfare capability "would disrupt financial markets and…civilian communications capabilities as well as other parts of the enemy's critical infrastructure. It would likely cross boundaries between government and private sectors…Ultimately, an unrestricted cyber-attack would likely result in significant loss of life, as well as economic and social degradation"). *See* also Kevin Coleman, "The Cyber Arms Race Has Begun," *CSO Online* (January 28, 2008) // http://www.csoonline.com/article/print/216991 (defining cyber war as using "attacks on computers . . . to disrupt communications and other pieces of infrastructure as a mechanism to inflict economic harm or upset defences").

[32] John W. Rollins and Catherine A. Theohary, *Cyber warfare and Cyber terrorism: In Brief* (Congressional Research Service (CRS) Report, R43955, March 27, 2015), 1 (The concept of kinetic use of force or warfare "involve[s] the forces and energy of moving bodies, including physical damage to or destruction of targets through use of bombs, missiles, bullets, and similar projectiles"). *See* also Cheng Hang Teo, "The Acme of Skill: Non-Kinetic Warfare" (Air Command & Staff Coll., Wright Flyer Paper No. 30, 2008): 2–3 // http://www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA485268&Location=U2&doc=GetTRDoc.pdf (providing a more detailed description of kinetic warfare).

[33] *See* Susan Landau, "National Security on the Line", *Journal of Telecomm. & High Tech. Law* 4 (2006): 429–31.

[34] Matt Murphy, *supra* note 2 (citing an unnamed book by Richard Clarke, a former White House staffer in charge of counter-terrorism and cyber-security).

circumstances, cyber war may also constitute cyber-crime, especially where cybercrime leads to cyber-attack, which initiates a cyber war or forms part of the offensive processes in a cyber-warfare. In such circumstance, the three concepts are fully integrated, where cyber-crime, cyber-attack and cyber warfare completely interface. However, even assuming this occurs, only non-state actors may be held responsible for cyber operations that straddle the three concepts. This may happen in several instances, first is where a cyber-attack is carried out in the course of an existing armed conflict in a way that undermines the functions of a computer network of the enemy military and governmental establishment, which violates the state's law or international criminal law and is committed by means of a computer system or network.[35] The second instance is where a non-state actor conducts a cyber-attack by means of a computer system or network that brings about a result comparable to a conventional armed attack for political or national security purposes, which then undermines the functioning of a computer network, and is a violation of the criminal law.[36]

2. NON-STATE ACTORS AND THE LEGAL IMPLICATIONS OF TRANSNATIONAL CYBER ATTACKS

2.1. CYBER-ATTACKS AND NON-STATE ACTORS

One of the challenges to the international legal order is the involvement of non-state actors in cyber-attacks. There is no question that this emerging category of international actors (non-state actors) perpetrates more cyber-attacks than states.[37] The main culprits appear to be international terrorist organisations, especially, al Qaeda.[38] For instance, in April 2010, the record of proceedings of a court in a case involving Mohamedou Ould Slahi, a suspected al Qaeda operative, showed that the group had successfully conducted cyber-attacks, one of which was an attack on an Israeli government computer in 2001.[39] The accused revealed during interrogation that al Qaeda used the internet to launch computer attacks,

[35] See Michael N. Schmitt, *supra* note 12, 75 (arguing that when a cyber-attack is carried out as part of an on-going armed conflict, IHL indisputably applies).
[36] Oona Hathaway, *et al.*, *supra* note 13: 836.
[37] *See* Michael A. Vatis, "Cyber Attacks during the War on Terrorism: A Predictive Analysis," *Institute for Security Technology Studies at Dartmouth College, Report OMB No. 074-0188* (September 2001): 5-9 (describing the barrage of cyber-attacks by non-state actors as at 2001 associated with the various conflict systems or particular conflicts including the Pakistani-Indian conflicts, the Israeli-Palestinian conflict, the Yugoslavian conflict and the US-China incidents).
[38] Natasha Solce, *supra* note 2: 293.
[39] *See* Christopher D. DeLuca, "The Need for International Laws of War to Include Cyber Attacks Involving State and Non-State Actors," *Pace Int'l L. Rev. Online Companion* 3 (2013): 291–292. *See* also Alex Kingsbury, "Documents Reveal Al Qaeda Cyber-attacks," *U.S. News* (April 14, 2010) // http://www.usnews.com/news/articles/2010/04/14/documentsreveal-al-qaeda-cyberattacks.

and that al Qaeda "also sabotaged other websites by launching denial of service attacks, such as one targeting the Israeli prime minister's computer server".[40]

Apart from al Qaeda, other terrorist groups like Hamas, Aum Shinrikyo, Hezbollah, and the Armed Islamic Group have reportedly strengthened their computer expertise.[41] In addition, four terrorist organisations in the US – 'Hammerskin Nation', 'Stormfront', 'Aryan Nation', and 'National Alliance' – have proven technology potentials to engage in cyber terrorism.[42] In Britain, authorities prepared for increased cyber-attacks due to the fact that al Qaeda called for a cyber-jihad as a result of the death of Osama bin Laden:[43]

> There will be more cyber terrorism. Groups will continue to benefit from the off-the-shelf technology in planning and conducting attacks, making operations more secure and potentially more lethal. The Internet and virtual space will be strategically vital.[44]

Unfortunately, despite the increasing importance of non-state actors in international relations and their enormous potential to initiate serious cyber-attacks, no provision is made in the international legal regime to govern such attacks. The existing rules have virtually nothing to say about non-state actors and cyber conflicts.[45] The UN Charter is only applicable to cyber-attack if such an attack was launched by a nation-state and the attack amounts to an armed attack.[46] Where a non-state actor (for instance a terrorist organisation) launches a cyber-attack against a state actor (and vice-versa), the Charter would not apply because there are no specific provisions in the Charter addressing cyber-attacks, much less on cyber-attacks or armed attack by non-state actors.

2.2. APPLICATION OF EXTANT INTERNATIONAL HUMANITARIAN LAW (IHL) TO CYBER-ATTACKS

International humanitarian law is an aspect of international law also known as the laws of war or law of armed conflict. It consists of two distinct bodies of law: jus ad bellum and jus in bello. The former consists of legal norms that govern conditions for resort to use of force in international law, including the prohibition of

[40] *Ibid*.
[41] Natasha Solce, *supra* note 2: 299. *See* also Michael A. Vatis, *supra* note 37: 13–14.
[42] See Christopher D. DeLuca, *supra* note 39: 292.
[43] Gerry Smith, "UK Authorities Brace for 'Cyber Jihad' By Al Qaeda after Bin Laden Death," *The Huffington Post* (July 12, 2011) // http://www.huffingtonpost.com/2011/07/12/al-qaeda-cyberjihad_n_895579.html.
[44] U.K. Secretary of State for the Home Dep't, *Contest: The United Kingdom's Strategy for Countering Terrorism* (Her Majesty's Stationary Office, July 2011), 41 // https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/97995/strategy-contest.pdf.
[45] *See* Duncan B. Hollis, "Why States Need an International Law for Information Operations," *Lewis & Clark Law. Review* 11 (2007): 1023, 1093.
[46] *See U.N. Charter*, Article 2(4) and Article 51.

use of force and its exceptions, namely, the right of self-defence and authorisation by the UN Security Council.[47] The latter on the other hand, regulates the nature of force utilised in an armed conflict, which includes persons legitimately entitled to participate in armed conflict, the means and methods used and the rules of targeting.[48] To bring this body of law within the context of cyber-attacks, we must note as earlier explained that not all cyber-attacks amount to cyber warfare. Thus, where a cyber-attack falls short of use of force or armed attack,[49] the question that usually arises is whether such cyber-attack is governed by contemporary international humanitarian law (IHL) or *jus in bello* principles. To resolve this puzzle, it is important to determine the initial question whether a particular cyber-attack may amount to an armed attack in the first place. Generally, this is not an easy task because of the absence of a concrete definition of 'armed attack' in the international law.

To begin with, the test proposed by Jean Pictet is quite instructive even though it relates more to finding out when an armed conflict exists. Under this test, a situation amounts to an 'armed attack' and subsequent 'international armed conflict' under the contemplation of Common Article 2 of the Geneva Conventions,[50] if the use of force is of "sufficient scope, duration, and intensity".[51] The elements of 'scope' and 'intensity' are the most important criteria as concerns the question of determination of an 'armed attack'. An act of 'force' constitutes armed attack if it reaches such intensity and extent as would result to significant loss of lives and monumental destruction of property. A more poignant explanation of armed attack is contained in the U.N. General Assembly resolution on the 'definition of aggression', [52] which likewise does not specifically define the concept, yet it

[47] *U.N. Charter*, Articles 2(4), 42 & 51.
[48] *See* Michael N. Schmitt, "'Attack' as a Term of Art in International Law: The Cyber Operations Context": 284; in: C. Czosseck, R. Ottis, and K. Ziolkowski, eds., *4th International Conference on Cyber Conflict* (Tallinn: NATO CCD COE Publications, 2012).
[49] The concepts of 'use of force' and 'armed attack' as contained in Articles 2(4) and 51 of the UN Charter respectively, are neither defined in the Charter nor any other international instrument. However, the word 'attack' in international humanitarian law refers to a particular category of military operations. Under Article 49(1) of the 1977 Additional Protocol I to the 1949 Geneva Conventions, it is defined as "acts of violence against the adversary, whether in offence or in defence". 'Use of force' on the other hand, from the perspective of jus ad bellum, is a broad concept, which does not necessarily require direct military violence. Thus, not every use of force constitutes an armed attack for the purpose of the exercise of the right of self-defence. *See* Michael N. Schmitt, *supra* note 48: 285-286. *See* generally Manny Halberstam, "Hacking Back: Re-evaluating the Legality of Retaliatory Cyber-attacks," *The Geo. Wash. Int'l L. Rev*. 46 (2013): 212-216 & 221-223.
[50] Article 2 states that: "The present Convention shall apply to all cases of declared war or of any other armed conflict which may arise between two or more of the High Contracting Parties, even if the state of war is not recognized by one of them". *See*, e.g., *Geneva Convention (III) Relative to the Treatment of Prisoners of War*, Aug. 12, 1949, 6 U.S.T. 3316, 75 U.N.T.S. 135 (hereinafter GC III).
[51] *See* Walter Gary Sharp, *Cyberspace and the Use of Force* (Virginia, Falls Church: Aegis Research Corporation, 1999), 60-61.
[52] *See* UN General Assembly, *'Definition of Aggression'*, G.A. Res. 3314, U.N. GAOR, 29th Sess., U.N. Doc. A/RES/3314 (Dec. 14, 1974). The definition of aggression has now received concrete legal backing under the amended ICC Statute. See *Rome Statute of the International Criminal Court*, July 17, 1998, 37 I.L.M. 1002 [hereinafter Rome Statute]. Articles 5(2) and 121 of the Statute provided for a compulsory amended conference after 7 years of coming into force of the treaty, to define the

provides examples of state actions or situations that may amount to armed attack.[53] These situations have gained extensive international acceptability.[54] Unfortunately, both the Pictet's test and the 'definition of aggression' address only traditional use of force, and therefore, are not particularly helpful in ascertaining how and when a cyber-attack constitutes an armed attack. To address this issue, and other questions relating to unconventional uses of force, three separate models are proposed.[55]

The first model is the 'instrument-based approach', which assesses whether the damage caused by a cyber-attack is such that can only be inflicted by a kinetic attack before the development of cyber capabilities.[56] If the damage is one that could only have been inflicted by kinetic attack prior to the advent of cyber capabilities, then it will be regarded as an armed attack. For instance, where a national power grid is shut down by means of cyber-attack, this would be regarded as armed attack because before the development of cyber capabilities shutting down of a national power grid could only be done through bombing or other forms of kinetic attack.[57] The second model, the 'effects-based approach', assesses the overall consequence of the cyber-attack on the victim state to determine if it significantly affects the state's wellbeing, including its political, economic and social infrastructure. Where the answer is positive, an armed attack is deemed to have taken place and the victim state is entitled to respond to it militarily.[58] The third model adopts the 'strict liability' approach where any cyber-attack against critical national infrastructure (CNI)[59] is deemed an armed attack.[60] This model is

international crime of aggression under Article 5(1). The conference was held in Kampala, Uganda in June 2010, which finally adopted the definition of the crime of aggression not too far from the original UN General Assembly 'Definition of Aggression Resolution'. *See* Article 8bis (2) of the amended Rome Convention. *See* the *Review Conference of the Rome Statute of the International Criminal Court*, Kampala, Uganda, May 31-Jun. 11, 2010, U.N. Doc. R/Con./Res.6, Annex I [hereinafter RC/Res.6]. *See* generally, Robert Heinsch, "The Crime of Aggression After Kampala: Success or Burden for the Future?" *Goettingen Journal of International Law* 2 (2010): 713-743; Michael Anderson, "Reconceptualizing Aggression," *Duke Law Journal* 60 (2010): 411.

[53] Article 3(a)-(g) asserts that "acts of aggression", includes invasion, bombardment, attacks on the victim state's armed forces or marine or air fleets and substantial involvement of a state in the activities of irregulars and mercenaries against another state. The provision also contain other examples of use of force that do not necessarily amount to armed attack. *See* also Article 8bis (2) of the Rome Statute. *See* particularly, Dominika Svarc, "Redefining Imminence: The Use of Force Against Threats and Armed Attacks in the Twenty-First Century," *ILSA J. Int'l & Comp. L.* 13 (2006): 172. But *see*, Michael N. Schmitt, *supra*, note 12, 55 (using the scale and effect threshold, argues that not every use of force rises to the level of an armed attack).

[54] *See* Thomas Wingfield, *The Law of Information Conflict: National Security Law in Cyberspace* (Texas: Aegis Research Corp, 2000), 111.

[55] David E. Graham, "Cyber Threats and the Law of War," *Journal of National Security Law & Policy* 4 (2010): 91.

[56] *See* Duncan B. Hollis, *supra* note 45: 1041.

[57] *See* David E. Graham, *supra* note 55: 91. *See* also Yoram Dinstein, "Computer Network Attacks and Self-Defense": 103–105; in: Michael N. Schmitt and Brian T. O'Donnell, eds., *Computer Network Attack and International Law* (Naval War College, International Law Studies, Vol. 76, 2002).

[58] *See* Thomas Wingfield, *supra* note 54, 117–130. *See* also Georg Kerschischnig, *Cyber Threats and International Law* (Eleven International Publishing, 2012), 294.

[59] *The US Critical Infrastructure Protection Act of 2001*, 42 U.S.C.S. §5195c(e) (2006) defines 'critical infrastructure' to mean "systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on

formulated against the backdrop of the catastrophic damage that could arise from attack on critical national infrastructure.[61] Overall, the United States prefers the effects-based approach,[62] although there is consensus among experts that, these models notwithstanding, cyber-attack in special circumstances may constitute armed attacks.[63]

The second task in determining the applicability of the extant regime of international humanitarian law to cyber-attack is to ascertain whether the principles of *jus in bello* governs any aspect of cyber-attack and indeed cyber warfare. On this issue, Swanson notes that due to the lack of physical or kinetic force in cyber-attack, (which is the conventional component of military attack), *jus in bello* principles may not be applicable in cyber warfare because of the absence of an armed conflict as understood in the Geneva Conventions.[64] However, the contents of the Additional Protocols of 1977 [65] to the Geneva Conventions and the commentaries to the Geneva Conventions of 1949 imply that the notion of 'armed conflict' is capable of an expansive interpretation.[66] As we stated earlier, some degree of intensity and duration is required to determine the existence of an armed conflict.[67] However, the underlying element of an armed conflict is the fact that an organised group of persons have taken measures or used force that injured, killed, damaged, or destroyed lives and property.[68] Therefore, cyber-attacks could well amount to armed conflict, if similar consequences flow from the attack. Moreover, the provisions of Article 36 of Additional Protocol I reveals that the drafters of the

security, national economic security, national public health or safety, or any combination of those matters". A 2009 report explained that critical infrastructure of a nation consists of both public and private assets, including banking and finance, electrical grids, oil and gas refineries and pipelines, water and sanitation utilities, telecommunications, and other systems. *See* Stewart Baker, McAfee, Inc., "In the Crossfire: Critical Infrastructure in the Age of Cyber War" (2009): 3 // http://newsroom.mcafee.com/images/10039/In%20the%20Crossfire_CIP%20report.pdf.

[60] *See* Sharon R. Stevens, "Internet War Crimes Tribunals and Security in an Interconnected World," *Transnat'l L. & Contemp. Probs.* 18 (2009): 676.

[61] *See* Walter Gary Sharp, *supra* note 51, 129–131; Sean Condron, "Getting It Right: Protecting American Critical Infrastructure in Cyberspace," *Harv. J.L. & Tech.* 20 (2007): 415–422; Eric Jensen, "Computer Attacks on Critical National Infrastructure: A Use of Force Invoking the Right of Self-Defense," *Stan. J. Int'l Law* 38 (2002): 228–231

[62] *See* Office of General Counsel, Department of Defense, An Assessment of International Legal Issues in Information Operations (May 1999), *reprinted in* Thomas Wingfield, *supra* note 54, 431, 453–454.

[63] *See ibid,* 117–130; Sean Condron, *supra* note 61: 415–422; Eric Jensen, *supra* note 61: 228–231.

[64] *See* Lesley Swanson, "The Era of Cyber Warfare: Applying International Humanitarian Law to the 2008 Russian-Georgian Cyber Conflict," *L.A. Int'l & Comp. L. Rev*. 32 (2010): 314; *see* also Michael N. Schmitt, "Wired Warfare: Computer Network Attack and Jus in Bello," *Int'l Rev. of the Red Cross* 84 (2003): 368-69.

[65] The two Additional Protocols of 1977 are *Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflicts*, June 8, 1977, 1125 U.N.T.S. 3 (hereinafter AP I) and *Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of Non-International Armed Conflicts*, June 8, 1977, 1125 U.N.T.S. 3 (hereinafter AP II).

[66] U.K. Ministry of Defence, *The Joint Service Manual of the Law of Armed Conflict* 3 (Wiltshire: The Joint Doctrine and Concepts Centre, UK, 2004).

[67] Lesley Swanson, *supra* note 64: 314.

[68] *Ibid*.

treaty envisaged future changes in the means and methods of warfare. It provides as follows:

> In the study, development, acquisition, or adoption of a new weapon, means or methods 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.[69]

The 'Martens Clause' in the preamble to the Hague Convention IV of 1907 contains a similar provision:

> Even in cases not explicitly covered by specific agreements, civilians and combatants remain under the protection and authority of principles of international law derived from established custom, principles of humanity, and from the dictates of public conscience.[70]

The implication of the above is that IHL principles of *jus in bello* apply where the effect of a cyber-attack brings the same consequence as the use of kinetic force.[71] Indeed, IHL rules clearly apply in a situation of armed conflict where cyber-attacks are used in combination with kinetic weapons.[72] It is unclear, however, whether IHL would apply where a cyber-attack is the first or sole attack in the conflict. Nevertheless, to ascertain whether IHL applies, the overall effects of the cyber-attack must be taken into consideration.[73] Thus, IHL applies whenever cyber-attacks attributed to a state are more than simply sporadic in nature and intended to cause injury, death, damage, or destruction, or where such consequences are reasonably foreseeable.[74]

Unfortunately, current IHL principles do not adequately regulate cyber-attacks. This is amply exemplified in several recent cyber-attacks, including the 2007 attacks on Estonia's infrastructure,[75] the 2010 Iranian Stuxnet worm attack,[76]

---

[69] AP I, *supra* note 65.
[70] Lesley Swanson, *supra* note 64: 315.
[71] *See* Knut Dormann, "Applicability of the Additional Protocols to Computer Network Attacks," Int'l Committee of the Red Cross (November 19, 2004) // http://www.icrc.org/eng/assets/files/other/applicabilityofihltocna.pdf.
[72] *See* Nils Melzer, "Cyber Operations and Jus in Bello," *Disarmament Forum* (2011): 4.
[73] Lesley Swanson, *supra* note 64: 316.
[74] *Ibid*.: 317.
[75] "Russia Accused of Unleashing Cyber war to Disable Estonia," *The Guardian* (May 17, 2007) // http://www.guardian.co.uk/world/2007/may/17/topstories3.russia4. *See* also Jeffrey Carr, *Inside Cyber Warfare* (CA: O'Reilly Media Inc. 2010), 2–4.
[76] *See* David Albright, Paul Brannan, and Christina Walrond, "Did Stuxnet Take Out 1,000 Centrifuges at the Natanz Enrichment Plant?" Institute for Science and International Security Report (December 22, 2010) // http://isis-online.org/uploads/isis-reports/documents/stuxnet_FEP_22Dec2010.pdf. *See* also "Stuxnet worm 'Targeted High-value Iranian Assets'," *BBC News* (September 23, 2010) // http://www.bbc.co.uk/news/technology-113880184; Manny Halberstam, *supra* note 49: 199–200.

the 2008 cyber-attacks heralding the Russian-Georgian conflict,[77] the 2011 alleged governmental attacks on WikiLeaks, and multiple Chinese cyber-attacks.[78] Although devastating, these attacks did not lead to the type of damage necessary to rise to the level of an armed conflict under current IHL.[79] However, assuming a non-state actor initiates such cyber-attacks and they rise to the level of an armed attack, would *jus in bello* rules apply to the conduct of the non-state actor given that non-state actors are not parties to IHL conventions? The fact that non-state actors are not parties to IHL treaties means that the extant regime of IHL does not adequately address the participation of non-state actors in armed conflict, not least cyber warfare. Thus, it is difficult to perceive, for instance, how the *jus in bello* principles of necessity,[80] distinction,[81] proportionality[82] and humanity[83] would apply in a situation where cyber-attacks are elevated to an armed attack and subsequently armed conflict from the stand point of cyber warfare.[84]

[77] "Georgian Websites Forced Offline in 'Cyber War'," *The Sydney Morning Herald* (August 12, 2008) // http://www.smh.com.au/news/technology/georgianwebsites-forced-offline-in-cyber-war/2008/08/12/1218306848654.htm. *See* also Lesley Swanson, *supra* note 64: 318.

[78] *See* Christopher D. DeLuca, *supra* note 39: 286-290 (for an extensive discussion of those cyber-attacks).

[79] *Ibid*.: 304. The Tallinn Manual also argues that these attacks did not rise to the level of an armed attack (*see* Michael N. Schmitt, *supra* note 12, 57–58).

[80] The principle of 'Military Necessity' from the perspective of jus in bello admits of all direct destruction of life or limb of armed enemies, and of other persons whose destruction is incidentally unavoidable in the armed contests of the war. *See* Articles 14 & 15 of the *Lieber Code, U.S. War Dep't, General Orders No. 100: Instructions for the Government of Armies of the United States in the Field* (April 24, 1863); *reprinted in* Dietrich Schindler and Jiri Toman, eds., *The Laws of Armed Conflicts: A Collection of Conventions, Resolutions and Other Documents*, 4th ed. (Boston: Martinus Nijhoff Publishers, 2004). *See* Burrus M. Carnahan, "Lincoln, Lieber and the Laws of War: The Origins and Limits of the Principle of Military Necessity," *Am. J. Int'l L.* 92 (1998): 213.

[81] The principle of 'distinction' or 'discrimination' requires that combatants and military objectives be distinguished from non-combatants and protected property or places. *See* Article 22 of the Lieber Code, *supra* note 80; Articles 48-52 AP I, *supra* note 65. *See* also Michael N. Schmitt, "The Impact of High Tech and Low Tech Warfare on Distinction": 169, 178; in: Roberta Arnold and Pierre-Antoine Hildbrand, eds., *International Humanitarian Law and the 21st Century's Conflicts: Changes and Challenges* (Lausanne: Ed. Interuniversitaires Suisses-Edis, 2005); Laurie R. Blank, "Taking Distinction to the Next Level: Accountability for Fighters' Failure to Distinguish Themselves From Civilians," *Valparaiso University Law Review* 46(3) (2012): 765.

[82] "Proportionality" in *jus in bello* requires that the anticipated loss of life and damage to property incidental to military attacks must not be excessive in relation to the concrete and direct military advantage expected to be gained. *See* Articles 51(5) and 57(2) of AP I, *supra* note 65. *See* also Samuel Estreicher, "Privileging Asymmetric Warfare (Part II)?: The 'Proportionality' Principle under International Humanitarian Law," *Chi. J. Int'l L.* 12 (2011): 143; Thomas Hurka, "Proportionality in the Morality of War," *Philo & Pub Aff*. 33 (2005): 34; Enzo Cannizzaro, "Contextualizing Proportionality: Jus Ad Bellum and Jus in Bello in the Lebanese War," *Int'l Rev. Red Cross* 88 (2006): 785–791.

[83] The principle of humanity in jus in bello prohibits unnecessary suffering in the use of means and methods of warfare during hostilities. It also dictates that military force directed against combatants must avoid or minimise 'unnecessary suffering' of the victims. Thus, it is forbidden to employ arms, projectiles or material calculated to cause unnecessary suffering. *See* Article 35(2) AP I, *supra* note 65. This rule reflects customary international law. *See* Jean-Marie Henckaerts and Louise Doswald-Beck, *Customary International Humanitarian Law* (ICRC, 2005), 244–250; Michael N. Schmitt, "Military Necessity and Humanity in International Humanitarian Law: Preserving the Delicate Balance," *Virginia Journal of International Law* 50(4) (2010): 795.

[84] *See*, however, Charlotte Lülf, "Modern Technologies and Targeting under International Humanitarian Law," *IFHV Working Paper* Vol. 3, No. 3 (December 2013) // http://www.ruhr-uni-bochum.de/ifhv/documents/workingpapers/wp3_3.pdf (arguing that the principles of necessity, distinction, proportionality, humanity apply in cyber-attacks and cyber warfare in the same measure as conventional warfare).

Nevertheless, these fundamental principles of *jus in bello* would apply where a state decides to respond to a cyber-attack by exercising its right of self-defence either by use of kinetic force or taking active defence measures, which may include electronic countermeasures designed to strike at an attacking computer system to halt an attack.[85] The use of active defence measures within cyberspace actually complies with the principle of military necessity because it offers the best option to shut down the attacking computer system.[86] However, the use of kinetic weapons in self-defence as response to cyber-attack may not be very effective in dislodging an on-going cyber-attack and would almost always amount to a disproportionate use of force, which offends the *jus in bello* principle of proportionality. Regarding the principles of humanity (avoidance of unnecessary suffering) and distinction, the trace back capabilities of active defence measures would ensure that only the source of the cyber-attack is targeted thus reducing collateral damage. The specific computer systems, network and cyber infrastructure used to initiate the cyber-attack is a direct and legitimate military objective rather than the use of kinetic force to target perpetrators who may not be distinguishable from civilians.[87]

The use of active defence measures (using cyberspace) as an option of the exercise of self-defence, however, has its shortcomings in the application of IHL to cyber warfare. The technicalities and responsibility involved in tracing an attack pattern in cyberspace routed through intermediary systems is huge. This not only takes time but also gives room for identity mistakes, especially if the attacker terminates the electronic connection that allowed him access to cyberspace.[88] Any measures taken in active defence against a wrong intermediary system is definitely contrary to the *jus in bello* principle of distinction.[89] However, if the tracing is successful, the attacking systems must still be properly mapped for active defence measures to be initiated specifically against them in the cyberspace, otherwise collateral damage arising from any attack may nonetheless be unavoidable.[90] Mapping involves the process of assessing the functions and blueprint of the

[85] David E. Graham, *supra* note 55: 99; *compare* Ruth Wedgwood, "Proportionality, Cyber war and the Law of War": 219, 227–230; in: Michael N. Schmitt and Brian T. O'Donnell, eds., *supra* note 57.
[86] *See*, e.g., Susan W. Brenner, *supra* note 2: 11; *see* generally Natasha Solce, *supra* note 2: 296–97.
[87] Jeffrey T.G. Kelsey, "Hacking into International Humanitarian Law: The Principles of Distinction and Neutrality in the Age of Cyber Warfare," *Mich. L. Rev*. 106 (2008): 1439 ("The highly interconnected nature of the military and civilian networks…renders much of the Internet a dual-use target"); *see*, e.g., Duncan B. Hollis, *supra* note 45: 1044.
[88] *See* Susan Brenner, "At Light Speed: Attribution and Response to Cybercrime/Terrorism/Warfare," *J. Crim. Law & Criminology* 97 (2007): 379.
[89] *See* Ruth Wedgwood, *supra* note 85; *see* also David Wheeler and Gregory Larsen, "Techniques for Cyber Attack Attribution," *Inst. Def. Analysis* (October 2003): 23–25 // http://www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA468859&Location=U2&doc=GetTRDoc.pdf (discussing methods to trace cyber attacks to their source); Jason Barkham, "Information Warfare and International Law on the Use of Force," *N.Y.U. J. Int'l L. & Pol.* 34 (2001): 103–104; Eric Jensen, "Unexpected Consequences from Knock-On Effects: A Different Standard for Computer Network Operations?" *Am. U. Int'l L. Rev*. 18 (2003): 1178–1179.
[90] *Ibid*.

attacking systems to arrive at an informed decision of the likely consequences (resulting damage) that would occur if actions are taken in the cyberspace.[91]

2.3. CYBER WARFARE AND THE CONCEPT OF DIRECT PARTICIPATION IN HOSTILITIES (DPH)

The distinction between combatants and civilians is one of the cardinal foundations of the laws of war.[92] Under the extant regime of IHL, civilians are not subject to attacks unless and until they take a direct part in hostilities.[93] This is enshrined in Additional Protocol I of 1977 in the following words: "civilians shall enjoy the protection of this section [of the Protocol], unless and for such time as they take a direct part in hostilities".[94] The interpretation of the provision had continued to be a subject of controversy until the International Committee of the Red Cross (ICRC),[95] after a 6-year 'clarification process' arrived at a reasonable construction of the provision in a publication known as the 'Interpretive Guidance'.[96] The Guidance itself has remained controversial because some scholars refused to accept it, and the major military powers have chosen to remain mute on its clarifications.[97] However, it remains useful in constructing a set of generally agreed parameters within which the debate about DPH can be conducted.[98]

To bring the discussion of the direct participation of civilians in hostilities within the purview of this paper bordering on cyber-attacks, it is worth noting that a good number of cyber-attacks are actually conducted by non-state actors. Members of these non-state actors are civilians from the standpoint of international humanitarian law. Thus, where non-state actors initiate cyber-attacks that are elevated to armed attack and subsequently lead to cyber warfare or even kinetic armed conflict, individual perpetrators of the attacks are civilians not combatants under the combined effect of Articles 50 and 43 of Additional Protocol I[99] and

[91] David E. Graham, *supra* note 55.
[92] *See* Susan W. Brenner and Leo L. Clarke, *supra* note 29: 1017. *See* also *Advisory Opinion on the Legality of the Threat or Use of Nuclear Weapons,* 1996 I.C.J. para. 79 (July 8) [hereinafter Nuclear Weapons].
[93] *See*, generally, Article 51 of AP II, *supra* note 65 (Article 51(2) states that "the civilian population as such as well as individual civilians shall not be the object of attack. Acts or threats of violence the primary purpose of which is to spread terror among the civilian population are prohibited").
[94] Article 51(3), AP I, *supra* note 65.
[95] *See* Y. Sandoz, C. Swinarski, and B. Zimmermann, eds., *Commentary on the Additional Protocols of 8 June 1977 to the Geneva Conventions of 12 August 1949* (ICRC, 1987), paras. 1942–44.
[96] ICRC, "Interpretive Guidance on the Notion of Direct Participation in Hostilities under International Humanitarian Law," *Intl Rev Red Cross* 90 (2008): 991 ('Interpretive Guidance').
[97] For a flavour of the disagreements and debates, *see* Ryan Goodman and Derek Jinks, "The ICRC Interpretive Guidance on the Notion of Direct Participation in Hostilities under International Humanitarian Law: An Introduction to the Forum", *NYU J Intl L Pol.* 42 (2010): 637–640.
[98] David Turns, "Cyber Warfare and the Notion of Direct Participation in Hostilities," *Journal of Conflict & Security Law* (2012): 286.
[99] Article 50 of API defines 'civilian' as any person who does not belong to one of the category of persons referred to in Article 4 (A)(1), (2), (3) and (6) of the Geneva Convention III and Article 43 of API. Meanwhile, Article 43(2) of the API defines combatant as "members of the armed forces of a Party to a

Article 4 of the Geneva Convention III,[100] unless they satisfy certain criteria. Such as "(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; [and] (d) that of conducting their operations in accordance with the laws and customs of war".[101] On a more subtle level, civilians who do not satisfy these criteria but who continue to take a direct part in hostilities on a regular basis are no longer allowed to enjoy the privileges of civilians; they are considered combatants for the purpose of targeting and detention.[102] The Interpretive Guidance therefore specify three elements to determine when civilians involved in an armed conflict become subject to attack as 'combatants' under the DPH principle. These are the 'threshold of harm', 'direct causation' and 'belligerent nexus':

> 1) *Threshold of harm*: the act of the 'civilian' must be likely to adversely affect the military operations of a party to an armed conflict or, alternatively, to inflict death, injury or destruction on persons or objects protected against direct attack;
>
> 2) *Direct causation*: there must be a direct causal link between the act of the 'civilian' and the harm likely to result either from that act, or from a coordinated military operation of which that act constitutes an integral part;
>
> 3) *Belligerent nexus*: the act must be specifically designed to directly cause the required threshold of harm in support of a party to the conflict and to the detriment of another.[103]

Non-state actors that initiate cyber-attacks and participate in cyber warfare are not only faceless and their identities shrouded in mystery, but also their legal status is often ambiguous under IHL. For example, individual participants in cyber warfare include: (a) those that design and write programmes that are used for offensive or defensive cyber warfare operations; (b) those that install these programmes on computer systems, act as service administrators ('webmasters') and provide technical maintenance for them; and (c) those that actually operate

conflict…". Article 43(1) on the other hand, defines "armed forces of a Party to a conflict" as organized armed forces, groups and units which are under a command responsible to that Party for the conduct or its subordinates, even if that Party is represented by a government or an authority not recognized by an adverse Party…".

[100] GC III, *supra* note 50. Article 4(A)(2) of the Convention broadens the definition of combatant for the purpose of according prisoner of war status to certain persons, including members of the armed forces of a party and members of "other militias and other volunteer corps" who meet certain requirements.

[101] *Ibid.*, Article 4(A)(2)(a)–(d). See also Article 1 Annex, *Hague Convention (IV) with Respect to the Laws and Customs of War on Land*, Oct. 18, 1907, 36 Stat. 2277, 187 Consol. T.S. 429 [hereinafter Hague IV] (which provide the criteria).

[102] These are individual members of non-state actors who perform a 'continuous combat function'. *See* ICRC, *supra* note 96, 33-39. See also Rule 35 of the Tallinn Manual, Michael N. Schmitt, *supra* note 12, 118–122. *See* generally Nil Melzer, "Keeping the Balance between Military Necessity and Humanity: A Response to Four Critiques of the ICRC's Interpretive Guidance on the Notion of Direct Participation in Hostilities," *Int'l L. & Pol*. 42 (2010): 831.

[103] ICRC, *supra* note 96, 995–96.

the computer programmes in a cyber-warfare scenario.[104] From the vantage point of international humanitarian law, these individuals may be either combatants or civilians depending on the circumstances. For instance, it is not uncommon for the military personnel of a party to an armed conflict, which comprise of a cyber-warfare component to make up any one of the above participants; or such individual participant to comprise of members of Militia forming part of the armed forces of a party to the conflict.[105] In this case, the participants are clearly combatants under the law of armed conflict as defined in the Hague Regulations[106] and Geneva Convention III.[107] Conversely, civilians involved in designing harmful programmes and operating computer systems used for cyber-attacks may form the narrow category of 'civilians accompanying the armed forces'[108] or in special circumstances, considered as 'scientist' or 'weapon experts' whose expertise is decisive in tilting the advantage in the conflict in favour of a party.[109] In these cases, such civilians may both be eligible for prisoner-of-war status and legitimate military targets for the enemy even if they did not actually press the button that launched the cyber-attack, as their roles either directly or indirectly contribute to the overall military advantage of a party to the conflict.[110]

Apart from these clear cases, the legal status of other individual participants in a cyber-attack or cyber warfare that has been elevated to an armed conflict is evaluated using the DPH principle. It is difficult in this regard to prove cumulatively all the three elements of DPH in order to satisfy the criteria of targeting individual members of non-state actors with kinetic force as combatants. Activities that constitute cyber-attack do not often satisfy the 'threshold of harm', which involves

[104] David Turns, *supra* note 98: 289.
[105] *See* Shane Harris, "The Cyber war Plan," *National Journal* (November 14, 2009) // http://www.nationaljournal.com/njmagazine/cs_20091114_3145.php (Raising concern however, about the status of civilian experts who may be co-opted by the military or Militia belonging to a party in the conflict, to protect both civilian and military infrastructure in the cyberspace or initiate counterattacks). *See* also Joshua E. Kastenberg, "Non-intervention and Neutrality in Cyberspace: An Emerging Principle in the National Practice of International Law," *A.F. L. Rev*. 64 (2009): 62.
[106] Article 1, *Hague Regulations Respecting the Laws and Customs of War on Land (Annex to The Hague Convention IV Respecting the Laws and Customs of War on Land, 18 October 1907)*, 36 Stat. 2277, 187 Consol. T.S. 429. The armed forces as such are not defined, but 'militia and volunteer corps' fulfilling the conditions of being under responsible command, having a fixed distinctive emblem recognizable at a distance, carrying arms openly, and conducting operations in accordance with the LOAC, are considered equally to be combatants.
[107] Prisoners of war are defined *inter alia*, as "members of the armed forces or of militias or volunteer corps forming part of the armed forces, and members of other militias (including organized resistance movements) that satisfy the requirements of Article 1 of The Hague Regulations: Article 4(A)(1)–(2), GC III, *supra* note 100.
[108] Article 4 (4), GC III, *supra* note 100 (civilians authorised to accompany the armed forces in an international armed conflict who do not take a direct part in hostilities remain civilians for the purpose of targeting, although if captured, they may enjoy the status of prisoner of war).
[109] David Turns, *supra* note 98: 291–292. *See* also Nils Melzer, *supra* note 72: 8.
[110] *See* W.A. Owens, K.W. Dam, and H.S. Lin, *supra* note 6, 266 (fn.25). *See* also M.N. Schmitt, H.A. Dinniss, and T.C. Wingfield, "Computers and War: The Legal Battle Space," Background Paper prepared for Informal High-Level Expert Meeting on Current Challenges to International Humanitarian Law, Cambridge (June 25–27, 2004): 10 // http://www.hpcrresearch.org/sites/default/files/publications/schmittetal.pdf.

military violence that adversely affects the operations or military capabilities of a party to the conflict.[111] The Interpretive Guidance provides that the specific act constituting DPH must be likely to cause death, injury or destruction;[112] thus, even if cyber-attack causes high inconveniences pertaining to public security, health and commerce, this may not in the absence of adverse military effects, result in the degree of harm required to qualify as direct participation in hostilities.[113] No doubt, there is a fine line between cyber-attacks that cause inconvenience on a massive scale and those that directly lead to death or destruction, or have adverse effect on military operations.

Regarding the element of 'direct causation', the Interpretive Guidance requires that the effect (harm) of the act in question must be brought about in one causal step, relegating to the background acts in which the causal chain of events is interrupted.[114] From the perspective of cyber warfare, this element is very difficult to fulfil because of the series of steps that the immediate effect of a particular cyber-attack would have to undergo to result in any degree of physical harm like death, injury or destruction.[115] Direct causation can be proven even in the absence of death or physical harm, if the cyber-attack directly affects military operations or the military capacity of the adverse party in the conflict. For instance, cyber operations, which aim to disrupt or incapacitate an adversary's radar or weapons systems, logistic supply or communication networks, would certainly qualify as direct participation in hostilities even if they do not directly cause any physical damage.[116] However, the element of the 'belligerent nexus' is the easiest to fulfil, because cyber warfare is a specialised activity that is easily integrated into the operations of most countries' militaries. In fact, most contemporary militaries have fully integrated cyber capabilities as a specialised command in the overall military formation; the US, for instance, has had a cyber military command since 2011.[117]

[111] See David Turns, *supra* note 98: 294-295 (tabulating activities of participants in cyber warfare that do or do not satisfy the threshold of harm).
[112] ICRC, *supra* note 96: 1018.
[113] *Ibid*.: 1019.
[114] *Ibid*.: 1021–22.
[115] *See* W.A. Owens, K.W. Dam, and H.S. Lin, *supra* note 6, 127, 268–70.
[116] *See* Nils Melzer, *supra* note 72: 8.
[117] Peter Dombrowski and Chris C. Demchak, *supra* note 2: 74 (noting that cyberspace was added as the fifth domain of US nonphysical arena of military conflict, including land, sea, air, space and cyber). *See* also US DOD, "Strategy for Operating in Cyberspace," *supra* note 1, 5 (establishing the U.S. Cyber Command USCYBERCOM as a sub-unified command of USSTRATCOM); Michael N. Schmitt, "Rewired Warfare: Rethinking the Law of Cyber Attack," *Int'l Rev. Red Cross* Vol. 96 (893) (2014): 190 (noting that China has also established a cyber command in its military formation).

2.4. CYBER-ATTACK AND THE TWIN CONCEPTS OF STATE RESPONSIBILITY AND ATTRIBUTION OF CONDUCT TO STATES

As stated, earlier non-state actors have been the main perpetrators of cyber-attacks in the recent past. Their principal targets have been both states' and non-states' critical infrastructure. The problem is that these non-state perpetrators of cyber-attacks are shadowy organisations, which can hardly be the subject of any comprehensive exercise of self-defence measures by state victims, especially where the consequences of the attacks rise to the level of an armed attack under international law.[118] Given that non-state actors operate from within the territories of other states, the question usually arise as to what responsibility these host states bear for transnational cyber-attacks on other states' infrastructure, and the degree of attribution of those attacks on the host states. A related controversy is whether non-state actors themselves could be held responsible for 'armed attack' and, consequently, whether they could constitute the object of the exercise of the right of self-defence under international law.[119] This controversy has become even more difficult to resolve in the context of cyber warfare because of the nature of the cyberspace itself, the volatility of any active defence measures by victim states (whether in counter-offensive or counter-defence) and the possibility of such measures causing damage to other states or individual private computers and cyber network infrastructure.[120]

The nature of cyberspace has made the attribution of cyber-attacks to states a herculean task. Cyber-attacks are often conducted by experts skilled in the art of disguise and therefore such operations are usually difficult to trace to any particular country, let alone a particular organisation or individual.[121] This difficulty associated with identification of perpetrators has rendered the traditional thresholds for attribution of conducts to states under international law inapplicable in cyber-attacks and cyber warfare. Thus, the 'effective control' criteria established in the *Nicaragua case*,[122] and the 'overall control' test recognised in the *Tadic case*,[123] are

[118] *See* Matthew Hoisington, "Cyber warfare and the Use of Force Giving Rise to the Right of Self-Defense," *B.C. Int'l & Comp. L. Rev.* 32 (2009): 446–452.
[119] For a good treatment of this issue, *see* Michael Schmitt, "Pre-emptive Strategies in International Law," *Mich. J. Int'l* Law, 24 (2003): 540–543.
[120] Sean Condron, *supra* note 61: 415; Yoram Dinstein, *supra* note 57: 111.
[121] Eric Jensen, *supra* note 61: 207. *See* also Matthew Hoisington, *supra* note 118: 452.
[122] *Military and Paramilitary Activities in and Against Nicaragua (Nicaragua v. U.S.)*, 1984 I.C.J. Rep. 392) (the ICJ described 'effective control' to mean that the non-state perpetrator of armed attack acts under the 'direction' and 'instruction' of the responsible state). *See* Davis Brown, "Use of Force Against Terrorism After September 11th: State Responsibility, Self-Defense and Other Responses," *Cardozo J. of Int'l & Comp. Law* 11 (2003): 10, 16.
[123] *Prosecutor v. Tadić*, Case No. IT-94-1-A, I.C.T.Y. App. Ch., at 49 (July 15, 1999) (the 'overall control' test lowered the threshold of attribution of acts of non-state groups to states. The Appeal Chamber of the ICTY described 'overall control' as involving the participation of the state in the planning and supervision of military operations; *ibid*, p. 145). *See* Shane Darcy, "Assistance, Direction and Control:

not feasible for attribution of cyber-attacks to states, as far as the identities of the perpetrators may not be accurately known. State victims of cyber-attacks are therefore often forced to employ 'passive computer security measures' in response to attacks (which is largely inadequate), in addition to demands on the State from which the attack came, to conduct an investigation and prosecute the attackers. Thus in practice, states avoid relying on 'conclusive attribution' of cyber-attacks to other states unless there is overwhelming evidence of state involvement.[124]

Although such proof is usually very difficult to find, state victims may rely on 'imputed responsibility'[125] to sustain attribution of cyber-attacks arising from the territory a state, to that state. Imputed state responsibility is premised on the failure of the state to implement the duty to prevent its territory from being used to attack other states.[126] Therefore, where a state is indifferent as to the continuous use of its territory to conduct cyber-attacks and it fails to investigate such attack or prosecute the alleged attackers, a presumption of collaboration with the attackers is usually made against it, and the attacks may be impliedly attributed to the state.[127]

CONCLUDING REMARKS

We have been able to uncover the fact that current IHL rules do not address the phenomena cyber-attack, cyber warfare and other allied issues. The increased number of cyber-attacks linked to non-state actors to which IHL does not apply exacerbates the problem posed by these concepts. Gone are the days when kinetic warfare was the principal method to cause massive destruction, injury and death. Today, state and non-state actors (including civilian cyber warriors) fight in a different battlefield (cyberspace) where they use computer-generated weapons. Thus, the very technologies that empower nations to lead and create a new world also empower people to disrupt and destroy the socio-economic system that relies

Untangling International Judicial Opinion on Individual and State Responsibility for War Crimes by Non-state Actors," *International Review of the Red Cross* 96(893) (2014): 259–261.

[124] *See* Eric Jensen, *supra* note 61: 236–237; Jason Barkham, *supra* note 89: 103–104.

[125] *See* Matthew J. Sklerov, "Solving the Dilemma of State Responses to Cyber-attacks: A Justification for the Use of Active Defenses against States Which Neglect Their Duty to Prevent," *Mil. L. Rev*. 201 (2009): 38–39.

[126] *Ibid*.: 62. *See* particularly *Convention on Cybercrime*, Council of Europe, Nov. 23, 2001, 41 I.L.M. 282, 2296 U.N.T.S. 167, which criminalizes cyber-attacks and confirms the duty of states to prevent their territories from being used by non-state actors to conduct these attacks against other states; *Eighth United Congress on the Prevention of Crime and the Treatment of Offenders*, G.A. Res. 45/121, para.3, U.N. Doc. A/RES/45/121 (Dec. 14, 1990); *Combating the Criminal Misuse of Information Technologies,* G.A. Res. 55/63, paras.1,3 U.N. Doc. A/RES/55/63 (Jan. 22, 2001) (which calls on states to criminalize cyber-attacks and prevent their territories from being used as safe havens from which to launch attacks); US White House, *The National Strategy to Secure Cyberspace 49-52* (2003) // http://www.dhs.gov/xlibrary/assets/National_Cyberspace_Strategy.pdf (noting the threat that cyber-attacks pose to international peace and security).

[127] *See* Vincent-Joel Proulx, "Babysitting Terrorists: Should States Be Strictly Liable for Failing To Prevent Transborder Attacks?" *Berkeley J. Int'l L*. 23 (2005): 622-641. *See* also David E. Graham, *supra* note 55: 94–98.

on it.[128] Cyber-attacks and cyber warfare have come to stay and because they are largely unregulated by current IHL, multifarious legal implications attend it. The consequences could be unfathomable, if nothing is done to regulate this new style of combat.

By way of suggestions, this paper makes two recommendations, which are derived from the finding already discussed above. The first notable finding is the fact that traditional international law situates non-state actors outside the borders of both *jus ad bellum* and *jus in bello* principles of humanitarian law. Despite their increasing importance in the matrix of transnational use of force under the present international dispensation, non-state actors remain at the periphery of the system of use of force under the UN arrangement; they can neither initiate an armed attack nor be the object of the exercise of the right of self-defence under traditional international law.[129] Since that the debate about the role and status of non-state actors in *jus ad bellum* is still raging,[130] this paper recommends that this group of participants in contemporary armed conflicts be given recognition under the extant regime of IHL. Recognising non-state actors would resolve the problem of attribution of cyber-attacks to states for the purpose of exercising the right of self-defence and it will advance the UN objective of maintenance of international peace and security.[131]

Secondly, we found that the extant regime of IHL does not give room for belligerent acts in the cyberspace. In fact, the very definition of cyber-attack is devoid of any relationship with either *jus ad bellum* or *jus in bello* principles of humanitarian law. Thus, there is a need to reconstruct the laws of war to expand the notion of armed conflict to cover cyber warfare. To begin with, IHL must clearly define the elements of cyber-attack that would qualify cyber operations as armed attack in international law. The new definition should define the various types of cyber-attacks and be broad enough to incorporate new methods of cyber-attacks. The benefit of such a clear but broad definition cannot be over-emphasised. It will aid in clarifying when a state may resort to its right of self-defence.[132] It will also

---

[128] See the US DOD, "Strategy for Operating in Cyberspace," *supra* note 1: 2.
[129] Norman G. Printer, Jr., "The Use of Force against Non-State Actors under International Law: An Analysis of the U.S. Predator Strike in Yemen," *UCLA J. Int'l L. & Foreign Aff.* 8 (2003): 334.
[130] *See*, for instance, Patrick W. Franzese, "Sovereignty in Cyberspace: Can It Exist?" *A.F. L. REV.* 64 (2009): 5–6 (showing that experts do not agree on whether a cyber-attack constitutes an "act of war," armed attack, or a use of force sufficient to trigger the application of the LOAC). *See* Michael N. Schmitt, *supra* note 12, 58–60.
[131] *See* Matthew Hoisington, *supra* note 118: 453 (recommending the reconstruction of IHL to recognise not just the right of states to self-defense against non-state perpetrators of cyber-attacks, but also the state's inherent right to anticipatory self-defense in response to a cyber-attack, especially when the attack targets critical national infrastructure). *See* also Daniel M. Creekman, "A Helpless America? An Examination of the Legal Options Available to the United States in Response to Various Cyber-attacks from China," *Am. U. Int'l L. Rev.* 17 (2002): 677–678.
[132] *Ibid.*: 654–655 (arguing that a new international convention on integrating cyber-attacks and cyber warfare into the core of IHL must identify and list critical national infrastructure which if attacked by

put in place an environment that will deter both state and non-state actors, because a clear definition will enjoy legitimacy (which will in turn command compliance) and will clearly state what is prohibited. Again, the whole gamut of IHL will have to be reconstructed with cyber-attacks and cyber warfare in mind, especially regarding the *jus in bello* principles of necessity, distinction, proportionality and humanity.

In the meanwhile, before the laws of war are modified to take cognisance of cyber-attacks, we recommend that states respond to transnational cyber-attacks by graduating their countermeasures on the basis of severity of the attacks.[133] Thus, mild attacks that are not illegal or do not rise to the level of use of force, could be responded to by use of non-forcible counter computer network attacks (CNA) that are commensurate in scale and effect to the initial CNA. Severe cyber-attacks that are elevated to use of force but do not reach the threshold of armed attack, may receive a counter response from an equivalent or proportional non-forcible counter CNA; while those elevated to armed attack may be met by an equal measure, in addition to a kinetic force option.

BIBLIOGRAPHY

1. Albright, David, Paul Brannan, and Christina Walrond. "Did Stuxnet Take Out 1,000 Centrifuges at the Natanz Enrichment Plant?" Institute for Science and International Security Report (December 22, 2010): 1–10 // http://isis-online.org/uploads/isis-reports/documents/stuxnet_FEP_22Dec2010.pdf.
2. Anderson, Michael. "Reconceptualizing Aggression." *Duke Law Journal* 60 (2010): 411–456.
3. Antolin-Jenkins, Vida M. "Defining the Parameters of Cyber War Operations: Looking for Law in All the Wrong Places?" *Naval Law. Rev*. 51 (2005): 132–169.
4. Baker, Stewart, McAfee, Inc. "In the Crossfire: Critical Infrastructure in the Age of Cyber War" (2009) // http://newsroom.mcafee.com/images/10039/In%20the%20Crossfire_CIP%20report.pdf.
5. Barkham, Jason. "Information Warfare and International Law on the Use of Force." *N.Y.U. J. Int'l L. & Pol.* 34 (2001): 57–114.

means of cyber weapons would give a state the right to use active defence measures, including kinetic self-defence or active defence in the cyberspace).

[133] *See*, e.g., Manny Halberstam, *supra* note 49: 224–233.

6. Billo, Charles G., and Welton Chang. *Cyber Warfare: An Analysis of the Means and Motivations of Selected Nation States*. Institute for Security Technology Studies, 2004.
7. Blank, Laurie R. "Taking Distinction to the Next Level: Accountability for Fighters' Failure to Distinguish Themselves from Civilians." *Valparaiso University Law Review* 46(3) (2012): 745–887.
8. Brenner, Susan W. "Is There Such a Thing as 'Virtual Crime'?" *Cal. Crim. L. Rev.* 4 (2001): 1-18.
9. Brenner, Susan W. and Leo L. Clarke, "Civilians in Cyber Warfare: Conscripts," *Vanderbilt Journal of Transnational Law* 43 (2010): 1011-1076.
10. Brenner, Susan. "At Light Speed: Attribution and Response to Cybercrime/Terrorism/Warfare." *J. Crim. Law & Criminology* 97 (2007): 363–381.
11. Brown, Davis. "Use of Force Against Terrorism After September 11th: State Responsibility, Self-Defense and Other Responses." *Cardozo J. of Int'l & Comp. Law* 11 (2003): 1-57.
12. Cannizzaro, Enzo. "Contextualizing Proportionality: Jus Ad Bellum and Jus in Bello in the Lebanese War." *Int'l Rev. Red Cross* 88 (864), 779 (2006): 779–827.
13. Carnahan, Burrus M. "Lincoln, Lieber and the Laws of War: The Origins and Limits of the Principle of Military Necessity." *Am. J. Int'l L.* 92 (1998): 213–248.
14. Carr, Jeffrey. *Inside Cyber Warfare*. CA: O'Reilly Media Inc., 2010.
15. Clarke, Richard A., and Robert K. Knake. *Cyber War: The Next Threat to National Security and What to do About it.* New York: Ecco, 2010.
16. Coleman, Kevin. "The Cyber Arms Race Has Begun." *CSO Online* (January 28, 2008) // http://www.csoonline.com/article/print/216991.
17. Condron, Sean. "Getting It Right: Protecting American Critical Infrastructure in Cyberspace." *Harv. J.L. & Tech.* 20 (2007): 403–422.
18. Creekman, Daniel M. "A Helpless America? An Examination of the Legal Options Available to the United States in Response to Various Cyber-attacks from China." *Am. U. Int'l L. Rev.* 17 (2002): 641–689.
19. Darcy, Shane. "Assistance, Direction and Control: Untangling International Judicial Opinion on Individual and State Responsibility for War Crimes by Non-state Actors." *International Review of the Red Cross* 96(893) (2014): 259–261.

20. DeLuca, Christopher D. "The Need for International Laws of War to Include Cyber Attacks Involving State and Non-State Actors." *Pace Int'l L. Rev. Online Companion* 3 (2013): 278–329.
21. Dinstein, Yoram. "Computer Network Attacks and Self-Defense": 99–120. In: Michael N. Schmitt and Brian T. O'Donnell, eds. *Computer Network Attack and International Law*. Naval War College, International Law Studies, vol.76, 2002.
22. *DOD Dictionary of Military and Associated Terms* (2001) // http://www.dtic.mil/doctrine/new_pubs/jp1_02.pdf.
23. Dombrowski, Peter, and Chris C. Demchak. "Cyber War, Cybered Conflict, and the Maritime Domain." *Naval War College Review* 67(2) (2014): 45–93.
24. Dormann, Knut. "Applicability of the Additional Protocols to Computer Network Attacks." Int'l Committee of the Red Cross (November 19, 2004) // http://www.icrc.org/eng/assets/files/other/applicabilityofihltocna.pdf.
25. Estreicher, Samuel. "Privileging Asymmetric Warfare (Part II)?: The 'Proportionality' Principle under International Humanitarian Law." *Chi. J. Int'l L.* 12 (2011): 1–143.
26. Franzese, Patrick W. "Sovereignty in Cyberspace: Can It Exist?" *A.F. L. REV.* 64 (2009): 1–54.
27. Gercke, Marco. *Understanding Cybercrime: Phenomena, Challenges and Legal Response*. ITU: Telecommunication Development Bureau, 2012.
28. German Federal Ministry of the Interior. *Cyber Security Strategy for Germany.* Berlin: Beauftragter der Bundesregierung für Informationstechnik, 2011.
29. Goodman, Ryan, and Derek Jinks, "The ICRC Interpretive Guidance on the Notion of Direct Participation in Hostilities under International Humanitarian Law: An Introduction to the Forum." *NYU J Intl L Pol.* 42 (2010): 637–640.
30. Gordon, Sarah, and Richard Ford. "On the Definition and Classification of Cybercrime." *J. Computer Virology* 1 (2006): 1–17.
31. Graham, David E. "Cyber Threats and the Law of War." *Journal of National Security Law & Policy* 4 (2010): 87–134.
32. Halberstam, Manny. "Hacking Back: Re-evaluating the Legality of Retaliatory Cyber-attacks." *The Geo. Wash. Int'l L. Rev*. 46 (2013): 199–258.
33. Hathaway, Melissa E., and Alexander Klimburg. "Preliminary Considerations: On National Cyber Security": 1–43. In: Alexander Klimburg, ed. *National Cyber Security Framework Manual*. Tallinn: NATO Cooperative Cyber Defence Centre of Excellence, Estonia Publication, 2012.

34. Hathaway, Oona, Rebecca Crootof, Philip Levitz, Haley Nix, Aileen Nowlan, William Perdue, and Julia Spiegel. "The Law of Cyber-Attack." *Calif. L. Rev*. 100 (2012): 817–886.
35. Heinsch, Robert. "The Crime of Aggression After Kampala: Success or Burden for the Future?" *Goettingen Journal of International Law* 2 (2010): 709–763.
36. Henckaerts, Jean-Marie, and Louise Doswald-Beck. *Customary International Humanitarian Law.* ICRC, 2005.
37. Hildreth, Steven A. "Cyber Warfare." Cong. Research Serv., CRS Report for Congress (2001): 1–29.
38. Hoisington, Matthew. "Cyber Warfare and the Use of Force Giving Rise to the Right of Self-Defense." *B.C. Int'l & Comp. L. Rev.* 32 (2009): 439–481.
39. Hollis, Duncan B. "Why States Need an International Law for Information Operations." *Lewis & Clark Law. Review* 11 (2007): 1023–1093.
40. Hurka, Thomas. "Proportionality in the Morality of War." *Philo & Pub Aff*. 33 (2005): 34–72.
41. ICRC. "Interpretive Guidance on the Notion of Direct Participation in Hostilities under International Humanitarian Law." *Intl Rev Red Cross* 90 (2008): 987–1026.
42. Jensen, Eric. "Computer Attacks on Critical National Infrastructure: A Use of Force Invoking the Right of Self-Defense." *Stan. J. Int'l Law* 38 (2002): 207–240.
43. Jensen, Eric. "Unexpected Consequences from Knock-On Effects: A Different Standard for Computer Network Operations?" *Am. U. Int'l L. Rev*. 18 (2003): 1168–1197.
44. Kalpokienė, Julija, and Ignas Kalpokas. "Hostes Humani Generis: Cyberspace, the Sea, and Sovereign Control." *Baltic Journal of Law & Politics* 5:2 (2012): 132–163.
45. Kastenberg, Joshua E. "Non-intervention and Neutrality in Cyberspace: An Emerging Principle in the National Practice of International Law." *A.F. L. Rev*. 64 (2009): 1–68.
46. Kelsey, Jeffrey T.G. "Hacking into International Humanitarian Law: The Principles of Distinction and Neutrality in the Age of Cyber Warfare." *Mich. L. Rev*. 106 (2008): 1431–1468.
47. Kerschischnig, Georg. *Cyber Threats and International Law.* Eleven International Publishing, 2012.
48. Kingsbury, Alex. "Documents Reveal Al Qaeda Cyber-attacks." *U.S. News* (April 14, 2010) //

http://www.usnews.com/news/articles/2010/04/14/documentsreveal-al-qaeda-cyberattacks.

49. Landau, Susan. "National Security on the Line." *Journal of Telecomm. & High Tech. Law* 4 (2006): 409–447.
50. Libicki, Martin C. "What is Information Warfare?" *Strategic Forum* No. 28 (1995): 1–3.
51. Little, Debra, John Shinder, and Ed Tittel. *Scene of the Cybercrime: Computer Forensics Handbook*. (MA: Syngress Publishing, Inc. Rockland, 2002).
52. Lülf, Charlotte. "Modern Technologies and Targeting under International Humanitarian Law." *IFHV Working Paper* Vol. 3, No. 3 (December 2013): 39–45 // http://www.ruhr-uni-bochum.de/ifhv/documents/workingpapers/wp3_3.pdf.
53. Melzer, Nil. "Keeping the Balance between Military Necessity and Humanity: A Response to Four Critiques of the ICRC's Interpretive Guidance on the Notion of Direct Participation in Hostilities." *Int'l L. & Pol*. 42 (2010): 831–877.
54. Melzer, Nils. "Cyber Operations and Jus in Bello." *Disarmament Forum* (2011).
55. Murphy, Matt, "War in the Fifth Domain: Are the Mouse and Keyboard the New Weapons of Conflict?" *Economist* (July 1, 2010).
56. Owens, William A., Kenneth W. Dam, and Herbert S. Lin, eds. *Technology, Policy, Law, and Ethics Regarding US Acquisition and Use of Cyber-attack Capabilities.* National Research Council Report, 2009.
57. Printer, Norman G., Jr. "The Use of Force against Non-State Actors under International Law: An Analysis of the U.S. Predator Strike in Yemen." *UCLA J. Int'l L. & Foreign Aff*. 8 (2003): 331–392.
58. Proulx, Vincent-Joel. "Babysitting Terrorists: Should States Be Strictly Liable for Failing to Prevent Transborder Attacks?" *Berkeley J. Int'l L*. 23 (2005): 616–667.
59. Rollins, John W., and Catherine A. Theohary. *Cyber warfare and Cyber terrorism: In Brief* (Congressional Research Service (CRS) Report, R43955, March 27, 2015).
60. Sandoz, Yves, Christophe Swinarski, and Bruno Zimmermann, eds. *Commentary on the Additional Protocols of 8 June 1977 to the Geneva Conventions of 12 August 1949*. ICRC, 1987.
61. Schaap, Arie J. "Cyber Warfare Operations: Development and Use under International Law." *A.F. L. Rev*. 64 (2009): 121–161.
62. Schindler, Dietrich, and Jiri Toman, eds. *The Laws of Armed Conflicts: A Collection of Conventions, Resolutions and Other Documents.* 4th ed. (Boston: Martinus Nijhoff Publishers, 2004.

63. Schmitt, Michael N. "'Attack' as a Term of Art in International Law: The Cyber Operations Context": 283–293. In: Christian Czosseck, Rain Ottis, and Katharina Ziolkowski, eds. *4th International Conference on Cyber Conflict.* Tallinn: NATO CCD COE Publications, 2012.
64. Schmitt, Michael N. "Military Necessity and Humanity in International Humanitarian Law: Preserving the Delicate Balance." *Virginia Journal of International Law* 50(4) (2010): 761–799.
65. Schmitt, Michael N. "Rewired Warfare: Rethinking the Law of Cyber Attack." *Int'l Rev. Red Cross* 96(893) (2014): 182–205.
66. Schmitt, Michael N. "The Impact of High Tech and Low Tech Warfare on Distinction": 169–189. In: Roberta Arnold and Pierre-Antoine Hildbrand, eds. *International Humanitarian Law and the 21st Century's Conflicts: Changes and Challenge.* Lausanne: Ed. Interuniversitaires Suisses-Edis, 2005.
67. Schmitt, Michael N. "Wired Warfare: Computer Network Attack and Jus in Bello." *Int'l Rev. of the Red Cross* 84 (2002): 365–399.
68. Schmitt, Michael N., ed. *Tallinn Manual on the International Law Applicable to Cyber Warfare.* Cambridge: Cambridge University Press, 2013.
69. Schmitt, Michael N., Harrison A. Dinniss, and Thomas C. Wingfield. "Computers and War: The Legal Battle Space." Background Paper prepared for Informal High-Level Expert Meeting on Current Challenges to International Humanitarian Law. Cambridge (June 25–27, 2004).
70. Schmitt, Michael. "Pre-emptive Strategies in International Law." *Mich. J. Int'l L*aw 24 (2003): 534–569.
71. Shane, Harris, "The Cyber war Plan," *National Journal* (November 14, 2009) // http://www.nationaljournal.com/njmagazine/cs_20091114_3145.php.
72. Sharp, Walter Gary. *Cyberspace and the Use of Force.* Virginia, Falls Church: Aegis Research Corporation, 1999.
73. Shimeall, Timothy, Phil Williams, and Casey Dunlevy. "Countering Cyber War." *NATO Rev*. 49 (2001): 16–19.
74. Sklerov, Matthew J. "Solving the Dilemma of State Responses to Cyber-attacks: A Justification for the Use of Active Defenses against States Which Neglect Their Duty to Prevent." *Mil. L. Rev*. 201 (2009): 1–85.
75. Smith, Gerry. "UK Authorities Brace for 'Cyber Jihad' By Al Qaeda after Bin Laden Death." *The Huffington Post* (July 12, 2011) // http://www.huffingtonpost.com/2011/07/12/al-qaeda-cyberjihad_n_895579.html.
76. Solce, Natasha. "The Battlefield of Cyber Space: The Inevitable New Military Branch – The Cyber Force." *Alb. L.J. Sci. & Tech.* 18 (2008): 292–336.

77. Stevens, Sharon R. "Internet War Crimes Tribunals and Security in an Interconnected World." *Transnat'l L. & Contemp. Probs.* 18 (2009): 657–676.
78. Svarc, Dominika. "Redefining Imminence: The Use of Force Against Threats and Armed Attacks in the Twenty-First Century." *ILSA J. Int'l & Comp. L.* 13 (2006): 171–219.
79. Swanson, Lesley. "The Era of Cyber Warfare: Applying International Humanitarian Law to the 2008 Russian-Georgian Cyber Conflict." *L.A. Int'l & Comp. L. Rev*. 32 (2010): 303–353.
80. Teo, Cheng Hang. "The Acme of Skill: Non-Kinetic Warfare." Air Command & Staff Coll., Wright Flyer Paper No. 30 (2008) // http://www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA485268&Location=U2&doc=GetTRDoc.pdf.
81. Turns, David. "Cyber Warfare and the Notion of Direct Participation in Hostilities." *Journal of Conflict & Security Law* (2012): 279–297.
82. U.K. Cabinet Office. *The UK Cyber Security Strategy: Protecting and Promoting the UK in a Digital World* (November 2011) // https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/60961/uk-cyber-security-strategy-final.pdf.
83. U.K. Ministry of Defence. *The Joint Service Manual of the Law of Armed Conflict.* 3. Wiltshire: The Joint Doctrine and Concepts Centre, UK, 2004.
84. U.K. Secretary of State for the Home Dep't. *Contest: The United Kingdom's Strategy for Countering Terrorism*. Her majesty's Stationary Office (July 2011) // https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/97995/strategy-contest.pdf.
85. *US Army Training & Doctrine Command, DCSINT Handbook No. 1.02, Critical Infrastructure Threats and Terrorism: Cyber Operations and Cyber Terrorism Handbook*. 2005.
86. US Department of Defense (DOD). "Memorandum for Chiefs of the Military Services, Commanders of the Combatant Commands, Dirs. of the Joint Staff Directories – Joint Terminology for Cyberspace Operations" (November 2011): 1-16 // http://www.nsci-va.org/CyberReferenceLib/2010-11-joint%20Terminology%20for%20Cyberspace%20Operations.pdf.
87. US Department of Defense (DOD). "Quadrennial Defense Review" (2010).
88. US Department of Defense (DOD). "Strategy for Operating in Cyberspace" (July 2011).
89. US White House. *The National Strategy to Secure Cyberspace* (2003) // http://www.dhs.gov/xlibrary/assets/National_Cyberspace_Strategy.pdf.

90. Vatis, Michael A. "Cyber Attacks during the War on Terrorism: A Predictive Analysis." *Institute for Security Technology Studies at Dartmouth College, Report OMB No. 074-0188* (September 2001).
91. Waxman, Matthew C. "Cyber-Attacks and the Use of Force: Back to the Future of Article 2(4)." *Yale Journal of International Law* 36 (2011): 411–452.
92. Wedgwood, Ruth. "Proportionality, Cyber war and the Law of War": 219–254. In: Michael N. Schmitt and Brian T. O'Donnell, eds. *Computer Network Attack and International Law.* Naval War College, International Law Studies, vol.76, 2002.
93. Wheeler, David, and Gregory Larsen. "Techniques for Cyber Attack Attribution." *Inst. Def. Analysis* (October 2003): 23–25 // http://www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA468859&Location=U2&doc=GetTRDoc.pdf.
94. Wingfield, Thomas. *The Law of Information Conflict: National Security Law in Cyberspace.* Texas: Aegis Research Corp, 2000.

LEGAL REFERENCES

1. *Advisory Opinion on the Legality of the Threat or Use of Nuclear Weapons*. 1996 I.C.J. para. 79 (July 8).
2. *Combating the Criminal Misuse of Information Technologies*. G.A. Res. 55/63, paras.1,3 U.N. Doc. A/RES/55/63 (Jan. 22, 2001).
3. *Convention on Cybercrime*. Council of Europe, Nov. 23, 2001, 41 I.L.M. 282, 2296 U.N.T.S. 167.
4. *Eighth United Congress on the Prevention of Crime and the Treatment of Offenders*. G.A. Res. 45/121, para.3, U.N. Doc. A/RES/45/121 (Dec. 14, 1990).
5. *Geneva Convention (III) Relative to the Treatment of Prisoners of War*. Aug. 12, 1949, 6 U.S.T. 3316, 75 U.N.T.S. 135.
6. *Hague Convention (IV) with Respect to the Laws and Customs of War on Land*. Oct. 18, 1907, 36 Stat. 2277, 187 Consol. T.S. 429.
7. *Lieber Code, U.S. War Dep't, General Orders No. 100: Instructions for the Government of Armies of the United States in the Field* (April 24, 1863).
8. *Military and Paramilitary Activities in and Against Nicaragua (Nicaragua v. U.S.)*. 1984 I.C.J. Rep. 392.
9. *Prosecutor v. Tadić*. Case No. IT-94-1-A, I.C.T.Y. App. Ch., at 49 (July 15, 1999).

10. *Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflicts*. June 8, 1977, 1125 U.N.T.S. 3.
11. *Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of Non-International Armed Conflicts*. June 8, 1977, 1125 U.N.T.S. 3.
12. *Review Conference of the Rome Statute of the International Criminal Court*. Kampala, Uganda, May 31-Jun. 11, 2010, U.N. Doc. R/Con./Res.6, Annex I.
13. *Rome Statute of the International Criminal Court*. July 17, 1998, 37 I.L.M. 1002.
14. *UN General Assembly, 'Definition of Aggression'*. G.A. Res. 3314, U.N. GAOR, 29th Sess., U.N. Doc. A/RES/3314 (Dec. 14, 1974).
15. *US Critical Infrastructure Protection Act of 2001*. 42 U.S.C.S. §5195c(e) (2006).