EFFICACY OF INTERNATIONAL HUMANITARIAN LAW IN ADDRESSING CYBER WARFARE AS A NEW WEAPON TECHNOLOGY: AN ANALYSIS OF THE GAPS AND WAY FORWARD

Joshua Mbinda Ngulu[*]

Abstract

This article is tailored towards interrogating the efficacy of the law of armed conflict, the Geneva Convention and its Protocols, in dealing with the menace of cyber warfare. The research finds that the law is ill prepared to deal with the contemporary means and methods of warfare. The author debunks assumptions consistently made in International Humanitarian Law (IHL) that the old laws can be stretched to cub these new technologies while pointing out various areas that need reconsideration in the wake of the development of cyber warfare. Most notably, this research suggests that time has come that the pressing need, to negotiate a binding instrument, to govern cyber warfare ought to be addressed. Greater certainty is advocated for herein, on this subject matter. The international legal regime is lagging behind the problems presented by the increasingly sophisticated technological possibilities in this area, and it is time to argue less and act more.

Key words: *Law of armed conflict, cyber warfare, International Humanitarian Law*

---

[*]Lecturer of Law at the School of Law, Moi University, Eldoret-Kenya, current PhD (Law) Candidate at the School of Law, University of Nottingham-United Kingdom. The author may be contacted through joshua.mbinda@gmail.com/joshua.ngulu@nottingham.ac.uk. I wish to register my gratitude for the constructive criticisms and comments I received from the participants of the Fourteenth Faculty Roundtable on International Humanitarian Law for East African Universities held on 14-15 August 2018 in Addis Ababa-Ethiopia The law cited is as at 30 January 2020.

1. INTRODUCTION

In early August 2008, a full-scale war broke out between Russia and Georgia over the disputed territory of South Ossetia, a pro-Russian autonomous region of Georgia.[1] Bombs were dropped throughout the Georgian capital of Tbilisi, with Russian bombers targeting Georgia's economic infrastructure, including the country's largest Black Sea port, Poti, and the main road connecting the southern part of Georgia with the East.[2] In the two months leading up to this conflict, Georgia's Internet infrastructure was also attacked and major Georgian website servers were brought down, hindering communication and causing confusion throughout the country.[3] The kind of attacks used is known as distributed denial of service attacks.[4] They are triggered when computers in a network are simultaneously ordered to bombard a website with millions of requests, which then overload the website server and cause it to shut down.[5] These cyber-attacks mainly hindered the Georgian government's ability to communicate with its citizens, as well as other nations, both before and during the

---

[1] Elene Gotsadze, Fighting with Russia Spreads to Cities Across Georgia, *CNN.COM, 8* August 2008, Available at http://www.cnn.com/2008/WORLD/europe/08/08/georgia.ossetial index.html#cnnSTCText. (accessed 28 January 2020).

[2] *Ibid*.

[3] Kim Hart, Longtime Battle Lines are Recast in Russia and Georgia's Cyberwar*,* *Wash Post*, 14 August 2008, at Dl. Available at http://www.washingtonpost.com/wpdyn/content/article/2008/08/13/AR2008081 303623.html; (accessed 28 January 2020).

[4] Bruce Etling, Cyber Warfare Precedes Georgian-Russian Hostilities*,* Berkman Center for Internet & Society at Harvard University, Internet & Democracy Blog, 11 August 2008. http://blogs.law.harvard.edulidblog/2008/08/11/cyber-warfare-preceds-georgianrussian-hostilities/. (accessed 28 January 2020).

[5] *Supra* note 3.

physical invasion by Russia.[6] This anecdote introduces to the reality of cyber warfare.

IHL has seen the development of various and diverse means and even methods of warfare. Unfortunately, the 1949 Geneva Conventions and the Additional Protocols of 1977 are one step behind the development of contemporary weaponry. Currently, the war is taking place on three fronts. The first is physical, the second is on the world of social networks, and the third is cyber.[7] Consequently, there is confusion about the applicability of IHL to cyber warfare – which might in fact stem from different understandings of the concept of cyber warfare itself, which range from cyber operations carried out in the context of armed conflicts as understood in IHL to criminal cyber activities of all kinds.[8]

Cyber-attacks turn the attention of IHL to a set of pressing questions. Erki Kodar[9] poses fundamental questions on the applicability and efficiency of IHL in dealing with cyber warfare. Some of these questions include: whether there are concrete and precise restrictions regarding the employment of cyber-attacks? Can IHL, a body of law mostly regulating international conflicts and conventional weapons, provide workable solutions? As cyber-attacks require a high level of knowledge of information technology and are thus more likely to be executed by civilian

---

[6] *Ibid*.

[7] Cowell Alan, Cyberwar and Social Media in the Gaza Conflict, The New York Times, 19 November 2012, Available at https://rendezvous.blogs.nytimes.com/2012/11/19/cyberwar-and-social-media-in-the-gaza-conflict/?_r=1. (accessed 29 January 2020).

[8] Cordula Droege, Get off My Cloud: Cyber Warfare, International Humanitarian Law, and The Protection of Civilians 886 *International Review of The Red Cross*, 2012 at pp. 533-38.

[9] Erki Kodar, Applying The Law Of Armed Conflict To Cyber Attacks: From The Martens Clause To
Additional Protocol I, *ENDC Proceedings*, Volume 15, 2012, at pp. 107–32.

experts, are the perpetrators of cyber-attacks then entitled to combatant privilege or is it a case of direct participation in hostilities? Can cyber-attacks be regarded as a means of warfare? Are cyber-attacks in compliance with the requirements of neutrality? What restrictions and modalities arise during targeting? These pertinent questions will receive answers in this article.

In light of the foregoing questions, this article examines inadequacies of IHL as currently constituted in dealing with cyber warfare. More certainty in the subject of cyber warfare and the actual laws governing such employment in IHL is advocated for and possibly, a binding document ought to be concluded to this effect.

This article intends to address, *inter alia*, the discordance and uncertainty in the definition of cyber warfare, the applicability of IHL principles to cyber warfare, the question of attribution and responsibility in relation to cyber warfare and the challenges that cyber warfare poses to the typology of armed conflicts and the concept of direct participation. Moreover, this article debunks the fallacy of safety afforded in the Martens Clause in dealing with cyber warfare.

2. DEFINITIONAL CHALLENGES

IHL provisions do not specifically mention cyber operations. Arguably, during the drafting and concluding of the Geneva Conventions and its Additional Protocols, such advanced modes of warfare were not contemplated. Because of this, and because the exploitation of cyber technology is relatively new and sometimes appears to introduce a complete qualitative change in

the means and methods of warfare,[10] it has occasionally been argued that IHL is ill-adapted to the cyber realm and cannot be applied to cyber warfare.[11] Even so, what is cyber warfare?

There is no official definition of cyber warfare at international level. Even so, scholars and various commentators have attempted defining the concept to suit their usage in diverse manners. For instance, cyber warfare has been described as:

> Cyber operations conducted in or amounting to armed conflict which involve the development and dispatch of computer code from one or more computers to target computers and can be aimed at either infiltrating a computer system to collect, export, destroy, change or encrypt data or trigger, alter, or otherwise manipulate processes controlled by the infiltrated system.[12]

Richard Clarke, a US cyber security expert defines it as, "Actions by a nation- state to penetrate another nation's computers or networks for the purposes of causing damage or disruption".[13] The Tallin Manual attempts to define it as, "a cyber operation whether offensive or defensive that is reasonably expected to cause injury or death to persons or damage or destruction to objects."[14] The International Committee of Red Cross (ICRC) has

---

[10] *Ibid*.

[11] Charles J. Dunlap Jr., Perspectives for Cyber Strategists on Law for Cyberwar, *Strategic Studies Quarterly*, Spring, 2011, at p. 81.

[12] Lesley Swanson, The Era of Cyber Warfare: Applying International Humanitarian Law to the 2008 Russian-Georgian Cyber Conflict, 32 Loy. L.A. Int'l & Comp. L. Rev. 303 2010. Available at https://digitalcommons.lmu.edu/cgi/viewcontent.cgi?article=1010&context=ilr (accessed 29 January 2020).

[13] Richard Clarke and Robert Knake, Cyber War: The Next Threat to National Security and What to Do about It New York: HarperCollins, 2010, at p.32.

[14] Michael Schmitt, Tallinn Manual on the International Law Applicable To Cyber Warfare- Prepared by the International Group of Experts at the Invitation of the

also attempted to define it as, "a means and methods of warfare that consist of cyber operations amounting to or conducted in the context of an armed conflict within the meaning of IHL."[15]

On the basis of these definitions, the researcher raises the question whether there is any binding legal framework under international law to govern and address the devastating effects of cyber warfare. If such a framework exists, it would beat logic to address a concept whose definition to this day, is still veiled in uncertainty. In 2003, at the 28th International Conference of the Red Cross and Red Crescent, states party to the Geneva Conventions declared that, 'In light of the rapid development of weapons technology and in order to protect civilians from the indiscriminate effects of weapons and combatants from unnecessary suffering and prohibited weapons, all new weapons, means and methods of warfare should be subject to rigorous and multidisciplinary review.'[16] This glaring loophole therefore begs for an answer which to date, IHL has failed to provide.

3. APPLICABILITY OF IHL TO CYBER WARFARE: IS A CYBER- ATTACK AN 'ATTACK' IN IHL?

Attacks are defined under Article 49(1) of Additional Protocol I as 'acts of *violence* against the adversary, whether in offense or in

---

NATO Co-operative Cyber Defence Centre of Excellence, Cambridge University Press, 2013 , at p. 91.

[15] ICRC, Cyber Warfare and International Humanitarian Law: The ICRC's position, 2013. Available at https://www.icrc.org/en/doc/assets/files/2013/130621-cyber-warfare-q-and-a-eng.pdf (accessed 29 January 2020).

[16] See the Report on the 28th International Conference of the Red Cross and Red Crescent, at p. 20, 26 December 2003. Available at https://www.icrc.org/en/doc/assets/files/other/icrc_002_1103.pdf (accessed 28 January 2020).

defence'.[17] The Commentary on the Additional Protocol I adds that attacks must involve 'combat action', as this is the likeliest way in which civilians will be affected by armed conflict.[18] Other questions linger as to whether and under which conditions, the destruction of data constitutes an 'attack' in the sense of IHL[19] and whether this can be termed, correctly so, as combat action. There is an 'act of violence' (i.e. an attack) if the act results in death or injury to persons, or damage or destruction to objects.[20] This definition includes acts that are non-violent but have violent consequences, such as biological or chemical weapons. Significant human physical or mental suffering is logically included in the concept of injury; permanent loss of assets, for instance money, stock etc, directly transferrable into tangible property likewise constitutes damage or destruction[21] The point is that inconvenience, harassment or mere diminishment in quality of life does not suffice is the requisite criterion.[22] This definition excludes non-physical, psychological, political or economic warfare.[23]

---

[17] Additional Protocol I Art. 49(1) [emphasis added].

[18] Claude Pilloud *et al*., International Committee of the Red Cross, Commentary on the Additional Protocols of 8 June 1977 to the Geneva Conventions of 12 August 1949, Geneva: *Martinus Nijhoff Publishers*, 1987 para. 1880, at p. 603.

[19] Michael. Schmitt, The Law of Cyber Warfare: Quo Vadis? *Stanford Law & Policy Review*, Vol. 25, 2014. Available at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2320755. (accessed 29 January 2020).

[20] Dinstein Yoram, The Conduct of Hostilities under the Law of International Armed Conflict*,* 3rd ed., Cambridge: *Cambridge University Press*, 2016 at pp. 2-3.

[21] Michael Schmitt, Wired Warfare: Computer Network Attack and *Jus in bello*, *IRRC*, Vol. 84, June 2002 at pp. 374-75. Available at https://www.icrc.org/en/doc/assets/files/other/365_400_schmitt.pdf (accessed 29 January 2020).

[22] *Ibid*.

[23] Michael Bothe, Karl Josef Partsch and Waldemar Solf, New Rules for Victims of Armed Conflicts: Commentary on the Two 1977 Protocols Additional to the Geneva Conventions of 1949*, The Hague: Martinus Nijhoff Publishers*, 2nd Edition, 6 December 2013., at pp. 289.

Cyber operations must result in death or injury to persons, or damage or destruction to objects in order to qualify as an attack. This may be problematic as cyber operations can result in a broad range of outcomes and might not necessarily involve kinetic effects. The qualification of a cyber operation as an attack is significant because it makes most of the substantive provisions restricting the conduct of hostilities operative.

Professor Michael Schmitt proposes a six-part test as to whether cyber-attack should be considered as an armed attack. The six part test includes severity, immediacy, directness, invasiveness, measurability and presumptive legitimacy. Regarding this six part matrix Schmitt propounds it in this manner:

a) severity: the type and scale of the harm;

b) immediacy: how quickly the harm materializes after the attack;

c) directness: the length of the causal chain between the attack and the harm;

d) invasiveness: the degree to which the attack penetrates the victim state's territory;

e) measurability: the degree to which the harm can be quantified; and

f) Presumptive legitimacy: the weight given to the fact that, in the field of cyber-activities as a whole, cyber-attacks constituting an armed attack are the exception rather than the rule.[24]

[24]Michael Schmitt, Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework, *37 Colum. J. Transnat'l L.* at pp. 914–15; See also Sean Kanuck, Recent Development: Information

Consequently, in applying this test, it appears that cyber warfare attacks are provided within the definition of Article 49 of Additional Protocol I of the Geneva Conventions.[25]

In the *Nuclear Weapons Case,* the International Court of Justice (the ICJ) held that IHL applies to all forms of warfare, regardless of the weapons employed.[26] Cyber operations that occur in the context of an armed conflict are therefore subject to humanitarian law.[27] Whereas cyber-attacks launched in the context and in furtherance of an armed conflict do not pose a challenge in their classification, difficulties arise as to whether a cyber-attack can constitute an armed conflict in and of itself. For some commentators, the lack of kinetic effects implies that cyber-attacks cannot bring an armed conflict into existence.[28]

Less certain, however, is the issue concerning the specific threshold of gravity and intensity of force required to constitute an "armed attack". This issue has been very contentious with regard to the use of kinetic weapons. Subsequently, a challenge is bound to arise in the case of cyber operations.[29] Indeed, this absence of

---

Warfare: New Challenges for Public International Law, 37 *Harv. Int'l L.J.* 272, 1996 at p. 290. ("Each suspect activity could be reviewed for its effects on other states, and sanctioned accordingly.").

[25] *Ibid*.

[26] ICJ, Legality of the Threat or Use of Nuclear Weapons*,* Advisory Opinion, *ICJ Reports*, para. 39, 1996, at p. 226.

[27] Michael Schmitt and Vihul, Liis (*ed.*), Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations: Prepared by the International Group of Experts at the Invitation of the NATO Cooperative Cyber Defence Centre of Excellence*,* Cambridge: *Cambridge University Press*, Rule 80. 2017. Rule 80,at p. 375.

[28] Eric Pomès, Technological Innovations and International Humanitarian Law: Challenges and Tensions, 46 *Polish Pol. Sci Y.B* 205, 2017 at p. 46.

[29] Yoram Dinstein, Computer Network Attacks and Self-Defense, *International Law Studies*, Vol. 76 *Computer Network Attack and International Law*, 105, 2002. Available at https://digital-

clarity raises considerable challenges particularly in relation to cyber operations because it becomes difficult to determine when such an operation would amount to an armed attack justifying resort to lawful self-defence measures contemplated in Article 51 of the UN Charter.[30]

This then begs the question "whether a cyber-attack is an action below the threshold of the use of force amounting to an armed attack".[31] These pertinent questions ought to be answered by the law of armed conflict but the Geneva Conventions and the Additional Protocol fall short in this respect.

4. APPLICABILITY OF THE PRINCIPLES OF IHL TO CYBER WARFARE

4.1 The Principle of Distinction

The principle of distinction between the civilian population and combatants and between the objects and military objectives

---

commons.usnwc.edu/cgi/viewcontent.cgi?referer=https://www.google.com/&httpsredir=1&article=1397&context=ils (Accessed 29 January 2020).

[30] Michael Schmitt, The Koh Speech and the Tallinn Manual Juxtaposed, 54, *Harvard International Law Journal*, 2012, 13, at p. 22: "Whether a cyber use of force qualifies as an armed attack depends on its 'scale and effects.' [U]ncertainty as to what those scale and effects are plagued the Tallinn Manual deliberations. The Experts observed, for instance, that the International Court of Justice differentiated a mere 'frontier incident' from an armed attack, but later opined that an attack on a single warship might qualify as an armed attack. Such inexplicable distinctions obfuscated their attempt to identify practical legal thresholds."

[31] Marco Roscini, World Wide Warfare – *Jus ad Bellum* and the Use of Cyber Force 14 *Max Planck Yearbook of United Nations Law*, 2010, 114, at p.130. Available at https://westminsterresearch.westminster.ac.uk/download/d0a8ce791f1273b5eebc437c728f518fbcf29c2cd5c823d0560027c14fcf77f8/315715/Roscini_2010_as_published.pdf (accessed 29 January 2020).

originates in Articles 48 and 52(2) of Additional Protocol I[32] In the *Nuclear Weapons Case*, the ICJ referred to this principle as the "cardinal principle"[33] of IHL as well as one of the "intransgressible principles of International Customary Law".[34]

This rule is not, however, simply determinable in cyber warfare due to the fact that most cyber infrastructure is meant for dual usage and therefore cannot fall within either the scope of a civilian object[35] or a military objective[36] due to such overlap.[37] These dual-use targets complicate the application of the principle of distinction.[38] This trickles down to the interrogation of how one can practically distinguish between a military computer and a civilian computer for instance. In reality, one cannot tell the difference between a military machine and a civilian machine. Some experts have suggested the marking of military computers in cyberspace, but one should tell how likely it is that the military will mark their computers and strategic cyber processes as being military?[39] It is not going to happen. It is simply not realistic that states flag out their most important military cyber assets to the enemy.

---

[32]Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts (Protocol I), 8 June 1977, available at www.icrc.org (accessed 29 January 2020).

[33]ICJ, Legality of the Threat or Use of Nuclear Weapons, Advisory Opinion, I.C.J. Reports, para 179, 1996 at p. 226.

[34] *Ibid.*

[35] Art 52(1) AP1.

[36] Art 52(2) AP1.

[37] Elizabeth Mavropoulou, Targeting in the Cyber Domain: Legal Challenges Arising from the Application of the Principle of Distinction to Cyber-Attacks - *Journal of Law & Cyber Warfare,* Vol. 4, No. 2, 24, 2015 at p. 26.

[38] Brian O'Donnell & James Kraska, Humanitarian Law: Developing International Rules for the Digital Battlefield, 8 *J. Conflict & Security L*. 133, 149, 2003 at p. 157.

[39] Robin Geiss, Humanitarian Aspects of Cyber Warfare XXXIV Round Table on Current Issues of International Humanitarian Law on International Humanitarian Law and New Weapon Technologies In Sanremo on 8-10 September 2011.

The reigning position, however, is that due to their military purpose such objects can be subject to attack.[40] This, therefore, presents a challenge and seemingly, this principle does not provide the intended protection it should serve. Further, due to the interconnectedness of the cyberspace, civilian cyber infrastructure that is not of dual use and would therefore be protected from direct attack might nevertheless come to harm. In the particular context of cyber operations, is an attack on military cyber infrastructure using malicious computer virus which subsequently spreads to connected civilian systems.[41] The question that will arise is whether cyber operations are capable of discriminating application or whether they are "blind" weapons.[42] Applying this logic, a belligerent is more likely to engage in attacks that violate the principle of distinction using cyber warfare than when using conventional methods since it can do so without incurring the political cost associated with civilian casualties. For example, a belligerent might use cyber weapons in place of conventional methods to attack targets traditionally protected as "civilian objects." IHL has protected these objects because a conventional attack would cause substantial civilian casualties and greatly affect civilian lives and property, while serving only an indirect military purpose.[43]

Unlike a conventional attack, a cyber-attack could neutralize these targets without causing physical injury to civilians or physical damage to the site, while the attacker could argue that the strike has at least some impact on the targeted belligerent's capacity to

---

[40] *Supra*, note 28, Tallinn Manual, Commentary on Rule 39, para. 1.

[41] William Boothby, Weapons and the Law of Armed Conflict, *Oxford University Press*, 2009 at p. 237.

[42] Dissenting Opinion of Judge Higgins, *Nuclear Weapons Case* at pp.588-89.

[43] Davis Brown, A Proposal for an International Convention To Regulate the Use of Information Systems in Armed Conflict, 47 *Harv. Int'l L.J.*, 2006 at p.179.

continue its military campaign.[44]As such, cyber warfare may be more likely to lead a belligerent to violate the principle of distinction. Further, as one commentator has stated 'it is less obvious that attacks with less tangible results, such as the disruption of a financial or social security system, or the disclosure of confidential personal information, constitute the sort of injury against which humanitarian law is supposed to protect civilians.'[45] Given these considerations, direct attacks on civilian objects are more likely with cyber weapons than with conventional weapons, regardless of the risk of war-crime accusations. [46]

Indeed the distinction in cyber warfare is an extremely complex issue, since the cyber weaponry can either significantly simplify the situation by precise targeting or make the situation extremely difficult due to side-effects of such attacks if not well targeted or when spreading gets out of control.[47] Albeit, the author does not dispute the fact that the principle of distinction ought to apply to cyber warfare, the traditional conception of the principle is not alive to the novelties of cyber warfare. Therefore, operation of this cardinal principle in relation to cyber warfare should be reconsidered.

4.2 Principle of Proportionality

The principle of proportionality in IHL is based on Article 51(5)(b),[48] which requires anticipation of incidental loss of civilian

---

[44] Vida M. Antolin-Jenkins, Defining the Parameters of Cyberwar Operations: Looking for Law in All The Wrong Places?, 51 *Naval L. Rev.*, 2005 at p.132.

[45] Lawrence Greenberg, Seymour Goodman and Kevin Soo Hoo., Information Warfare and International Law, *National Defense University*, 1998 at p. 12.

[46] *Supra* note 37, at p 156.

[47] Eva Knopová, New IHL Framework for Cyber Warfare LLM thesis, available at https://is.cuni.cz/webapps/zzp/download/120249532 (accessed 8 August, 2018).

[48] *Supra* note 31.

lives, injuries and damages to civilian objects and make sure that those will not exceed the concrete and direct military advantage brought by the attack.[49] In the opposite case, the attack is, by the IHL rules, prohibited as indiscriminate.[50] The Institute of International Law points out that existing international law prohibits the use of all weapons that, by their nature, affect indiscriminately both military and non-military objectives.[51] This rule presents a challenge at the face of it since it is very difficult to evaluate the military advantage in cyber warfare against the incidental loss. This is so both because cyber operations are a relatively novel phenomenon and so little is known about their impact; and because the interconnected nature of cyberspace makes it particularly difficult to foresee all the possible effects of such operations.[52] It is also contested as to what amounts to 'damage' in the digital arena and whether it is only restricted to physical damage or even loss of functionality in objects.

Indeed, the application of this principle to cyber-attacks is quite complicated. It raises the question of what damage is to be taken into account for the analysis of proportionality. Cyber attacks produce different types of effects;[53] immediate effects; destruction, corruption, data corruption, system damage, (as happened in the Estonian and Georgian conflicts); destruction/neutralization of the

---

[49] Robert Kolb and Richard Hyde, An introduction to the International Law of Armed Conflicts, *Hart Publishing* 2008 at p. 48.

[50] Art 51(4) AP1.

[51] International Committee of the Red Cross, The Distinction between Military Objectives and Non-military Objectives in General and Particularly the Problems Associated with Weapons of Mass Destruction*, Inst. of Int'l L*. 2 Sept. 9, 1969, *available at http://www.icrc.org/ihl.nsf/WebPrint/445-* (accessed 30 January 2020).

[52] *Supra* note 9.

[53] Marco Roscini, Cyber Operations and the Use of Force in International Law. *Oxford University Press*, 2014, at p 52.

machine or infrastructure like Stuxnet. Injury to civilians can result due to either, like in Estonia or Georgia. This challenge illustrates the importance of commencing an international dialogue on these issues to bring clarity to existing law of war principles in this context. They also demonstrate that the law of war alone cannot address the new challenges posed by cyber-attacks. Clearly, the law lags behind in dealing with the advancement of technology or weaponry and as such, special considerations should be made in clearing the air in having a proportionality analysis in relation to cyber warfare.

4.3 Principle of Precaution in Attack

In conducting military operations, constant care has to be taken to spare the civilian population, civilians and civilian objects from attacks and the effects thereof. Everything feasible should be done to verify that the objectives to be attacked are neither civilians nor civilian objects and are not subject to special protection but are military objectives and that it is not prohibited to attack them.[54] At a minimum, IHL requires military commanders to 'know not just where to strike but be able to anticipate all the repercussions of an attack'.[55] Belligerents are further required to cancel or suspend an attack if it becomes apparent that it will entail a breach of the principle of proportionality.[56] In compliance with this strict threshold, a party planning to undertake a cyber-attack should do everything feasible to gain the information necessary to verify that the projected target is a military objective and to evaluate the extent of the harm that such attack will cause

---

[54] Art 57 AP1.

[55] Jeffrey Walker, The Demise of the Nation–State, The Dawn of New Paradigm Warfare, and a Future for the Profession of Arms, 51 *A.F. L. Rev*. 2001, 323, at pp. 337–38. See also, Bradley Graham, Military Grappling With Guidelines For Cyber Warfare; Questions Prevented Use on Yugoslavia, *Wash. Post*, 8 November, 1999, at p.1.

[56] Art 57 AP1.

as weighed against its direct and solid military advantage. If expertise required to undertake such precautionary measures is not available, such attacks should be done away with. This therefore presents challenges in practice due to the intricately intertwined nature of the cyber networks and this calls for extreme caution and extensive research to classify the object of attack before the actual attack to prevent indiscriminate attacks on services and data essential to the survival and wellbeing of civilians.

Flowing from the foregoing, it will be practically impossible to take precaution if the parties cannot distinguish between military objectives and civilian objects. Therefore, the dialogue towards certainty as advocated for in this article should encapsulate this thorny issue.

4.4 Attribution and Cyber Warfare

Another difficulty in applying the rules of IHL to cyberspace, stems from the digitalization on which cyberspace is built. Digitalization ensures anonymity and thus complicates the attribution of conduct.[57] IHL assumes parties to the conflict are known, whereas anonymity is inherent to most cyber operations and attribution to a state is difficult and can be denied.[58]

It is a generally accepted rule in international law that States bear the international legal responsibility for wrongful conduct that is

---

[57] Jakob Kellen Berger, International Humanitarian Law and New Weapon Technologies', 34th Round Table on Current Issues of International Humanitarian Law, San Remo, 8-10 September 2011.

[58] Puneet Bhalla, Seminar Report on Contemporary Challenges in International Humanitarian Law Related to New Technologies, *Vij Books India Pvt Ltd*, New Delhi, 6 November. 2015 at p. 9.

attributable to them.[59] This rule applies similarly in the case of cyber operations. However, its practical application is very problematic because cyber operations often enlist unsuspecting computers from around the world in order to "spin a web of anonymity around the attacker(s) thus making accurate attribution uniquely difficult."[60] The practical difficulty of attributing a cyber-attack is exacerbated by the inherent characteristics of cyber space: anonymity, multi-stage actions, and the rapidity with which actions are executed.[61] It is a general rule that the international wrongful cyber conduct of State organs, even when they act in official capacity but beyond their instructions, is attributable to the State.[62] But this rule is less clear in the case of non-State actors who conduct wrongful cyber operations either on the specific instruction of or with the encouragement of the State. It is also unclear whether "a non-State actor's cyber operations that are not attributable to a State can nevertheless qualify as an armed attack

---

[59] United Nations, Draft Articles on Responsibility of States for Internationally Wrongful Acts, 2008, UNGA Res A/RES/56/83. Available at https://legal.un.org/ilc/texts/instruments/english/commentaries/9_6_2001.pdf (accessed on 30 January 2020). Text adopted by the International Law Commission at its fifty-third session, in 2001, and submitted to the General Assembly as a part of the Commission's report covering the work of that session (A/56/10). The report, which also contains commentaries on the draft articles, appears in the Yearbook of the International Law Commission,, vol. II, Part Two,as corrected of 12 December 2001. See also; James Crawford, Articles on Responsibility of States for Internationally Wrongful Acts, Lauterpacht Research Centre for International Law, University of Cambridge, 2012 at pp. 1-5. Available at https://legal.un.org/avl/pdf/ha/rsiwa/rsiwa_e.pdf (accessed 30 January 2020).

[60] Oona Hathaway *et al*, The Law of Cyber -Attack' 100, *California Law Review, 2012, at pp.*817-23.

[61] Nicholus Tsagourias, Cyber Attack, Self-Defence and the Problem of Attribution 17(2) *Journal of Conflict & Security Law*, 2012, at p. 233.

[62] *Draft Articles of State Responsibility* 44-45; *Case Concerning US Diplomatic and Consular Staff in Tehran (US v Iran)*, 1980, ICJ Reports 3, para 74; see also, Jay Kesan & Carol Hayes, Mitigative Counterstriking: Self-Defense and Deterrence in Cyberspace 25 *Harvard Journal of Law and Technology, 2011-2012 at p.* 482.

justifying a defensive response at the level of a use of force against that non-State actor."[63]

Some problematic scenarios illustrate the legal problems that arise in the case of cyber operations. Consider the case where the origin of a cyber operation can be traced to cyber infrastructure belonging to State A; does this engage the international responsibility of that State A? Another instance is where cyber means belonging to or provided by State A fall into the hands of insurgents acting against State B, but not under the instruction of State A; does this engage the international responsibility of State A? The Stuxnet Worm incident, concerning a cyber operation against nuclear centrifuges in Iran, is a clear example of the challenges posed by cyber operations with particular regard to attribution.[64] In sum, this is an area that deserves *a* considerable further thought.

4.5 The Martens Clause: Debunking the Fallacy of a Fallback

Whereas law evolves slowly, new means and methods of warfare are swiftly being developed and are changing to adapt to contemporary warfare. Bridging the temporal and contextual gap between the moment of the law's formation and the moment of its application is thus becoming an ever growing and more urgent challenge.[65] The Geneva conventions and Protocols date back to 1949 and 1977 respectively. These are clearly 'old' laws that present a challenge in fitting in the 'new' circumstances and the

---

[63] *Supra* note 21.

[64] John Richardson, Stuxnet as Cyberwarfare: Applying the Law of War to the Virtual Battlefield, *J. Marshall Journal of Computer & Info Law*, 29(1), 2011 at pp. 1 – 29.

[65] *Ibid.*

dynamics of warfare. This is what this article terms as "new wine being fitted into old wineskins". This is understandable since the law of war dates back to the nineteenth century and has not yet been updated for applicability in the Information Age.[66] The only purported solace is that these laws were painted with a *broad brush* and some of the provisions have escalated to principles forming part of customary international law; for instance, the principles of distinction,[67] precautions in attack and the effects of an attack[68] and proportionality.[69] Further, a safeguard is provided in the Martens Clause[70] which has since been codified providing thus:

Until a more complete code of the laws of war is issued, the High Contracting Parties think it right to declare that in cases not included in the Regulations adopted by them, populations and belligerents remain under the protection and empire of the principles of international law, as they result from the usages established between civilized nations, from the laws of humanity and the requirements of the public conscience.[71]

---

[66] Hilaire Mccoubrey, International Humanitarian Law: Modern Developments in the Limitation of Warfare 1, *Ashgate*, 2nd ed.1998 at p.1. This text discusses comprehensively on how the principles of IHL have evolved to their present understanding.

[67] Rules 1-10, Customary Rules of International Humanitarian Law.

[68] Rules 15-22, Customary Rules of International Humanitarian Law.

[69] Rule 14, Customary Rules of International Humanitarian Law.

[70] Preamble of the 1899 Hague Convention (II) with Respect to the Laws and Customs of War on Land (entered into force 4 September 1900) and 1907 Hague Convention (IV) Respecting the Laws and Customs of War on Land (entered into force 1 January 1910).

[71] Rupert Ticehurst, The Martens Clause and the Laws of Armed Conflict, *International Review of the Red Cross*, No. 317, 1997 at p. 125.

Many commentators have run to this provision as a fallback when the law of armed conflict is clouded with uncertainty.[72] It is almost a scapegoat provision where legal loopholes exist. However, the mere fact that one resorts to the Martens Clause vindicates the position that the law does not address itself to this issue. Further, the notion of principles of humanity and dictates of public conscience is fluid. This concept can attract debate akin to the question of morality. It is relative in all respects depending on many external factors and as such, it cannot be left to deal with the complex issues revolving around cyber warfare.

4.6 The Softness of the Tallinn Manual

The Tallinn Manual is a non-binding document prepared by a group of experts. It identifies international law relevant to cyber warfare and sets up ninety five rules governing cyber warfare.[73] Whereas critics of this piece might argue that the manual exists to fill the loopholes advanced courtesy of the advent of cyber warfare, it is merely an academic, non-binding study. Borrowing from the general principles of international law, it is merely persuasive in the eyes of the law and inspirational and cannot be resorted to solve the pertinent issues raised herein conclusively. Therefore, until states conclude a binding document on this subject matter, the cloud of uncertainty still floats over the operations in cyber warfare.

---

[72] Okore Jayalo, International Humanitarian Law and Cyber Warfare 15th International Humanitarian Law Essay Competition for East African University Students' July 2017 at p. 5.

[73] *Supra* note 15.

5. POTENTIAL CHALLENGES POSED BY CYBER WARFARE TO TRADITIONAL CONCEPTIONS IN IHL

This article acknowledges and pinpoints various challenges that the employment of cyber warfare in armed conflicts possesses. The author foresees with a hawk eye that in the case that an assumption is made that IHL, as currently constituted, is equal to the task in dealing with cyber warfare, then among others, the question of classification of conflicts, attribution and the notion of direct participation in hostility will face unforetold overhaul beyond the logical ends.

5.1 Overhaul on the Typology of Armed Conflicts

Typology involves the characterization of the specific type of conflict as international, internal or otherwise.[74] Armed conflicts in IHL have traditionally been classified as international armed conflict, to which the four Geneva Conventions and Additional Protocol I are applicable, and non-international armed conflicts, to which Common Article 3 to the Geneva Convention and Additional Protocol II, apply.

The difficulty of reliably classifying a particular conflict is amplified in the case of cyber operations owing to their uniqueness as non-kinetic capabilities that are launched in cyber space.[75] First, unlike conventional operations involving kinetic weapons, cyber operations are capable of producing massive and widespread disruptive effects on a particular society or its economy without

[74] Michael Schmitt, Classification of Cyber Conflict,*Journal of Conflict and Security Law,17 (2), 2012 at p.*245.

[75] Michael Schmitt, War, Technology and International Humanitarian Law HPHPCR, Occasional Paper Series 4, 2005, at p. 43.

necessarily causing any physical damage that is often associated with combat action.[76]

Further, the actors involved in cyber operations may vary from unrelated individuals, insufficiently organized groups or groups that are organized but which exist entirely online.[77] This raises significant challenge in trying to determine affiliations for purposes of according the consequential legal protection and enforcing compliance with international humanitarian law.

Moreover, cyber operations relevant to international law are cross-border and they occur in cyberspace,[78] and this, therefore, complicates the classification of conflict relative to the location of the operations.

In addition to this, in the specific context of non-international armed conflict, the collective qualification of participants in cyber operations as an organized armed group will present a particular challenge.[79] Also, there is sharp division concerning whether the

---

[76] National Research Council, Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities. Washington, DC: The National Academies Press, 2009 at pp. 127. Available at https://doi.org/10.17226/12651.(accessed 30 January 2020).

[77] *Supra*, note 75 at p. 245.

[78] Matthew Skelrov, Solving the Dilemma of State Responses to Cyberattacks: A Justification for the Use of Active Defenses Against States Which Neglect Their Duty to Prevent 201 *Military Law Review*,1, 2009, at p. 62. See also Christopher Joyner & Catherine Lotrionte, Information Warfare as International Coercion: Elements of a Legal Framework 12 *European Journal of International Law, 2001, at pp.* 825-65.

[79] David Graham, Cyber Threats and the Law of War 4 *Journal of National Security Law and Policy*, 2010 at pp. 87-98. See also, Knut Dörmann, The Applicability of the Additional Protocols to Computer Network Attacks; An ICRC Viewpoint', Available at https://www.icrc.org/en/doc/assets/files/other/applicabilityofihltocna.pdf (accessed 30 January 2020).

requisite test of protracted armed violence[80] would be satisfied, thus bringing into effect the law of non-international armed conflict, in the case of cyber incidents that are not destructive, but which nevertheless have severe consequences.[81]

Resultantly, the typology of armed conflicts should have an overhaul in light of the advent of cyber warfare. If not so, it will be very difficult to classify this contemporary form of warfare within the predetermined traditional setup.

5.2 The Notion of Direct Participation in Hostilities and Cyber Warfare

If the actors in cyber-attacks are civilians, the problem in applying IHL becomes more complex. This brings as to the notion of direct participation in hostilities and thereby considering such civilians as direct participants in hostilities for purposes of the Geneva law.[82] This would mean that these civilians are illegal combatants and, therefore, not immune from retaliatory attack.[83] Civilians are not prohibited from directly participating in cyber operations amounting to hostilities but forfeit their protection from attacks for such time as they so participate.[84] Combatants are permitted to take part in hostilities, while civilians are afforded protection so

---

[80] *Prosecutor v Tadic* (Jurisdiction) ICTY-94-1 (2 October 1995) para 70.

[81] *Supra* note 51.

[82] International Committee of The Red Cross, International Humanitarian Law and The Challenges of Contemporary Armed Conflicts, 31st International Conference of the Red Cross and Red Crescent, Geneva, Switzerland, 28 November- 1 December 2011 at pp. 9-10.. Available at https://e-brief.icrc.org/wp-content/uploads/2016/08/4-international-humanitarian-law-and-the-challenges-of-contemporary-armed-conflicts.pdf. (accessed 30 January 2020).

[83]Michael Schmitt, Wired Warfare: Computer Network Attack and *Jus in Bello*, 846 *Int'l Rev. of the Red Cross* , 2002, at pp. 365-66. (Quoting Joint Chiefs Of Staff, Department Of Defense Dictionary Of Military And Associated Terms, Joint Publication 1-02 203, 2001.

[84] *Supra* note 74, Tallinn Manual *Rule 29.*

long as they do not take direct part in the hostilities.[85] Direct participation can involve causing damage to the belligerent or supplying the enemy's armed forces.[86] The International Committee on the Red Cross (ICRC) has released guidelines which establish a three-pronged test for direct participation. First, the act must be likely to adversely affect military operations or the military capacity of a party to an armed conflict or, alternatively, to inflict death, injury, or destruction on persons or objects protected against direct attack (threshold of harm). Second, there must be a direct causal link between the act and the harm likely to result either from that act, or from a coordinated military operation of which that act constitutes an integral part (direct causation). Finally, 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 (belligerent nexus).[87]

Cyber-attacks require a high level of knowledge of information technology and are thus more likely to be executed by civilian experts.[88] Due to the characteristics of the field, modern weapons and IT systems are seldom operated exclusively by the members of armed forces.[89] This increases the risk that civilians working in the armed forces, especially in the area of operations, will be

---

[85] Arts. 48, 50(1), 51 (2) and 52(1) AP I.

[86] Art 51(3) AP1.

[87] Nils Melzer, Interpretive Guidance on the Notion of Direct Participation in Hostilities under International Humanitarian Law. Geneva: ICRC, Geneva, Switzerland, 2009 at p. 46.

[88] Erki Kodar, Applying The Law of Armed Conflict To Cyber Attacks: From The Martens Clause To Additional Protocol 1, ENDC Proceedings, Vol. 15, 2012 at p. 107-32. Available at https://www.ksk.edu.ee/wp-content/uploads/2012/12/KVUOA_Toimetised_15_5_Kodar.pdf (accessed 30 January 2019).

[89] *Ibid.*

considered to be direct participants in hostilities.[90] This, therefore, creates a problem since if it is established that civilians are behind such attacks, they lose their protection as civilians and this poses a threat to civilian cyber networks. However, this is not a problem unique to cyber warfare. The pertinent question would be, for instance, does conducting a cyber operation make a civilian lose protection? How is it determined that such a civilian or the other took an active part in the operation? These questions seem basic but providing clear cut answers to them has proved problematic.

Consequently, it is difficult to determine the status of a civilian who participates directly in the hostilities; for example launching a cyber-attack against one of the parties to the conflict. There is a debate amongst scholars as to the necessary degree of damage for such a determination to be made.[91]For the ICRC, it is necessary for the act to cause physical or material damage.[92] However, for the *Tallinn Manual on the International Law Applicable to Cyber Warfare*, there is direct participation in hostilities as soon as the act adversely affects the opposing military operations. This difference illustrates perfectly that interpretation is subject to the interests of the interpreter of the rule. The ICRC's interpretation is intended to limit the loss of protection against attacks, whereas the purpose of the interpretation of the *Tallinn Manual*, which is fairly close to American interests, is to facilitate the loss of such protection.

---

[90] Michael Schmitt. Applicability of the Additional Protocols to Computer Network Attacks. – Conduct of Hostilities, Information Warfare. 19 November 2002 at pp. 8-9. Available at *<http://www.icrc.org/eng/resources/documents/misc/68lg92.htm>, (accessed 30 January 2020).*

[91] Allan Collin, Direct Participation in Hostilities from Cyberspace,. *Virginia Journal of International Law*, *54* (1), 2013 at pp. 173 – 193.

[92] *Supra* note 88 at p. 46.

Moreover, the ICRC requires there to be a link between the act and the damage, whereas the *Tallinn Manual* merely requires an intention.[93] The challenge will be to determine whether an individual who designs viruses may be considered as a direct participant in hostilities. As such, it is time to commence discussions that will lead to a solid answer to the question of cyber warfare.

6. CONCLUSION

The law on armed conflict as currently provided for in the Geneva Conventions and its Additional Protocols of 1949 and 1977 respectively is inadequate to deal with the new concept of cyber warfare. Whereas it is desirable to adopt the view of *Michael N. Schmitt,*[94] that the law of armed conflict was intended to cover all aspects and forms of warfare, despite this glory that has been attributed to IHL, it is notable as has been demonstrated above that the IHL falls short of its given glory. Cyber warfare challenges some of the most fundamental principles of IHL. It is not disputed that IHL is only applicable if cyber operations are conducted in the context of and related to an armed conflict; what if the cyber operations occur in the absence of armed conflict? Or what is the intensity test? Secondly on the principle of distinction, how does one distinguish between military and civilian objects? Thirdly on proportionality, what damage is to be taken into account while cyber warfare produces different effects? Fourthly, how is it possible to take precaution if the parties cannot distinguish between military objectives and civilian objects? Fifthly, how do you attribute the conduct to a state whereas cyber warfare is founded on anonymity?

---

[93] *Supra* note 15 at p. 119.

[94] Michael Schmitt, Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework, 37 *Colum. J. Transnat'l L.*, 1999 at p. 914–15.

The application of IHL poses serious challenges that were not anticipated during the drafting of the existing laws of armed conflict, which are clearly 'old' laws that present a challenge in fitting in the 'new' circumstances and the dynamics of warfare. There is need for new law. Pouring new wine into old skins is hazardous. There is a warning that 'Neither do people pour new wine into old wineskins, if they do, the skins will burst; wine will run out and the wineskins will be ruined. No, they pour new wine into new wineskins, and both are preserved."[95]

[95] Matthew 9, 17, Holy Bible, King James Version.