A Game of Code: Challenges of Cyberspace as a Domain of Warfare

*Christopher Rosana Nyabuto**

Abstract

The military capabilities that the world witnesses in modern day armed conflicts are a sort of science fiction brought to life. Most of the techniques in cyber warfare were never thought possible, let alone anticipated in times past especially during the framing of key International Humanitarian Law (IHL) instruments. This paper analyses the challenges that cyber warfare poses to state responsibility. The analysis also discusses how the anonymity of parties in cyber warfare presents challenges to the application of existing law. The rationale for this study is the fact that cyberspace as a domain of warfare is still in its early days despite the many ambiguities and puzzles it has sparked in various circles of discussion. The study relies on literature reviews and case studies to make its salient points. Ultimately, the study argues that cyber warfare is subject to IHL; however, it breeds new possibilities that may require greater adherence to consistent legal review of weapons and greater willingness of the international community to apply IHL to this domain of warfare.

Key words: cyber-attack, state responsibility, armed conflict, anonymity

I. Introduction

Doctor Frankenstein's monster slowly rose from the table with life.[1] The young doctor had achieved what no man had ever done – to create life itself and

* The author is an LLB Candidate at Kenyatta University Law School. At the time of writing this paper, he served as a legal intern at the International Committee of the Red Cross, Nairobi Regional Delegation. The author wishes to acknowledge Ms Jacquelene Mwangi, Ms Jane Njeri Ngugi, Francis Monyango and Emmanuel Marsuk Lomole for their support, encouragement and warm criticism in writing this paper.

1 *Frankenstein* is a novel detailing the life of Victor Frankenstein, a scientist who tinkered with biology and philosophy till he created a living creature in a somewhat human frame. Dr Frankenstein never referred to the creature he made as human and neither did he give it a name. He was so ashamed and scared of what he had made that he resorted to calling it 'monster' or 'demon'. Shelley M, *Frankenstein,* Barnes and Nobles Classics, New York City, 2003.

watch it move with might and power. Boundless. Strong. Eloquent. Nevertheless, ugly. The monster was a new creation that was never thought possible. This is the form in which humanity finds itself 199 years after Shelley's classic work 'Frankenstein' was first published. A world with no limits, a world with no steel or flesh but also a world with new dangers to which we find ourselves victim. Cyberspace is the new world. Cyber warfare is its dangerous hand.[2] Humanity is Frankenstein, cyberspace is the monster we have created and now it haunts us. The law has always been our refuge, but will it become a solace in the face of the new reality of cyber warfare?

With this question in mind, Smith recently proposed that the time had come for the world to adopt a 'digital Geneva Convention'.[3] He argued that cyberspace is a unique realm not properly addressed by existing international law.[4] He acknowledged the rising number of cyber-attacks on hospitals, power grids and other infrastructure essential to human survival.[5] To his credit, the Geneva Conventions do not address cyber warfare directly. Nevertheless, the violations that may result from cyber warfare in an armed conflict would still fall under the realm of IHL as shown in subsequent sections of this paper.

The author argues that it is unnecessary to create a new treaty governing cyber warfare because the existing treaties and customary law address sufficiently the violations that occur from it as a means of warfare. Furthermore, a new treaty would only be appropriate once the existing challenges to current laws are

---

2 Cyber warfare is the attempt by parties to an existing armed conflict to utilise technological tools in order to wield dominance over their opponents in the realm of cyberspace. Lin H, 'Cyber conflict and international humanitarian law' 94(886) *International Review of the Red Cross,* 2012, 517.

3 Parker B, 'Bots and bombs: Does cyberspace need a "Digital Geneva Convention"?' IRIN, 15 November 2017 on <http://www.irinnews.org/analysis/2017/11/15/bots-and-bombs-does-cyberspace-need-digital-geneva-convention?utm_source=IRIN+-+the+inside+story+on+emergencies&utm_campaign=ba54d1efd8-RSS_EMAIL_CAMPAIGN_ENGLISH_AID_AND_POLICY&utm_medium=email&utm_term=0_d842d98289-ba54d1efd8-75433709>on 15 December 2017.

4 Parker B, 'Bots and bombs: Does cyberspace need a "Digital Geneva Convention"?' IRIN, 15 November 2017 on <http://www.irinnews.org/analysis/2017/11/15/bots-and-bombs-does-cyberspace-need-digital-geneva-convention?utm_source=IRIN+-+the+inside+story+on+emergencies&utm_campaign=ba54d1efd8-RSS_EMAIL_CAMPAIGN_ENGLISH_AID_AND_POLICY&utm_medium=email&utm_term=0_d842d98289-ba54d1efd8-75433709>on 15 December 2017.

5 Parker B, 'Bots and bombs: Does cyberspace need a "Digital Geneva Convention"?' IRIN, 15 November 2017 on <http://www.irinnews.org/analysis/2017/11/15/bots-and-bombs-does-cyberspace-need-digital-geneva-convention?utm_source=IRIN+-+the+inside+story+on+emergencies&utm_campaign=ba54d1efd8-RSS_EMAIL_CAMPAIGN_ENGLISH_AID_AND_POLICY&utm_medium=email&utm_term=0_d842d98289-ba54d1efd8-75433709>on 15 December 2017.

resolved.[6] It is unwise to add more legal instruments to the pile while the current laws are struggling to adjust. This paper demonstrates that the greatest challenge is the lack of certainty in identifying perpetrators owing to the anonymity that actors enjoy. Such a discussion is significant given the prevalent attacks on daily life by a method never thought possible – computer code. The realm of computer code directly injures the lives of civilians by crippling critical infrastructure. For instance, a cyber-attack that disables hospital equipment essentially killing those civilians on life-support constitutes a war crime. A war crime is a war crime whether committed through computer code or by a machete.[7]

In fact, an all-out cyberwar would result in excessive and widespread damage only comparable to a nuclear attack.[8] Full-scale cyber warfare could even be equated to nuclear weapons owing to its inability to distinguish military and civilian objectives, combatants and non-combatants.[9] The only major difference in this analogy is that nuclear weapons are not as readily obtainable to civilians unlike hacking skills that can be learnt by anyone.[10] Sadly, cyber warfare is capable of causing greater damage to civilians by destroying the systems that sustain their daily life.[11] Thus, Sinopoli states:

> 'The potential for disastrous consequences in a nuclear attack can be matched in the case of an all-out attack using cyber-warfare. The example of a cyber-attack where critical infrastructures are destroyed or otherwise rendered useless can leave a state in a helpless position, causing unnecessary suffering to its citizens'.[12]

Aside from the introduction, this paper is divided into four parts. Part II outlines the peculiarities of cyber warfare including the importance of anonymity in cyberspace and whether cyber-attacks are viewed as normal attacks in IHL. This part starts by discussing the principle of distinction in the context of cyberspace. It discusses the various legal provisions that prohibit attacks against civilians and civilian objects and whether attackers may sufficiently implement

---

6 Some of these challenges are discussed in later sections of the paper.

7 A war crime is a serious violation of the laws and customs of war applicable in armed conflict. Henckaerts JM and Doswald-Beck L, *Customary International Humanitarian Law – Volume 1: Rules,* Cambridge University Press, Cambridge, 2005, 568.

8 Swanson L, 'The era of cyber warfare: Applying international humanitarian law to the Russian-Georgian cyber conflict' 32(2) *Loyola Los Angeles International Comparative Law Review*, 2010, 303-333.

9 Scott S, 'From nuclear war to net war: Analogising cyber-attacks in international law' 27(1) *Berkeley Journal of International Law,* 2009, 192-251.

10 Sinopoli A, 'Cyberwar and international law: An English school perspective' Published Graduate Thesis, University of South Florida, Florida, 2012, 51.

11 Swanson L, 'The era of cyber warfare: Applying international humanitarian law to the Russian-Georgian cyber conflict', 303-333.

12 Sinopoli A, 'Cyberwar and international law: An English school perspective', 50.

them in their attacks given the interconnectedness of systems. Part III discusses issues arising from attribution and responsibility. Once risk, death, or destruction occurs, in what way would the law impute culpability to the individual or state? Part IV demonstrates the application of the principles discussed in this paper to case studies. It also acknowledges the imbalance of cyber power in the world; certain states have a higher capability to wage sophisticated cyber-attacks than others. Part V calls for the obligation to conduct regular weapons reviews while urging responsible parties to fulfil their obligations under Article 36 of Additional Protocol I (AP I).

II. Peculiarities of Cyber Warfare

This section discusses the hurdles of applying the principle of distinction in cyber warfare due to the Internet-dependent nature of contemporary life. The Internet is a dual-use object; the military and civilians use it. All other systems or services connected to the Internet may suffer harm by virtue of this interconnectedness.[13] The section also defines an 'attack' and the effect of anonymity towards cyber warfare.

i. Distinction in cyber warfare

In armed conflict, 'the right of the parties to the conflict to choose methods or means of warfare is not unlimited'.[14] Moreover, the nature of means or methods of warfare does not affect the applicability of the law of armed conflict.[15] Hence, the basic principles of armed conflict, for instance, the principle of distinction, still extend to the field of cyber operations.[16]

Article 48 of AP I provides:'In order to ensure respect for and protection of the civilian population and civilian objects, the parties to the conflict shall at all times distinguish between civilian objects and military objectives and accordingly shall direct their operations only against military objectives'.[17] A

[13] Bannelier-Christakis K, 'Is the principle of distinction still relevant in cyber warfare?' in Tsagourias N and Buchan R (eds), *Research handbook on international law and cyberspace,* Edward Elgar Publishing, Cheltenham, 2015, 343-365.

[14] Article 35(1), *Protocol additional to the Geneva conventions of 12 August 1949, and relating to the protection of victims of international armed conflicts (Additional Protocol I)*, 8 June 1977, 1125 UNTS 17512.

[15] International Group of Experts, *Tallinn manual on the international law applicable to cyber warfare*, Cambridge University Press, Cambridge, 2013, 105.

[16] International Group of Experts, *Tallinn manual,* 105.

[17] Article 48, *Additional Protocol I.*

military objective is an object whose 'nature, location, purpose, or use make an effective contribution to military action and whose partial or total destruction, capture or neutralisation, in the circumstances ruling at the time, offers a definite military advantage'.[18] It follows that civilian objects would be all other objects that do not fall under the classification of military objectives.

Cyberspace prompts the question, 'what could amount to a legitimate target, or specifically a military target, as to warrant a cyber-attack that complies with IHL'? The common marker of cyber-attacks is their wide-reaching implication affecting the civilians and the military in equal measure. For instance, a cyber-attack on an electric grid would have an indiscriminate effect on civilians and combatants alike. Article 51 of AP I outlaws indiscriminate attacks yet that is the very nature of cyber-attacks.[19] In fact, the importance of this principle was affirmed by the International Court of Justice (ICJ) which held as follows:

> 'The cardinal principles contained in the text constituting the fabric of humanitarian law are the following. The first is aimed at the protection of the civilian population and civilian objects and establishes the distinction between combatants and non-combatants; states must never make civilians the object of attack and must consequently never use weapons that are incapable of distinguishing between civilian and military objects'.[20]

In December 2015, the Ukrainian power company Prykarpattyaoblenergo experienced an outage, which they attributed to Russian cyber-attacks.[21] The American cyber firm iSight Partners later identified the pro-Russian hacking group, Sandworm, as the perpetrator.[22] This attack on the power grid is the first confirmed successful hack on a power plant. It left 230,000 people in the dark for almost six hours prompting the power company to drive manually to the substations to switch the power on.[23] The immediate effect was hours of no electricity; but months after the attack most of the power centres were still not

---

18 Henckaerts JM and Doswald-Beck L, *Customary international humanitarian law – Volume 1: Rules,* 29.

19 Article 51, *Additional Protocol I* provides that 'indiscriminate attacks are prohibited. Indiscriminate attacks are: (a) those which are not directed at a specific military objective; (b) those which employ a method or means of combat which cannot be directed at a specific military objective: or (c) those which employ a method or means of combat the effects of which cannot be limited as required by this Protocol'. See Kodar E, 'Applying the law of armed conflicts to cyber attacks: From the Martens Clause to Additional Protocol I' ENDC Proceedings, 15, 2012, 115.

20 *Legality of the threat or use of nuclear weapons*, Advisory Opinion, ICJ Reports 1996, 44.

21 Zinets N, 'Ukraine hit by 6500 hack attacks, sees Russian "cyberwar"' Reuters, 29 December 2016 on <http://www.reuters.com/article/us-ukraine-crisis-cyber-idUSKBN14I1QC> on 20 March 2017.

22 Zinets N, 'Ukraine hit by 6500 hack attacks, sees Russian "cyberwar"' Reuters, 29 December 2016 <http://www.reuters.com/article/us-ukraine-crisis-cyber-idUSKBN14I1QC> on 20 March 2017.

23 Bacet J, 'Inside the cunning, unprecedented hack of Ukraine's power grid' Wired, 3 March 2016 <https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/> on 20 March 2017.

fully operational.[24] The attack was highly sophisticated and showed months of planning alongside well-trained cyber actors.[25] This attack was a violation against the prohibition of attacking civilians and civilian objects, which is a facet of the principle of distinction.

Applying the principle of distinction to cyber-attacks is a challenge for the combatants because there are times when an attack intended for a military objective may result in the destruction of a civilian object.[26] There is no fool proof separation between civilian objects and military objectives.[27] There is no guarantee that an attack on a military objective will not spill over to civilian objects.[28] However, this is not a gap in the law but a weakness of cyber warfare in adjusting to the requirements of IHL.

ii. The peculiarity of cyber-attack

By definition, 'attacks' are 'acts of violence against the adversary, whether in offence or in defence'.[29] On its part, a 'cyber-attack' is 'a cyber-operation, whether offensive or defensive, that is reasonably expected to cause injury or death to persons or damage or destruction to objects'.[30]Attacks are not limited to acts of violence that have physical force but they also include acts that achieve damage without purely physical consequences.[31] The consequences of an act of violence are what determine whether a certain act amounts to an attack.[32] For instance, a cyber-operation that takes control of a dam and results in the release of 'dangerous forces' qualifies as an attack. [33] Such a cyber-operation would also

---

24 Bacet J, 'Inside the cunning, unprecedented hack of Ukraine's power grid' Wired, 3 March 2016 <https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/> on 20 March 2017.

25 Bacet J, 'Inside the cunning, unprecedented hack of Ukraine's power grid' Wired, 3 March 2016 <https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/> on 20 March 2017.

26 Kodar E, 'Applying the law of armed conflicts to cyber attacks', 115.

27 Kodar E, 'Applying the law of armed conflicts to cyber attacks', 115.

28 Kodar E, 'Applying the law of armed conflicts to cyber attacks', 115.

29 Article 49(1), *Additional Protocol I.*

30 International Group of Experts, *Tallinn manual*, 106.

31 International Group of Experts, *Tallinn manual*, 107.

32 International Group of Experts, *Tallinn manual*, 107.

33 Henckaerts JM and Doswald-Beck L, *Customary international humanitarian law – Volume 1: Rules*, 139. The term 'dangerous forces' is derived from Rule 42 which states that 'Particular care must be taken if works and installations containing dangerous forces, namely dams, dykes and nuclear electrical generating stations, and other installations located at or in their vicinity are attacked, in order to avoid the release of dangerous forces and consequent severe losses among the civilian population'. See also International Group of Experts, *Tallinn manual*, 223. In this paper, 'dangerous forces' and 'violent forces' are used interchangeably.

violate the prohibition against 'severe losses among the civilian population'.[34] Furthermore, such an attack violates the principle of proportionality pursuant to Article 57(2)(b) of AP I which requires that no attacks shall be conducted that result in the 'incidental loss of civilian life, injury to civilians, damage to civilian objects, or a combination thereof, which would be excessive in relation to the military advantage anticipated'.

The prohibitions against attacking civilians and civilian objects vis-à-vis the definition of 'attacks' as acts of violence that involve combative effects or force poses a dilemma.[35] The dilemma is that most cyber operations do not involve direct 'release of dangerous forces'.[36] Schmitt captures this conundrum as follows:

> 'The cognitive dilemma is that cyber operations do not directly involve the release of violent forces. This raises the questions, whether and when cyber operations qualify as attacks under international humanitarian law such that its prohibitions and restrictions thereon apply'.[37]

Furthermore, the occurrence of injury in the notion of 'attack' also includes 'significant human suffering or mental anguish' and loss of property.[38] If the act in question only amounts to a 'mere inconvenience or discomfort' then the consequences are too inadequate to qualify as an attack.[39] For instance, the use of cyber capabilities that merely deface websites or interrupt media as in the Russo-Georgian armed conflict do not amount to an attack within the realm of IHL.[40] In like manner, the utilisation of cyber capabilities in the Syrian armed conflict to gather information about civilians does not qualify as an attack because the cyber capabilities are merely contributing to other actions of the attackers.[41]

---

34 Article 56(6), *Additional Protocol I.*

35 Schmitt M, '"Attack" as a term of art in international law: The cyber operations context' 4th International Conference on Cyber Conflict, Tallinn, 2012,290.

36 Schmitt M, '"Attack" as a term of art in international law: The cyber operations context', 290.

37 Schmitt M, '"Attack" as a term of art in international law: The cyber operations context', 290.

38 Richardson J, 'Stuxnet as cyber warfare: Applying the law of war to the virtual battlefield', *Social Science Research Network*, 2011, 14.

39 Schmitt M, 'Wired warfare: Computer network attack and *jus in bello*', 84 *International Review of the Red Cross,* 2002, 381.

40 Swanson L, 'The era of cyber warfare: Applying international humanitarian law to the Russian-Georgian cyber conflict', 323.

41 Lee B, 'The impact of cyber capabilities in the Syrian civil war' *Small Wars Journal*, 2016 – <http://smallwarsjournal.com/jrnl/art/the-impact-of-cyber-capabilities-in-the-syrian-civil-war> on 20 November 2017.

iii. Anonymity

Cyberspace is the latest frontier of modern warfare.[42] Its true power lies in the perpetrators' ability to mask their identity behind their computers, unlike in kinetic operations where rivals are aware of the other party's identity in most cases.[43] Dominance in cyber warfare is almost synonymous with anonymity.

In fact, parties not only clutch at their anonymity, but they also go to great lengths to erase any trace of evidence that would reveal their identity. The cyber capabilities of states are usually highly sophisticated due to the growing fear of the potential threats to national security in recent times.[44] Cyber warfare can be waged using a keyboard from halfway around the world without sending marching troops to the battlefield. It may execute all the desired commands of the parties and even result in gross violations of IHL but the very ability to eliminate adversaries with such accuracy comes with a price – attribution of responsibility when evidence has already been erased. Ages past have been bloodied under cloak and dagger; our time lives in fear of cloak and keyboard.

The *Sony Hack* involved a cyber-attack against Sony Studios in America and it spawned questions on whether it amounted to the use of force, but more importantly, whether this amounted to an act of war which would activate the application of IHL. Specifically, it raised the question whether the destruction of data and leaking of emails, reached the threshold of an armed conflict.[45] Mandia and Lewis attributed the *Sony Hack* to the North Korean government on the basis that the attack was sophisticated in a manner akin to their military style.[46] Secondly, the malware in the *Sony Hack* was identical in form to the one used in the 2013 attack against the South Korean banks.[47] In the 2013 South Korean hack, the actions were attributed to North Korea.[48]

---

42 Lt. Gen Richard P. Mills, speech, AFCEA Technet Land Forces East Chapter Lunch, 21 August 2012 <https://www.slideshare.net/afcea/afcea-technet-land-forces-east-aberdeen-chapter-lunch-ltgen-richard-p-mills-usmc> on 22 November 2017.

43 Rosana C, 'Anonymity prevents application of rules of war in cyber attacks' Business Daily,29 August 2017, <https://www.businessdailyafrica.com/analysis/Anonymity-prevents-application-of-rules-of-war-in-cyber-attacks/539548-4076126-kg5j7g/index.html> on 3 February 2018.

44 ICRC, *International humanitarian law and the challenges of contemporary armed conflicts*, 2011, 39.

45 Schmitt M, 'The state of humanitarian law in cyber conflict' Just Security, 6 January 2015 - <https://www.justsecurity.org/18891/state-humanitarian-law-cyber-conflict/> on 15 January 2017.

46 Croft S and Messick G, 'The attack on Sony' CBS News, 12 April 2012<http://www.cbsnews.com/news/north-korean-cyberattack-on-sony-60-minutes/>on 15 January 2017.

47 Croft S and Messick G, 'The attack on Sony' CBS News, 12 April 2012<http://www.cbsnews.com/news/north-korean-cyberattack-on-sony-60-minutes/>on 15 January 2017.

48 Croft S and Messick G, 'The attack on Sony' CBS News, 12 April 2012<http://www.cbsnews.com/news/north-korean-cyberattack-on-sony-60-minutes/>on 15 January 2017. However, this is

According to the Tallinn Manual, such actions would qualify as an armed attack within Article 49(1) of AP I: 'attacks means acts of violence against the adversary, whether in offence or defence'. The Tallinn Manual also defines a cyber-attack as a 'cyber operation, whether offensive or defensive that is reasonably expected to cause injury or death to persons or damage or destruction to objects'.[49] Therefore, the destruction of data in the *Sony Hack* would qualify as an armed attack and all relevant laws of IHL would apply in the event that an armed conflict ensues.[50] Moreover, biological, chemical or radiological attacks do not produce kinetic force but are duly recognised as armed attacks. Thus, it is unnecessary for a cyber-attack to produce purely physical effects in order for IHL to apply. [51] If America responded to the cyber-attack in a similar manner, it would amount to an international armed conflict with North Korea.

III. Responsibility and Attribution

From a technical standpoint, the Internet is a continuum of internet protocol (IP) addresses. Each computer or device used to access the Web requires a distinct identifying IP address.[52] Information is transmitted on the Internet in the form of packets, which contain the destination points and other relevant instructions. [53] The packets are then relayed through routers.[54] Routers are primarily designed to relay information without verifying its source or whether the source is pretentious.[55] The whole structure is set to ensure information follows its course, but it does not endeavour to establish the veracity of the source or when the source has been altered in order to obscure the location of the sender.

Cyber intrusions and attacks may be investigated to the point of revealing the sending computer's IP address but that does not stand to satisfy the identity

problematic when it comes to assigning individual criminal responsibility (or some variation thereof) or state responsibility.

49 International Group of Experts, *Tallinn manual,* 106.

50 International Group of Experts, *Tallinn manual,* 106.

51 International Group of Experts, *Tallinn manual,* 106. The Tallinn Manual describes this as 'kinetic force'.

52 Clark D and Landau S, 'Untangling attribution' 2 *Harvard National Security Journal,* 2011, 1-30.

53 Shuler R, 'How does the internet work?' 2002 – <https://web.stanford.edu/class/msande91si/www-spr04/readings/week1/internetwhitepaper.htm> on 15 February 2017.

54 Clark D and Landau S, 'Untangling attribution', 15.

55 Clark D and Landau S, 'Untangling attribution', 15.

of the actor behind the keyboard.[56] For one to claim with certainty that K committed a cyber-attack against P, it is not sufficient to rely on the evidence of IP addresses. The realm of the Internet is sculptured in a way that computers can be commandeered with malicious code.[57] To add to this sophistication, the attackers can 'spoof'[58] the IP addresses of the primary computers that are used in the attack, in essence altering their identity in a way that leaves evidence pointing to other machines. For example, American intelligence officials faced these difficulties of attribution of individual criminal responsibility in 1998. They investigated certain cyber-attacks against the Department of Defence. Their investigations led them to believe that Iraq was responsible for the attacks, yet the real culprits were two teenagers from Northern California.[59]

Though these cyber-attacks are executed in cyberspace, the damage is felt in the real world; the effects do not remain virtual. The destruction of a dam or a nuclear facility, which subsequently decimates a nearby village, is no doubt a war crime and a grave breach of IHL. The legal framework of IHL succinctly prohibits the relevant crimes that are committed in an armed conflict. However, there are evidentiary problems that could arise in attribution and responsibility. The violations committed have real effects, but it begs the question on how the perpetrators may be held responsible. This section analyses some of the challenges that the law faces when it comes to the attribution of acts either to individuals or to states as the case may be.

i. State responsibility

State responsibility originates from state sovereignty and equality of states.[60] Under international law, when a state commits an internationally wrongful act against another state, there is an obligation to make reparations.[61] International law does not distinguish between treaty violations and contractual or tortious responsibility and so, any violation against another state of whatever origin brings an inescapable duty to make reparations.[62]

---

56 Swanson L, 'The era of cyber warfare', 303-333.

57 Clark D and Landau S, 'Untangling attribution', 15-17.

58 This means disguising the computers' IP address as that of another.

59 Beam C, 'Cyberspace invaders: Is a cyber-attack an act of war?' Slate, 7 November 2008 – <http://www.slate.com/id/2204123> on 18 November 2017.

60 Dimitrovska M, 'The concept of international responsibility of state in the international public law system' 1(2) *Journal of Liberty and International Affairs*, 2015, 4.

61 Shaw M, *International law,* 6ed, Cambridge University Press, Cambridge, 2008, 778.

62 Shaw M, *International law,* 779.

According to the Eritrea-Ethiopia Claims Commission, allegations of a breach of state responsibility can be made with the availability and presentation of 'clear and convincing evidence'.[63] However, the ICJ held, 'charges of exceptional gravity' against a state must be proved by evidence that is 'fully conclusive'.[64] Further, the seriousness of matters of state responsibility requires that if a state supports a certain allegation it must prove the existence of those facts.[65]

State responsibility has three components: first, the existence of an international obligation between two particular states; secondly, the occurrence of an act or omission, which is imputable to the state responsible; and thirdly, that loss or damage has occurred from the unlawful act or omission.[66] In the same vein, Judge Huber in the *Spanish Zone of Morocco Claims* highlighted that:

> 'Responsibility is the necessary corollary of a right. All rights of an international character involve international responsibility. Responsibility results in the duty to make reparation if the obligation is not met'.[67]

With the same emphasis, the rule is echoed in Article 1 of the International Law Commission's Articles on State Responsibility.[68] Further, Article 91 of AP I and Article 3 of the Convention respecting the Laws and Customs of War on Land provide for compensation when certain rules of IHL are violated.[69]

In order to appreciate the complexity of the matter, Lord West averred that states could be afforded plausible deniability. In an interview, he stated thus:'The moment you mention a particular state, they will deny it. The problem with cyberspace is that attribution is extremely difficult. It's almost impossible to do it in terms of evidence that would be necessary in a court of law'.[70]

---

63 Shaw M, *International law,* 780.

64 *Case concerning the application of the Convention on the prevention and punishment of the crime of genocide (Bosnia and Herzegovina v Serbia and Montenegro) case*, ICJ Reports 2007, 90.

65 *Genocide Convention case*, ICJ, para. 204.

66 Shaw M, *International law,* 780.

67 *Spanish Zone of Morocco Claims, General Decisions (Principles of State Responsibility),* United Nations Reports of International Arbitral Awards, 641.

68 Article 1, *Draft articles on responsibility of states for internationally wrongful acts with commentaries,* 2001, A/56/10.

69 Henckaerts JM and Doswald-Beck L, *Customary international humanitarian law,* 530-550.

70 Doward J, 'Britain fends off flood of foreign cyber-attacks' The Guardian, 7 March 2010 –<https://www.theguardian.com/technology/2010/mar/07/britain-fends-off-cyber-attacks> on 13 February 2017.

ii. Attribution

As in individual criminal responsibility, evidentiary problems arise in attribution of cyber-attacks to states. Graham explains the difficulty of obtaining credible and convincing evidence in the following terms:

> 'Given the anonymity of the technology involved, attribution of a cyber-attack to a specific state may be very difficult. While a victim state might ultimately succeed in tracing a cyber-attack to a specific server in another state, this can be an exceptionally time-consuming process, and, even then, it may be impossible to definitively identify the entity or individual directing the attack. For example, the 'attacker' might well have hijacked innocent systems and used these as 'zombies' in conducting attacks'.[71]

Identifying the responsible state remains elusive. Perpetrator states may contract hacker collectives or similar non-state actors with cyber capabilities to conduct attacks against another state. International courts and tribunals applying the tests of 'effective control' and 'overall control' would run into hurdles since it would be challenging to ascertain the level of control or support from the state involved.[72] By and large, the difficulties in attribution only serve to promote a climate of impunity for the states.[73]

It is 'attributability … [the] ability to say 'who did it' that makes law work. When a transgressor can be identified, penalties can be assessed, and retaliation and deterrence are possible – and so is legal regulation'.[74] Ascertaining the source of attacks is extremely challenging within cyber operations and that in essence poses a problem to the application of the law. This is not a weakness of the law but an indication of the 'genetic' make-up of technology. The forte of technology stands in conflict with the law because technology assures anonymity in cyber operations while the law seeks the concealed identity in order to act.

At this level of possibilities, state K can launch an attack against state P while commandeering computers in state D and spoofing the IP addresses to make it seem as though state H is responsible for the attack. These complications are compounded even further by the use of 'distributed denial of service' (DDoS) attacks. DDoS attacks use the combined power of thousands of computers in order to impair a specific website.[75] Swanson writes that 'through DDoS

---

71 Graham D, 'Cyber threats and the law of war' 4(1) *Journal of National Security Law & Policy,* 2006, 92.

72 Chatham House, *Cyber security and international law meeting summary,* 2012, 11.

73 Graham D, 'Cyber threats and the law of war', 92.

74 Glennon M, 'The road ahead: Gaps, leaks and drips' 89 (362) *International Law Studies*, 2013, 380.

75 Margulies P, 'Sovereignty and cyber attacks: Technology's challenge to the law of state responsibility' 14(496) *Melbourne Journal of International Law*, 2013, 496.

attacks, like those against Georgia, the cyber-attacker shuts down a website by bombarding it with large amounts of traffic'.[76] DDoS attacks make the websites affected inaccessible. Such attacks make it extremely difficult to trace the original actor while simultaneously accomplishing its objective. The location and IP address of a computer are far too unreliable in assigning responsibility for any violations of IHL committed through cyber means.

As it stands, there are state actors who make use of non-state actors in order to carry out cyber-attacks against other states.[77] States capitalise on plausible deniability in order to ensure that they avoid any blowback that might result from a botched operation.[78] These outsourcing strategies by states create additional difficulties in identifying perpetrators of cyber-attacks.[79] For instance, the cyber-attacks on Georgia in 2008 as Russia's armies marched onto its territory cannot be definitively linked to the Kremlin.[80]

Under the law of state responsibility, the conduct of persons or entities acting on the instructions of, or under direction or control of, a state shall be attributable to that state.[81] The cyber-attacks of these outsourced entities are directly attributable to the controlling states. In some instances, the state may have municipal legislation enabling independent contractors to carry out such tasks on behalf of the state concerned. Article 5 of the Draft Articles on State Responsibility provides that persons or entities not being state organs, who are empowered to carry out these tasks in a governmental capacity, are equated to state organs. Being a state organ, their actions attract international legal responsibility in case of any violations of IHL.

---

76 Swanson L, 'The era of cyber warfare: Applying international humanitarian law to the Russian-Georgian cyber conflict', 303-333.

77 'Marching off to cyberwar' The Economist, 4 December 2008 – http://www.economist.com/node/12673385 on 13 February 2017; Williams C, 'Cyber attacks will "catastrophically" spook public, warns GCHQ' The Register, 22 February 2010 – <http://www.theregister.co.uk/2010/02/22/csoc_report/> on 13 February 2017.

78 'Marching off to cyberwar' The Economist, 4 December 2008– http://www.economist.com/node/12673385 on 13 February 2017. Williams C, 'Cyber attacks will "catastrophically" spook public, warns GCHQ' The Register, 22 February 2010 – <http://www.theregister.co.uk/2010/02/22/csoc_report/> on 13 February 2017.

79 'Marching off to cyberwar' The Economist, 4 December 2008– http://www.economist.com/node/12673385 on 13 February 2017. Williams C, 'Cyber attacks will "catastrophically" spook public, warns GCHQ' The Register, 22 February 2010 –< http://www.theregister.co.uk/2010/02/22/csoc_report/> on 13 February 2017.

80 Sinopoli A, 'Cyberwar and international law', 39-40.

81 Article 8, *Draft articles on state responsibility for internationally wrongful acts*, ILC 53rd Report, 2001, UN Doc A/56/10.

iii. Unable or unwilling?

On 13 February 2017, Akbarrudin, India's Permanent Representative to the United Nations (UN), stated, 'Current international law is not well positioned to support responses to cyber-attacks'.[82] Akbarrudin's position was informed by the 26/11 terror attacks in Mumbai. In essence, India stated that current international law is ill-positioned in addressing the barrage of cyber-attacks that plague a world with budding interconnectedness.[83]

In recent times, states have tried to forge a legal framework to govern cyber warfare or hostile actions within cyberspace. These efforts were precipitated by Russia and China's submissions in the drafting process of the *International Code of Conduct for Information Security* (Code).[84] The Code requires states 'not to use information and communications technologies, including networks, to carry out hostile activities or acts of aggression, pose threats to international peace and security or proliferate information weapons or related technologies'.[85] The Code somewhat reflects the hurdles that may arise in the negotiation of a cyber-treaty by providing insight into the matters that are of particular interest to states.[86]

The amorphous nature of cyber warfare and its accompanying cyber weapons renders any agreements on its regulation an uphill task.[87] As a preliminary matter, states are already plagued with the conundrum of definitional agreement.[88] The international community cannot easily reach legal consensus on a matter that is constantly evolving and whose specific components present definitional challenges.[89]

---

82 'India says international law not ready to deal with cyber attacks' E Hacking News, 15 February 2017 – <http://ehackingnews.com/2017/02/india-says-international-law-not-ready.html?utm_content=bufferccd02&utm_medium=social&utm_source=twitter.com&utm_campaign=buffer&m=1>on 23 February 2017.

83 'India says international law not ready to deal with cyber attacks' E Hacking News, 15 February 2017 – <http://ehackingnews.com/2017/02/india-says-international-law-not-ready.html?utm_content=bufferccd02&utm_medium=social&utm_source=twitter.com&utm_campaign=buffer&m=1>on 23 February 2017.

84 *International code of conduct for information security*, UN Doc. A/66/359, 14 September 2011.

85 *International code of conduct for information security*, 4.

86 Arimatsu L, 'A treaty for governing cyber-weapons: Potential benefits and practical limitations' 42nd International Conference on Cyber Conflict, Tallinn, 2012, 92.

87 *Group of governmental experts on developments in the field of information and telecommunications in the context of international security*, UN Doc A/68/98, 24 June 2013, 7.

88 *Group of governmental experts on developments in the field of information and telecommunications in the context of international security*, 7.

89 *Group of governmental experts on developments in the field of information and telecommunications in the context of international security*, 7.

The inability to forge a legal framework specifically targeted at cyber warfare, also faces problems from other fronts. Firstly, for a treaty to work the state must give its consent and support the realisation of the listed goals pursuant to the doctrine of *pacta sunt servanda*.[90] For instance, in reference to arms control treaties, states give such support and consent due to their monopoly or control over the subject matter.[91]

Concerning cyber weapons, states do not have such control, monopoly or ownership and thus any cyber treaty would not evoke commitment because malware, spyware or malicious programs are mainly under the thumb of the private sector.[92] The states, for the most part, tend to be major users rather than major owners. In short, states would be unwilling to act in vain by promising to control what is beyond their scope.

Secondly, and more importantly, non-compliance is a major possibility due to the outlook on cyber warfare.[93] Compliance will potentially entail the establishment of a 'reliable verification system'[94] that makes it unlikely for states to submit to external measures that would 'require scanning all computers and storage devices owned and used by the state including all classified systems'.[95]

In the name of national interest, it is inconceivable that any state would be willing to be bound. Such verification measures are a step towards ensuring international security, but it seems too high a price on an individual basis. States would rather forgo collective advantage than experience individual vulnerability.[96] Consequently, a possible cyber treaty would be ineffective because its implementation would go contrary to each state's national interest. In parallel terms, Goldsmith and Wu specified:

> 'National governments are sometimes too close to (or too reflective of) their populations. They sometimes reject the rational or best solution to a global problem in favour of a local tradition or in obedience to a powerful local interest group. Many believed that international standards applied to the Internet would eliminate the parochialism of

---

90 Article 26, *Vienna Convention on the Law of Treaties*, 23 May 1969, 1155 UNTS 331. *Pacta sunt servanda* is a universally recognised principle that parties to an agreement must fulfill their obligation. Shaw M, *International law*, 10, 29, 50 and 94.

91 *Group of governmental experts on developments in the field of information and telecommunications in the context of international security*, 6.

92 *Group of governmental experts on developments in the field of information and telecommunications in the context of international security*, 7.

93 Arimatsu L, 'A treaty for governing cyber-weapons', 92.

94 Arimatsu L, 'A treaty for governing cyber-weapons', 92.

95 Arimatsu L, 'A treaty for governing cyber-weapons', 92.

96 *Group of governmental experts on developments in the field of information and telecommunications in the context of international security*, 6.

> territorial legalism. International standards could reflect a kind of collection of best practices from around the world – the opposite of the tyranny of the unreasonable. An international approach could not only clear up confusion and conflict, but it could also wash clean the prejudice and ignorance hiding in the basement of national government'.[97]

The Group of 7 (G7) nations created the *G7 Declaration on Responsible States Behaviour in Cyberspace* (Declaration) on 11 April 2017.[98] The Declaration recognises that cyberspace can be a domain for the destruction of critical infrastructure that provide public services.[99] It reiterates the need for states to refrain from cyber-enabled interference of democratic political processes.[100] The Declaration affirms the applicability of current international law to cyberspace while urging states to build cyber confidence building measures (CBMs).[101] It has striking similarities to some of the provisions of the UN Charter, for instance, in its requirement that 'states should refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any state'.[102] The Declaration is a positive step towards addressing the challenges of using cyberspace as a frontier of armed conflict.

Another step in regulating behaviour in cyberspace is the European Union's Convention on Cybercrime, otherwise known as the 'Budapest Convention'. Nevertheless, the convention is not immediately applicable in the context of armed conflict because it deals with cybercrime as opposed to cyberspace as a domain of warfare. Cyber warfare is still in its early days and so states are unable to regulate it sufficiently at present because they do not possess sufficient knowledge on the future evolution of this means of warfare.[103] The Tallinn Manual is still the greatest advancement in regulating cyber warfare.

---

97 Goldsmith J and Wu T, *Who controls the internet? Illusions of a borderless world*, Oxford University Press, Oxford, 2008, 26.

98 Farnesina Ministero degli Affari Esteri e della Cooperazione Internazionale, 'G7 Foreign Ministers Meeting', 11 April 2016 – <http://www.esteri.it/mae/en/sala_stampa/archivionotizie/approfondimenti/ministeriale-g7.html> on 20 November 2017.

99 G7 declaration on responsible states behaviour in cyberspace, Lucca, 11 April 2017. The Declaration was a supplement to the 2016 'G7 principles and actions on cyber'.

100 G7 declaration on responsible states behaviour in cyberspace, Lucca, 11 April 2017.

101 G7 declaration on responsible states behaviour in cyberspace, Lucca, 11 April 2017.

102 G7 declaration on responsible states behaviour in cyberspace, Lucca, 11 April 2017.

103 This is made in comparison with the regulation of nuclear weapons. Nuclear weapons have existed for decades yet it took a considerable amount of time for discussion on their regulation until the Treaty on the Prohibition of Nuclear Weapons was birthed on 7 July 2017. Thus, it is too early for the sufficient regulation of cyber warfare because international law generally develops at a slow pace and especially when the subject in question is the regulation of technology. Rosana C, 'Self-regulation, soft laws best way to regulate technology' Business Daily Africa, 22 October 2017 <http://www.businessdailyafrica.com/analysis/soft-laws-the-best-way-to-deal-with-technology/539548-4151212-2avpmnz/index.html> on 21 November 2017.

IV. Applying IHL to Modern Armed Conflicts

Most recently, the use of cyber operations has been manifested overtly in the 2008 international armed conflict between Russia and Georgia,[104] the Afghanistan and Iraq armed conflicts,[105] the Libya and Syria non-international armed conflicts,[106] and partly in the 2014 Russia and Ukraine international armed conflict.[107] This section focuses on a sample of these conflicts within the paradigm of cyber warfare as analysed thus far in this work. Specifically, the section analyses the violation of IHL principles within cyber warfare – distinction, necessity, proportionality, and precaution.

i. The Russo-Georgian armed conflict

The world watched the Georgian conflict on screens and read widely on news sites but the cyber-attacks on Georgia stood in the shadows of the frenzied Russian tanks moving onto their neighbour's soil.[108] The cyber-attacks effectively deactivated Georgian news sites and government websites[109] thus gagging and blinding the Georgian people simultaneously[110] – they could neither obtain information nor communicate the incident to the rest of the world.[111] The cyber assault was chiefly positioned to 'isolate and silence'[112] so that the Georgian media could not relay information while the larger state was in a (somewhat) virtual quarantine.

From the coordinated double-edged attack on Georgia, it is plausible that the Russian government sanctioned the cyber-attacks to facilitate a crippling assault on Georgian infrastructure.[113] However, Sinopoli writes that, 'there was no direct linkage between Russian government involvement and the cyber-

[104] Tikk E, Kaska K and Vihul L, *International cyber incidents: legal considerations*, Cooperative Cyber Defence Centre of Excellence, Tallinn, 2010, 11.

[105] Schmitt M, 'Rewired warfare: Rethinking the law of cyber attack' 96(893) *International Review of the Red Cross*, 2014, 189.

[106] Schmitt M, 'Rewired warfare', 189.

[107] Schmitt M, 'Rewired warfare', 189.

[108] Allan C, 'Attribution issues in cyberspace' 13(2) *Chicago-Kent Journal of International and Comparative Law*, 2013, 58.

[109] Ashmore W, 'Impact of alleged Russian cyber attacks' 11(4) *Baltic Security and Defense Review*, 10.

[110] Shakarian P, 'The 2008 Russian cyber campaign against Georgia' 91(6) *Military Review*, 2011, 1.

[111] Allan C, 'Attribution issues in cyberspace', 58.

[112] Corbin K, 'Lessons from the Russia-Georgia cyber war' Internet News.Com, 12 March 2009 – <http://www.internetnews.com/government/article.php/3810011/lessons-From-the-russia-Georgia-Cyberwar.htm>on 2 March 2017.

[113] Malek M, 'Georgia & Russia: The "unknown" prelude to the "five day war"', 227-232.

attacks'.[114] Sanctioned or not, that may simply be conjecture as it cannot be definitively proved. It is certain that the Russian government benefited directly from these cyber-attacks but its direct involvement is still a matter of reasonable doubt.[115] In the words of Ashmore, 'according to outside investigators there is no direct proof of any Russian government in the cyber-attacks'.[116]

The cyber-attacks comprised DDoS attacks with botnets[117] and combined with Structured Query Language (SQL) injection attacks.[118] Various actors assisted in the Georgian situation by sending experts to mitigate the effects of the cyber-attacks.[119]

Nonetheless, the cyber-attacks in Georgia resulted in widespread confusion and hampered communication as they successfully brought down the websites but they did not amount to a violation of IHL principles.[120] The confusion and inconvenience caused by targeting the websites is permissible regardless of whether these were civilian objects or military objectives.[121]

ii. Syria's armed conflict

Since 2011, the Syrian Electronic Army has acted in support of President Bashar al-Assad's regime by stifling political dissent through various means including website defacement, phishing, malware, and spamming.[122] According to Lee, the Syrian war is a fulfilment of a prophecy by McNeill who had stated that the growth of mass communications technology would rival police power thus undercutting the ability of governments in developing countries to retain power.[123] The traditional monopoly on force by the state is effectively under

---

114 Sinopoli A, 'Cyberwar and international law', 40.

115 Ashmore W, 'Impact of alleged Russian cyber attacks', 10

116 Ashmore W, 'Impact of alleged Russian cyber attacks', 10.

117 A botnet is a network of computers infected with malicious software and controlled as a group without the owner's knowledge. European Network and Information Security Agency, *Botnets: Detection, measurement, disinfection & defence,* 2011, 2.

118 SQL injection attacks are harder to track and trace due to their sophistication and they are a show of greater expertise. United States Computer Emergency Readiness Team, *Practical identification of SQL injection vulnerabilities,* 2012, 1.

119 Ashmore W, 'Impact of alleged Russian cyber attacks', 10.

120 Swanson L, 'The era of cyber warfare', 303-333.

121 Schmitt M, 'Wired warfare', 365.

122 Noman H, 'The emergence of open and organised pro-government cyber attacks in the Middle East: The case of the Syrian electronic army' Open Net Initiative, 5 May 2011– <https://opennet.net/emergence-open-and-organized-pro-government-cyber-attacks-middle-east-case-syrian-electronic-army> on 20 November 2017.

123 Lee B, 'The impact of cyber capabilities in the Syrian civil war' Small Wars Journal, 26 April 2016 – <http://smallwarsjournal.com/jrnl/art/the-impact-of-cyber-capabilities-in-the-syrian-civil-war> on 20 November 2017.

fire because cyber capabilities are easily accessible to states and non-state actors alike.[124] With the Syrian conflict moving online, it begs the question whether this is becoming a prototype for future wars.[125]

The Free Syria Army carried out DDoS attacks against the Syrian government and any pro-Assad media outlets.[126] Civilian individuals with hacking skills have utilised their skills in support of either side of the conflict but mainly for the opposition.[127] This is in response to the government's efforts of Internet censorship to inhibit the cyber capabilities of the opposition or release of any injurious news regarding Assad's crackdown on civilian dissent.[128] The Syrian Electronic Army also uploads malware onto social media sites to attack any opposition sympathisers or; specifically, to obtain the opposition's passwords and to carry out surveillance.[129] As a ruse of war, the Syrian Electronic Army subsequently also supplied fake battle plans to the opposition in order to draw them into ambushes.[130]

The Syrian conflict is living proof that the incorporation of cyber capabilities into kinetic warfare magnifies the effects of the attacks.[131] The armies of lone hackers and hacker collectives such as Syrian Electronic Army aid the ground forces in carrying out the attacks more efficiently because they can use Remote Access Tools to monitor opposition groups and pinpoint their locations.[132] The Syrian Electronic Army supplies information regarding the identities and locations of opposition groups through back channels to the Assad regime which then tortures and executes the individuals.[133]

---

124 This includes civilians.

125 Makuch B, Cyberwar, Season 1 Episode 5, "Syria's Cyber Battlefields".

126 Shehabat A, 'The social media cyber-war: The unfolding events in the Syrian revolution 2011' 6(2) *Global Media Journal*, 2013, 2.

127 Lee B, 'The impact of cyber capabilities in the Syrian civil war'Small Wars Journal, 26 April 2016 – <http://smallwarsjournal.com/jrnl/art/the-impact-of-cyber-capabilities-in-the-syrian-civil-war> on 20 November 2017.

128 Lee B, 'The impact of cyber capabilities in the Syrian civil war'Small Wars Journal, 26 April 2016 – <http://smallwarsjournal.com/jrnl/art/the-impact-of-cyber-capabilities-in-the-syrian-civil-war> on 20 November 2017.

129 Warf B and Fekete E, 'Relational geographies of cyber-terrorism and cyberwar' 20(2) *Space and Polity*, 2016, 9.

130 Lee B, 'The impact of cyber capabilities in the Syrian civil war' Small Wars Journal, 26 April 2016 – <http://smallwarsjournal.com/jrnl/art/the-impact-of-cyber-capabilities-in-the-syrian-civil-war> on 20 November 2017.

131 If the malicious code is of the magnitude of Stuxnet it cripples a nation's infrastructure in seconds leaving civilians and soldiers affected in like manner. The ability to wage massive attacks with strokes of a keyboard is gradually rivalling the depredations of ground troops. For instance, the damage and lives lost if a customised Stuxnet worm is unleashed into the hospitals, the electric grid or a nuclear plant.

132 Makuch B, Cyberwar, Season 1 Episode 5, 00:19:48.

133 Makuch B, Cyberwar, Season 1 Episode 5, 00:19:48.

Furthermore, the cyber tools used in the Syrian conflict can be procured easily and are available to anyone with a computer or phone.[134] The most one needs to do is search for them on a search engine and press 'download and install'. The availability of cyber tools has divested the state of its monopoly to use force but that also comes at a price – civilians effortlessly commit more crimes in armed conflict either in support of any party or for egotistical interests and this makes for a conflict of everyone against everyone. The ease of procuring cyber tools exacerbates the violations of IHL during an armed conflict. The fact that civilians can conduct these attacks anonymously may create a temptation to participate directly in hostilities thus losing protection under IHL. The greatest drawback is that this increases the damage and devastation resulting from cyber warfare.

It is apparent that the incorporation of cyber capabilities alongside kinetic tactics exacerbates the effect of armed conflict. In the event that these attacks are made against critical infrastructure of a state, the effects would be beyond calculation.[135] It may be too soon to assume that the future does not hold conflicts where attacks will be solely dependent on the 'keyboard combatant'.[136] Further, the vagaries of war are compounded by the ability of civilians to take a direct part in cyber-attacks. The skills can be learnt easily by anyone and the attendant tools are available for download on the Internet. Consequently, the loss of monopoly to wage war has made conflicts more dangerous while leaving civilians ever more exposed as in the Syrian armed conflict.

iii. The imbalances of cyber power

Cyber power is 'the ability to obtain preferred outcomes through the use of the electronically interconnected information resource of the cyber domain'.[137] There are inequalities of cyber power within the various states in the international community.[138] Each state has a different amount of power, with some on the extreme end of the spectrum with massive power while others barely catching up.[139] To this extent, cyber power is also 'the ability to withstand cyber-attacks and to deploy the digital infrastructure, necessary for a productive and secure economy'.[140]

---

134 Electronic Frontier Foundation, *Quantum of surveillance: Familiar actors and possible false flags in Syrian malware campaign,* 2013, 2.

135 See generally Chatham House, *Cyber security and international law,* 2012.

136 See generally Chatham House, *Cyber security and international law,* 2012.

137 Nye S, 'Cyber power' *Belfer Center for Science and International Affairs*, 2010, 3-4.

138 Gomez M, 'Identifying cyber strategies vis-à-vis cyber power' De La Salle University, Manila, 3-4.

139 Gomez M, 'Identifying cyber strategies vis-à-vis cyber power', 3-4.

140 Hamilton B, Cyber power index: Findings and methodology, 2011, 20.

In essence, each state can wage cyber warfare but only to the extent of their capabilities. However, states will not resort to cyber warfare if they know that any retaliation will leave them more vulnerable. For political suitability, some states may also avoid the use of cyber warfare if the geopolitical effects would deny them plausible deniability. It leaves the less capable states at the mercy of the cyber powerful states, which may decide whether it would be in their interest to utilise such a means of warfare.

V. Weapons Review under Article 36 of Additional Protocol I

The nature of cyberspace creates a cloud of uncertainty and impunity where criminals, states, and non-state actors may commit certain crimes without detection. It creates an infamous atmosphere where states may outsource elements of cyber warfare to hacker syndicates in support of their ground forces. The violations committed may be ascertained from existing motives from geopolitical events but that is of no particular importance in court due to the inexistence of admissible evidence. Alternatively phrased, a cyber-attack may benefit a specific state but such an observation is insufficient in order to impute the state's involvement and culpability. Hence, perpetrators find a safe haven of less political risk, and assured plausible deniability.

As a grim result, the difficulty in obtaining admissible evidence in cyber warfare prepares a fertile ground for transnational crime due to the existing uncertainty of establishing the actor responsible.[141] It creates a precarious position of the possibilities of total war because the tools and skills used in cyber warfare are readily available to civilians and soldiers alike. Civilians taking part in hostilities directly lose their protection under IHL.[142] However, the inherent goal of IHL is the alleviation of the attendant suffering emanating from armed conflict rather than to legitimise the use of cyber warfare as a tool for violations.[143]

In this regard, Article 36 of AP I provides:

> 'In the study, development, acquisition or adoption of a new weapon, means or methods of warfare, a High Contracting Party is under obligation to determine whether

[141] See generally Sinopoli A, 'Cyberwar and international law' and Graham D, 'Cyber threats and the law of war'.

[142] Henckaerts JM and Doswald-Beck L, *Customary international humanitarian law*, 19.

[143] For further discussion ICRC, 'What limits does the law of war impose on cyber attacks?' 28 June 2013 <https://www.icrc.org/eng/resources/documents/faq/130628-cyber-warfare-q-and-a-eng.htm> on 23 March 2017.

> 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'.[144]

Despite the valid points made in this Article, a very limited number of states are known to carry out a legal review of emerging weapons.[145] The uniqueness of new weapons poses a myriad of challenges in the application and interpretation of IHL[146] because it may be too soon to analyse all the foreseeable effects of a new weapon at the point of its invention.[147] Nevertheless, states have an obligation to carry out such reviews in order to promote implementation of IHL. In the context of cyber warfare, the Tallinn Manual stands as the first of its kind to offer guidance on the matter in the absence of equivalent legal reviews. The Tallinn Manual explains the applicability of international law towards cyber-attacks.

Article 36 of AP I may carry a solution to the challenges and complexities of cyber-attacks. The futuristic style of the Article sought to address future weapons and in the instant case, states should conduct regular reviews of weapons in order to find solutions for the issues at hand. Since cyber warfare is a phenomenon that evolves despite the evident imbalances of cyber power, international cooperation in weapons review would be the best way to grapple with these complexities. In order to apply Article 36 appropriately, it is important that states understand how cyberspace and cyber-attacks keep changing and how they work.[148] Moreover, Article 36 is an excellent opportunity for states to anticipate the problems that may arise in the future and to find ways to implement IHL in the development of future means and methods of warfare.[149] In a Sun Tzu fashion, those who are not thoroughly aware of the disadvantages of the use of cyber-attacks cannot be thoroughly aware of the advantages of the use of cyber-attacks.[150]

---

144 Article 36, *Additional Protocol I.*

145 ICRC, *A guide to the legal review of new weapons, means and methods of warfare: Measures to implement Article 36 of Additional Protocol I of 1977,* 2006.

146 ICRC, *International humanitarian law and the challenges of contemporary armed conflicts*, October 2015, 39.

147 In Plato's *Phaedrus,* Socrates states "...the discoverer of an art is not the best judge of the good or harm which will accrue to those who practice it…" This was a story pointing out that invention of a new technology does not come with the equal wisdom of knowing the possible effects that it will bring. Plato, *Phaedrus and Letters VII and VIII*, Penguin Books, New York, 1973, 96 as cited in Postman N, *Technopoly: The surrender of culture to technology*, 1ed, Vintage Books, New York, 1992, 4.

148 McClelland J, 'The review of weapons in accordance with Article 36 of Additional Protocol I' 85(850) *International Review of the Red Cross*, 2003, 405.

149 McClelland J, 'The review of weapons in accordance with Article 36 of Additional Protocol I', 410.

150 The original quote goes 'Therefore, those who are not thoroughly aware of the disadvantages in the use of arms cannot be thoroughly aware of the advantages in the use of arms'. Sun Tzu, *The Art of War,* circa 500 BC.

Notwithstanding the recommendation towards international cooperation, a state is not obliged to publicise its legal reviews of weapons.[151] In the negotiation process of the Additional Protocols to the Geneva Conventions of 1949, there were suggestions for the creation of a central body whose sole responsibility would be conducting weapons reviews.[152] The international community abandoned the suggestion in favour of the current state-centred process in Article 36. A uniform system would not be feasible due to the differences in the way each state would approach their legal review of weapons.[153]

One of the foremost subjects for legal review is what would constitute a 'cyber weapon'. There is a general failure to distinguish what qualifies as a weapon in the realm of cyber.[154] Specifically, it begs the question whether it is computer code, or the computer itself that qualifies as the weapon.[155] Thus, regular weapons reviews would be an appropriate step towards finding solutions to the apparent ambiguities of cyber-attacks.

VI. Conclusion

The difficulty in assigning responsibility does not mean that no one should be held responsible. The delegation of tasks to code and keyboard does not absolve the actors from their ethical and legal responsibilities. The obligations exist and cannot be typed away in the name of cyber warfare because human consciousness and judgment cannot be delegated in order to escape the consequences of our actions during warfare.[156] In the line of inventive steps and methods in order to make warfare more sophisticated, humans should always remain as the point of blame. If a state goes up in flames due to a cyber-attack from my country,

151 Zimmerman B, Pilloud C, Santoz Y et al, *Commentary on the Additional Protocols of 8 June 1977,* Martinus Nijhoff, Geneva, para. 1470. 'However, it should be added that a state which respects the obligation provided for in Article 36, and determines that a new weapon is prohibited, is not automatically obliged to make public its findings. This reservation is quite understandable, as modern strategy very often relies not on deployment of military means in the traditional ways, but on new possibilities resulting from research and which consists of creating an imbalance of military strengths vis-à-vis the enemy precisely by means of superior technology in the form of new weapons'.

152 McClelland J, 'The review of weapons in accordance with Article 36 of Additional Protocol I', 414.

153 McClelland J, 'The review of weapons in accordance with Article 36 of Additional Protocol I', 414.

154 Brown G and Metcalf A, 'Easier said than done: Legal review of cyber weapons' 7(115) *Journal of National Security Law and Policy*, 2014, 120.

155 Alternatively, it could be both the computer and the malicious code. For further discussion see generally Arimatsu L, 'A treaty for governing cyber-weapons'.

156 Bernard V, 'New technologies and warfare, humanitarian debate: Law, policy, action' 94(886) *International Review of the Red Cross,* 2012, 464.

it would be foolhardy to claim that the keyboard is to blame. In the realm of criminal law, we do not blame guns for crimes and hold them culpable. It would be illogical to assert that technology is somehow to blame when violations are committed. 'Science cannot be placed above its consequences'.[157]

Asimov and Shulman said, 'The saddest aspect of life right now is that science gathers knowledge faster than society gathers wisdom'.[158] Given the nuances that the use of cyber means have brought to the application of the law of armed conflict, it is upon us to take constructive steps in order to secure the safety and dignity of human life rather than cheapen it by letting keyboards and code decide our fate. Human life is more than two-dimension diagrams or pixels on a screen – the law of armed conflict is made with this in mind and no matter how complex cyber warfare has become, states need to find a way to ensure compliance with the new normal.

Thus, states should endeavour to implement their obligations under IHL within the realm of cyber warfare rather than use this new means of warfare as a way to evade their responsibilities. The obligations of IHL are still relevant even with the growth of technology. The worth of human life as protected under humanitarian law does not disappear with changes in means and methods of warfare. The alleviation of suffering in armed conflict is still a matter of overriding importance and this should remain in the mind of humanity as the law seeks to effect change in the world one keyboard at a time.

157 Bernard V, 'New technologies and warfare', 464.

158 Asimov I and Shulman J, *Isaac Asimov's book of science and nature quotations,* 1ed, Weidenfeld and Nicolson, New York, 1988, 281.