THE JOURNAL OF DIGITAL FORENSICS, SECURITY AND LAW

Journal of Digital Forensics, Security and Law

Volume 17 Article 8

3-24-2022

Fault Lines In The Application Of International Humanitarian Law To Cyberwarfare

HUMNA SOHAIL
International Islamic University, Islamabad, humnasohail97@gmail.com

FAULT LINES IN THE APPLICATION OF INTERNATIONAL HUMANITARIAN LAW TO CYBERWARFARE

Humna Sohail
LLM International Law Candidate
at International Islamic University
Islamabad, Pakistan
humnasohail97@gmail.com

ABSTRACT

The dynamics of warfare have changed from the conventional wars fought on the battlefield to virtual warfare as states have been involved in the cyber arms race. From simple distributed denial-of-service (DDoS) attacks to the potent Stuxnet and Flame the cyberweapons vary in their potential human cost. The Law of Armed Conflict (LOAC) is drafted flexibly to adapt to changing circumstances. This paper is primarily based upon the assumption that existing treaty law is sufficient in many aspects yet in some areas treaty-making is also needed. What is the foreseeable solution is the comprehensive state practice for interpreting the existing rules (*lex lata*) regulating the armed conflict in the cyber context. This is because armed conflicts in cyberspace differ from kinetic warfare in multiple dimensions. The world community is yet to reach a consensus on how LOAC protects at times of cyberwarfare. From defining the basic terms like attack and object to the attribution needs resolution. Given such ambiguity, international humanitarian law (IHL, interchangeably used with LOAC) will more frequently be violated in conflicts occurring in cyberspace than in physical space. Efforts by states in sincere exploitation of existing laws are the sine qua non for the evolution of IHL in the cyber context.

Keywords: international humanitarian law, cyberwarfare, cyberattack, data, attribution, international armed conflict, non-international armed conflict

1. INTRODUCTION

A sword never kills anybody: it is a tool in the killer's hand.
(Lucius A. Seneca)

International Humanitarian Law (IHL) consists of a body of rules, both conventional and customary, that regulates the conduct of belligerents during an armed conflict by prohibiting the use of certain methods means of warfare. The term war is deliberately omitted for a war-like situation might exist even when there is no formal declaration of war. So, to determine the applicability of IHL, it is quintessential to determine the onset of an armed conflict. The test for it was laid down by International Criminal Tribunal for Former Yugoslavia (ICTY) in the *Tadic*[1] case in the following words:

> "An armed conflict exists when states resort to force in their relations *inter se* or when there is a protracted armed violence between governmental forces and organized armed groups or between such groups only."

The said criterion also implies classifying armed conflicts broadly into international armed conflict (IAC) or an armed conflict not of an international character (NIAC also termed internal armed conflict). The said classification is essential for there are different laws applicable to each kind of conflict. Many of the treaty-based provisions have attained the status of customary norms, and as such, they bind all states equally[2]. However, many states are yet to ratify the Additional Protocols, and the provisions therein are not customary, and as such, they are binding only onto the states who have ratified them. The drafters intended to regulate physical warfare, and the modern warfare mediums like cyberspace were not known then.

The technological sophistication has enabled States to develop new weapons, and the law governing the use of such weapons needs to be exhaustive enough to adapt to changing circumstances[3] (Kathleen, 2006). Notwithstanding the relatively lesser number of scenarios where states have acknowledged the employment of cyber warfare during an armed conflict, the debate on the legal issues incidental to the conflicts involving cyberspace is high (Gisel, 2020). Cyberwarfare is referred to as the fifth domain of warfare, the other conventional domains being the land, air, sea, and outer space. Cyberspace offers virtual connectivity independent of territorial limits. With the multiple benefits of such interconnectivity comes the drawbacks, such as the users in interface with the network can easily be targeted where ever they are (Dinniss, 2008). There is always a possibility of a bug in the product unknown to manufacturers at the time of release, which the attacker can exploit for various purposes. For

[1]ICTY, The Prosecutor v Dusko Tadic, IT-94-1-AR72, Appeals Chamber, Decision, 2 October 1995, para 70.

[2]The core IHL treaties include the Hague Conventions of 1899 and 1907; Geneva Convention (I) for the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field, 1949; the Geneva Convention (II) for the Amelioration of the Condition of the Wounded, Sick, and Shipwrecked Members of Armed Forces at Sea, 1949; the Geneva Convention (III) Relative to the Treatment of Prisoners of War, 1949; The Geneva Convention (IV) Relative to the Protection of Civilian Persons in Time of War, 1949; Three Additional Protocols shortened as AP I, APII, AP III.

[3]Article 36 of Additional Protocol I obliges State Parties to review the legality of employment of any new weapon at each of the state of the study, development, acquisition and adoption. This is because the combatants are not given absolute freedom in choosing means and methods of warfare under article 22 of the 1907 Hague Regulations Respecting the Laws and Customs of War on Land, and Article 35(1) of Additional Protocol I.

instance, the attacker succeeds in penetrating the main server of a hospital, and thereby all the interconnected devices are compromised, even the pacemaker installed inside the patient's body. Through command and control software, the attacker can even break down the pacemaker's functioning, which will ultimately result in the patient's death in the absence of any backup. So one can speak volumes of the human costs of wired or cyber operations[4]. This calls for an in-depth dwelling into the potential issue that the world would probably come across in the near future as all states, from giant economies to the poor and developing nations, are enhancing their cyber capabilities.

Cyber operations do not take part in a legal vacuum as they are becoming part of modern-day armed conflicts, which demands the evolutionary interpretation of IHL. This paper focuses on some significant debates in the study of IHL in cyberwarfare. Firstly, the history of cyber-attacks is briefly discussed to tell readers about the onset of debate. Introducing cyberwarfare is followed by a brief discussion on how the network functions and types of attacks based on purposes. The very terms "attack" and "object" in the cyber context are analyzed in detail as they form the basis of every provision of LOAC. The contemporary debates as to the interpretation of these terms are included in the scope of the present study. Lastly, the attribution issue in cyberwarfare is analyzed to introduce the reader to the difficulty involved in classifying the armed conflict, which is crucial because there is a different set of rules applicable to each class of armed conflict. The study ends with the recommendation that mainly revolves around the need that states should be more expressive in their practices concerning cyber warfare as IHL is still in the budding phase. The need of the hour is that a new customary norm should emerge, but states need to put sincere efforts as in the horizontal hierarchy of sovereign states law-making power vests in states. The recent cyberattacks in the ongoing armed conflict between Russia and Ukraine by the 'patriots' once again brought the application of IHL to the limelight.

[4]For reference see ICRC Report titled "The Potential Human Cost of Cyber Operations" based on its expert meeting held in Geneva from 14-16 November 2018 explaining the comprehensible devastating consequences of cyberwarfare.

2. THE ONSET OF DEBATE ON NEXUS BETWEEN IHL CYBERWARFARE

To make the debate better understandable for the reader, the history of cyber armed conflict that diverted the attention of international humanitarian law experts is discussed. The very beginning of the twenty-first century marked the independence of Estonia from the Soviet Union, which had occupied the land since the Second World War. The Statue (bronze soldier) at the center of Tallinn, the capital of Estonia, was removed by the Tallinn residents who took the statute to be the sign of being occupied by the Soviet Union for nearly half a century (McGuinness, 2017). This enraged the ethnic Russians living in Estonia, who started social media campaigns for riots. This marked the onset of attacks from worldwide on both government and private cyberinfrastructures of Estonia. The disruption so caused halted the normal functioning of the state for some ten days. Though it was an issue of law concerning the justification for the use of force (*jus ad bellum*) and not IHL, it was for the first time the world was witnessing the attacks in a domain not discussed before. In 2008 the debate on the application of IHL to cyberwarfare started following the

Russo-Georgian war, which is regarded as "the first case in the history of a coordinated cyberspace domain attack synchronized with major combat actions in the other warfighting domains" (David, 2011). These attacks were more disruptive than destructive (Swanson, 2010). These attacks have played a huge role in making analysts and scholars think of the nexus between IHL and attacks in the cyber domain (Tikk, 2010).

There have been certain international and national efforts to develop the rules governing the armed conflicts in cyberspace. The most significant being the Tallinn Manual compiled by the twenty individuals in the international group of experts (IGE) under the auspices of the North Atlantic Treaty Organisation (NATO) and observership of the International Committee of the Red Cross (ICRC). The Manual was intended to be based on existing law (lex lata), and nowhere was it intended to be referring to an altogether new law (*lex feranda*). For this reason, the rules in the Manual stayed closer to the rules of IHL, a lex specialis for regulating the conduct of hostilities during an armed conflict. However, the sovereign states have the prerogative of making binding rules for them either by a treaty formation or by the consistent and coherent state practices out of the sense of legal obligation developing a new customary norm. Manual has only the persuasive value for the States. Some states, including France, have come up with laws specifically on the subject matter beforehand, which is a positive sign in terms of expression of state practice.

Whenever some grey area in terms of war comes under discussion, the first provision that legal minds refer to is the Martens Clause that was initially the part of the preamble of Hague Convention II of 1899 and then incorporated as a substantial part in the Geneva law[5] and the Hague law[6]. The Martens clause extends the application of international law based on coherent and consistent usages, public conscience, and humanity to complex cases. The vitality of said clause is manifested from the fact that it is restated in modern conventions and has been referred to by international courts[7] and tribunals[8], especially where they faced the instances of legal vacuum (non-liquet), and it has become part of customary international law[9]. The insertion of this clause primarily made IHL of an evolving nature capable of dealing with and adapting to the changing dynamics of warfare. IHL has undoubtedly filled in the potential legal gaps by the way it is drafted. Questions and debates as to the evolution of "interpretation" of IHL are the tasks of the states, courts, organizations tasked with disseminating IHL (primarily ICRC), and the researchers. As far as cyber warfare is concerned, the researchers and the non-state neutral entities have been positively playing their role, and now it is the states that need to step up by way of practice or by entering into an international agreement. The latter does not seem to be a viable solution as states do not seem to be willing to be vocal about the restrictions on their cyber capabilities, which is improving over time) (Turns, 2012).

[5]Article 63 para 4 of GC I; Article 62 para 4 of GC II; Article 142 para 3 of GC III; Article 158 para 4 of GC IV; Article 1 (2) of AP I Preamble of AP II.

[6]Preamble of the 1907 Hague Convention (IV).

[7]For example, ICJ, Case Concerning Military and Paramilitary Activities In and Against Nicaragua (Nicaragua v USA) Merit Judgment of 1986, para. 218.

[8]For example, ICTY, The Prosecutor v. Kupreškić et al [Judgment] 2000, paras. 525-6.

[9]ICJ, Legality of the Threat or Use of Nuclear Weapons [Advisory Opinion] 1996 para. 84.

3. THE FAULT LINES IN THE APPLICATION OF IHL TO CYBERWARFARE

3.1 Interpretation of the term attack in a cyber context

In the technical sense, cyber warfare refers to the weaponized use of digital tools employed for the system-to-system attack via a data stream. The cyber operations based on purpose can be classified into Computer Network Exploitation (CNE) and Computer Network Attack (CNA) (Beck, 2002). The former refers to data theft without the intent of damaging the functionality of the system compromised (access operations). The latter aims to generate targeted effects on the system, including data tampering by deleting or altering, disabling the function, or physical damage to the system (effect operations).

For a cyber operation to constitute a cyberattack for triggering the application of IHL, the determining factor is the reasonable expectation of death or injury to persons or destruction or damage to objects, notwithstanding whether such an operation was offensive or defensive[10]. The term attack at this point needs to be analyzed since it forms the basis of several general principles and special prohibitions in terms of the IHL. The prohibitions against indiscriminate attacks, attacks against civilians, attacks against civilian objects, an attack against medical personnel, attacks against the natural environment, attacks against dangerous forces, and so on beg the question of what is meant by "attack" in a cyber context. Article 49 (1) of Additional Protocol I defines attack in the following terms:

> "... acts of violence against the adversary, whether in offense or defense."

So violence is the indicative factor for classifying which military operations could be called attacks irrespective of the domain in which such an attack is carried out. For this reason, psychological cyber operations do not fall within the meaning of attack for want of violence[11]. Now, these violent attacks should not be restrictively interpreted to mean only those violent acts that release kinetic forces. IHL has a consequential-based approach since every principle is centered on the central theme of protecting civilians from the "effects" of conflict to the possible extent. So it is the violent consequences, not the nature of acts, that determines the scope of the attack[12]. For instance, conventionally destroying the electric grid system supplying electricity to the whole city is equivalent in terms of consequences to the use of cyber operations for causing such destruction. Thus such cyber operation qualifies as an attack. As a matter of law, it has been agreed universally that biological and chemical attacks are in legal sense attacks despite no kinetic release and was discouraged in its employment as a means of warfare even before the specific convention was entered into[13]. Thus one can by analogy extend this principle to cyber warfare.

There is support from several provisions of Additional Protocol I and the customary rules to interpret the term violence. It is agreed among the majority of experts that

[10] Rule 30 of Tallinn Manual on the International Law Applicable to Cyberspace.

[11] German Manual, para 474.

[12] In other words IHL is not worried about acts that are violent or involve the transfer of kinetic force what IHL cares about are the consequences.

[13] *In Prosecutor v Dusko Tadic* (Decision on the Defence Motion for Interlocutory Appeal, 1995) paras 120-124 the ICTY decided against the use of chemical weapons in either forms of armed conflict. Analogically the same is true for the cyberattacks.

the violence must not be de minis which will not qualify the operation as an attack. The indicative factors include the excessive death, destruction, or combination thereof, damage to the environment that is severe, widespread, and long-term[14], severe losses arising from the destruction of critical infrastructure[15]. It is pertinent to mention here that the law forbids those attacks that can "foreseeably cause" the required extent of harm. So though the cyberattack might not have caused the required harm to the system directly targeted yet, such an attack has the potential of causing more significant harm to the person or objects, which would be prohibited had the attack been that of a conventional nature. So it will be absolute absurdity and irrationality if one arrives at a different conclusion merely because the warfare is conducted in a cyber domain. So, till here, what constitutes cyber operation has been discussed, which will be used in defining the term cyber warfare.

In its study on the limitations imposed by IHL on the cyberattacks, ICRC defined cyber warfare in the following terms:

> "[Cyberwarfare refers to] 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 (ICRC, 2013)."

The above definition gives two possibilities. Firstly, if it meets the criteria of armed conflict, a cyber operation in itself can be cyber warfare. Secondly, if conducted in furtherance of an armed conflict, the cyber operation can be termed as cyberwarfare.

Moreover, not all the conflicts or attacks come within the purview of IHL but only the 'armed conflicts. The terms "resort to armed force" and "armed conflict" is not expressly defined in the treaty IHL (Droege, 2012), so the resort has to be made to *jurisprudence* to discover the true meaning and apply it in the cyber context. Here is a trichotomy of approaches as to the cyber operation amounting to an armed attack and thereby triggering the application of IHL. These are the permissive approach, the restrictive approach, and the functional approach. The underlying idea of the permissive approach is that the cyber operations not causing the actual physical destruction are deemed permissible. This is an over-exclusive interpretation that, if applied to the potential situations, will defeat the very purpose and spirit of IHL. This approach opens gates for the mysteries that will not be resolved had the law been strictly interpreted even when the surrounding circumstances in which it is to be applied are evolving. The restrictive approach is based on the principle of distinction that the military objectives could only be targeted, and any attack against a civilian object is unlawful. But in the cyber domain, does this principle implies that all the operations against civilians are unlawful? Which will be analyzed later. The approach adopted by the majority in the Tallinn manual is called the *functionality* approach, whereby damage includes an operation that, albeit not physically damaging or destructive, affects the functionality of the cyberinfrastructure against which it is directed. The determining factor here is whether the infrastructure attacked is prevented from performing its intended function. If yes, then civilian objects will enjoy the protection of IHL against the damage arising therefrom. Though this seems to be a sensible approach, the dispute arises whether the functioning shall be permanently disrupted to call such an operation an attack or even the temporary disruption would cause the operation to fall within the meaning of attack under IHL.

[14] Article 35 (3) of AP I. The environment is also specifically protected under article 55 of AP I.

[15] Article 56 (1) of AP I.

The disabling of the object in a cyber operation (the functionality approach) finds support in Article 52 of AP I when it talks about the “neutralization" of objects. If one adopts the functionality approach, the only cyber incident that would fulfill an attack requirement was the “Operation Olympic Games.” The nuclear enrichment facilities were targeted, especially the centrifugal apparatus installed for the purification of Uranium in the nuclear facility of Natanz, Iran. Cyber analysts named the bug developed by the coalition of the U.S. and Israel as Stuxnet. From 1000 to 5000 centrifuge machines broke down, and it was programmed to remain unnoticed even by the cyber security measures taken in the Natanz nuclear facility. So this cyber operation affected the functionality of the devices targeted, and thus this fulfills the functionality approach of attack. ICRC views the disability of an object as the sole criterion for defining the term attack irrespective of whether it is brought by cyber means or kinetic means, and the writer also thinks it to be the most suitable approach in pragmatic terms (ICRC, 2013). The way the attacks should be interpreted and how such an approach could be refined depends on the relevant State practices.

3.2 Interpreting the term object in cyber context: Is data an object or not?

Another important area of dispute amongst legal experts is whether data can be called an object for attack? Since the very thing against which a cyber attack is conducted is data. If it is called an object and a civilian object, then it will enjoy the protection afforded by IHL to civilian objects, and hacking would be a war crime. Even in the commentary of the Tallinn Manual, it is expressed that the views of the IGE were divided. The majority view was that data could not be interpreted as an object. They based their view on the ICRC’s commentary on article 52 of Additional Protocol I, which states that an object is something that is “visible" and "tangible." Since data is virtual thus, it does not come within the ordinary meaning of the term object.

Furthermore, they argued that no expressed state practice suggests that data is protected as an object. This interpretation implies that "any" cyber operation against civilian data will not be an attack against a civilian object if the functionality of the infrastructure attacked remains intact. Minorities believe that data is an object and that any cyber operation against civilian data is an attack on a civilian object and is thus prohibited by IHL. They argue that the interpretation should be influenced by the surrounding and evolving circumstances. The expert calls the former interpretation to be under-inclusive and the latter interpretation to be over-inclusive. Here the reference to the balancing approach adopted by IHL is relevant. IHL is a body of law that seeks to balance military necessity and humanitarian consideration. Those who interpret data as not an object overemphasize the military necessity. At the same time, the other group interpreting data as an object overemphasizes the humanitarian considerations. So in the true spirit and purposes of IHL, both these views are not correct. Again States have the authority of interpreting it, and the States would be more inclined towards interpreting data as not an object because they will want to attack the data during counterinsurgencies to deprive the military of the support of the civilian population. Still, data is to be protected based on the functionality test that the data cannot be manipulated where it will affect the intended use of the infrastructure containing such data.

ICRC’s position on this issue is that the data that enjoy special protection under IHL

have a comprehensive normative framework (ICRC, 2015). For instance, medical data is protected because it is "medical" data, not because it is an object, and IHL provides special protection to the purpose such data serves. This is especially relevant in the current backdrop of the pandemic situation. The same is valid for protecting the humanitarian assistance data not because it is an object but because of its function, which enjoys special protection in IHL. The concern is about that data which is essentially civilian data but does not enjoy special protection under IHL. The general rules regulating the conduct of hostilities cover the protection of such data like tax records, bank accounts, company data, and election records. If such data is tampered with or deleted, it can halt the functioning of governmental organizations and private businesses. It might have the potential of causing harm to civilians greater than that resulting from the destruction of physical objects. Reconciliation with the underlying purpose (*raison detre*) of IHL is impossible if one concludes that in today's cyber-reliant world, the operation against civilian data is not an attack against a civilian 'object' (ICRC, 2016).

3.3 Difficulty of Attribution in Cyber Context: Classification of Armed Conflict in Cyberspace

Suppose a person within the territory of Japan, at the request of the U.S. government, compromised the functionality of all the electricity grid stations in Iran, which is engaged in an armed conflict with France, a staunch ally of the U.S. This resulted in a complete electricity blackout in Iran for seven hours which halted the smooth functioning of all the sectors of the country with special reference to health care facilities and critical civilian infrastructure. The attacker is amongst the top cyber experts in the world, and thus, the attack is likely to have been conducted without leaving behind any clue as to the true origin of the attack. This illustration manifests, amongst others, one of the biggest concerns for IHL application to the armed conflicts in the cyber domain, i.e., the issue of attribution (i.e., identifying the source of the attack and "who did it? Rather more precisely "who is to blame") for three main reasons. Firstly, in an ongoing armed conflict, IHL regulates only those cyber operations which have a causal link with the ongoing armed conflict. Establishing that link and determining whether it was conducted in furtherance of an armed conflict attribution is indispensable. Secondly, IHL has a distinct set of rules applicable to International Armed Conflicts (IACs), when two or more states resort to the use of force and Non-International Armed Conflicts (NIACs) essentially involve at least one non-state organized armed group. The concepts of foreign intervention and NIAC spillover are linked to it, which the state practices and judicial decisions have settled down. Until the attacker is not identified, the lack of attribution would make the classification of armed conflict impossible, and in turn, the applicable law would be doubtful. Thirdly, the accountability for the attack is based on attribution and identification of the attacker.

Two famous tests govern the attribution based on state control: the effective control test and the overall control test. The former test propounded by ICJ in the Nicaragua case [16] considers a state responsible for the acts of non-state actors only when each of the acts during the conflict were carried out in furtherance of State-specific instructions. This legal regime was applied to the 2008 Russo-Georgian War, where the threshold of

[16]ICJ, *Case Concerning Military and Paramilitary Activities In and Against Nicaragua* (Nicaragua v USA) Merit Judgment of 1986.

effective control of Russia over alleged perpetrators was not met. The digital forensic evidence substantiated the coordination of cyber-attacks with the ongoing armed conflict in a physical domain which convincingly indicated the involvement of the Kremlin (Russian government). However, Russia called the attacker Russian patriots on whom the government lacked overall control. This leads to the claim that the "attribution fixation of the effective control test is a de facto license for impunity in the cybersphere" (Healey, 2012).

Hence owing to the difficulty in standards of proof, the much-celebrated test in judicial decisions is the less stringent overall control test laid down by ICTY[17]. In the given backdrop of limitations of cyber attribution, the overall control test is more compatible as it entails the responsibility onto the states having a role in organizing, planning, and coordinating the non-state groups besides mere financial and logistical support[18]. If this test were applied to the Russo-Georgian war, there would have been a *prima facie* case of Russian responsibility as the available strategic and forensic evidence pointed towards the Russian influence over the "cyber patriots" (Assumpcao, 2020).

These attributions are irrespective of the domain in which they are carried out. However, identifying the perpetrator of the attack is essential for determining the issue of state attribution (referring to the example of the Iranian attack given at the start of the discussion) and determining whether the conflict is IAC or NIAC. Cyber warfare's ease in denial of responsibility is likely to appeal to states in using it for attacking purposes in the future. At times in this paper, the rules applicable to biological, nuclear, and chemical warfare (which are also the new means and methods of warfare) have been by way of analogy extended to warfare in the cyber domain. Nevertheless, biological and chemical warfare attribution is not an issue since the state exercises monopoly and control over its nuclear and chemical facilities. The cyber domain bestows upon attackers the possibility of hiding their identities and carrying out attacks without the fear of being identified by defenders. Even the attacker can program the malware in such a way as to falsify his identity and to shift responsibility, in the event defender can locate the attacker, onto someone who was not even aware of it (false attribution). So anonymity issue is yet to be resolved, and such a breakthrough is not likely to happen in the near future (Jastram, 2011). Currently, threefold assumptions dominate the virtual or cyber attribution issue (Rid, 2015). The first assumption is the least optimistic one and thinks internet redesign to be the only way out for the most intractable issue (Singer, 2014) of cyber attribution (McConnell, 2020). Most of the legal debate is posited on this assumption (Waxman, 2011) (Tsagourias, 2013) (Roscini, 2014). The second assumption is an intermediary approach and views that depending on the case, the issue of attribution could be solved by discovering the culprit, or it remains unsolved and leads merely to obfuscated log files, spoofed I.P. addresses, or any other dead trail (Healey, 2013). The third assumption is highly optimistic because the attributive evidence is readily comprehensible, and the only obstacle is finding out the evidence for which proponents have presented models[19]. The determinative factors in practical terms include

[17]ICTY, *The Prosecutor v. Dusko Tadic*, IT-94-1-AR 72 [Appeals Chamber Decision, October 2, 1995].

[18]*Prosecutor v Lubanga* (Decision on Confirmation of Charges) ICC-01/04-01/06 [January 29, 2007], para 211; *Case Concerning the Application of the Convention on the Prevention and Punishment of the Crime of Genocide* (Bosnia and Herzegovina v Serbia and Montenegro) ICJ Rep 43 [2007]: para 404.

[19]The famous two models are the Diamond Model of Intrusion Analysis by Sergio Caltagirone, Andrew Pendergast and Christopher Betz and The Kill Chain

findings of digital forensics (technical investigation) and strategic investigation based on intelligence information, history, and the knowledge of possible attackers on assessment of incentive involved (cost-benefit analysis) (Lin, 2012). This could help in tracing the attacker for taking further action.

The non-international armed conflict (NIAC) is "protracted armed violence between governmental authorities and organized armed groups or between such groups within a State."[20] The two requisites, keeping in view the definition provided in common article 3 to all G.C.'s and article 1 of AP II, for a conflict to be NIAC are organized armed groups and required level of intensity. The threshold for a NIAC is higher than for IAC as the mere riots or sporadic acts of violence are excluded from the scope of NIAC. In *Prosecutor v Limaj* the ICTY adopted a lenient approach and deemed the presence of 'some' level of organization sufficient for proving the first requisite[21]. This requirement requires a case-by-case analysis, but some of the indicative factors ICTY looked into in the Limaj case were: formal hierarchy, order from the superior, the establishment of headquarters, disciplinary rules, and recruits. Thus, those cyber-attacks conducted by an individual *sua sponte* are not an armed conflict of either category. Another implication is that merely the occurrences of cyber-attacks in parallel may be called collective but are not organized (such as Estonian attacks). There is a possibility that the individuals tasked with specific responsibilities like looking for vulnerabilities, programing and designing malware, launching it, and taking defenses against counter-attacks arrange in hierarchically organized form with one assuming the virtual responsible command.

Moreover, it is acknowledged that such an organization is not necessarily required to be as sophisticated as is in regular armed forces; nevertheless, there should be some organization[22]. The lack of interaction in the physical world cast doubts about the organization of the cyber armed group. This also raises the problem of maintaining discipline as the command control, if any, is merely online. Moreover, the AP II has put in place an additional requirement of the ability to comply with the rules of IHL, which though is not the requirement under common article 3 to all four Geneva Conventions yet it is considered as a 'convenient criteria'[23] and was applied by ICTY[24] in classifying the conflict. If compliance is necessary for classifying the conflict as a NIAC, then possibly all virtual attacks/ operations will be outside the definition of NIAC for want of effective means for ensuring compliance[25].

The second criteria for a NIAC to be the protracted armed conflict lack any bright-line test, yet certain factors support in determin-

Analysis by Eric M. Hutchins, Michael J. Cloppert and Rohan M. Amin.

[20] *Tadic case, para 70; Prosecutor v Akayesu* (Judgment) ICTR-96-4-T (September 2, 1998) para 619; *Prosecutor v Bemba Gombo* (Decision on Confirmation of Charges) ICC-01/05-01/08 (June 15, 2006) para 229. Similar definition is adopted in article 8 (2) (f) of the Statute of International Criminal Court [the Rome Statute] of 2002.

[21] *Prosecutor v Limaj* (Judgment) ICTY-03-66-T (November 30, 2005) para 89.

[22] ICRC Commentary on Additional Protocol III, para 4663

[23] ICRC, *Commentary: I Geneva Convention for the Amelioration of the Condition of the Wounded and Sick in the Armed Forces in the Field* (J Pictet (ed.) 1952) 49.

[24] *Prosecutor v Boskoski* (Judgment) ICTY-04-82-T (July 10, 2008) para 205.

[25] In *Prosecutor v Hadzihazanovic* (Appeals Chamber Decision on Interlocutory Appeal Challenging Jurisdiction in Relation to Command Responsibility) ICTY-01-47-AR72 (July 16, 2003) paras 16–22 the relation between responsible command and command responsibility was discussed and it was held that where the members of group lacked responsible command then attributing their acts to an individual will be illogical.

ing it, like the intensity of the armed conflict to distinguish it from mere internal disturbances. The high threshold might exclude several cyber operations from the definition of NIAC.

States are yet to classify the cyber conflicts, not in furtherance of an ongoing armed conflict. However, it will undoubtedly pose serious complex issues in the future. The writer can see the customary norm evolving in the near future as the dependency on cyberinfrastructure increases with time and the states have been developing more disruptive cyber-attack tools. States, therefore, will act in a particular way out of the sense of legal obligation (*opinio juris*) to tackle the legal problems incidental to such attacks. IHL in the cyber context is in the budding phase and will develop with time.

4. CONCLUSION

"*If the new and frightful weapons of destruction which are now at the disposal of the nations seem destined to abridge the duration of future wars, it appears likely, on the other hand, that future battles will only become more and more murderous.*"
Henry Dunant, A Memory of Solferino, 1862

The present study attempted to highlight the basic debates fundamental to IHL in cyber warfare. This is a vast topic, but the scope was limited to the discussions on the interpretation of general terms. The paper has clarified that these debates will continue until some viable solution is adopted. The dilemma is that the IHL developed in the times of conventional warfare when the cyber-attack was but fiction. The only way out is either a new convention specifically devoted to cyber-armed conflicts or the consistent state practices out of a sense of legal obligation that will develop binding customs on the subject matter. Even though states are reluctant in making a norm or entering into treaty relations, potentially curtailing their use of cyber weapons, Tallinn Manual is a hope for the future of IHL in cyberwarfare.

Moreover, states will indulge more and more in devastating cyber conflicts (as is the case with autonomous weapons) as they are involved in the cyber arms race. This will probably lead to the emergence of a new norm, but that emergence is nowhere in the immediate future (maybe it would take decades). The attacking states will be more likely to interpret the provisions of the existing law of armed conflict to act as a scapegoat from any responsibility. For instance, interpreting data not as an object as they are and will like to continue attacks against civilian data. Unlike the convention on chemical and biological weapons, cyber weapon treaties, though best serves the problem, should be forgotten in the given backdrop of enhanced military reliance. The need for treaty-making for a new form of warfare was felt in the aftermath of World War II (the new domain at that time was airspace), in the words of J. M. Spaight: "It now remains to show why it is better to proceed by creating a new and special code . . . rather than by building upon and adding to the rules already governing land warfare" (Spaight, 1924). The author guesses that once the state practice has fully developed, only then would the treaty-making be possible, which will be nothing but the expression of those norms developed. However, before any such development, the rules of IHL should continue to govern the cyberwarfare and be interpreted in the light of the values on which IHL is premised.

REFERENCES

Kathleen. (2006). A Guide to the Legal Review of New Weapons, Means and Methods of Warfare. Geneva, Switzerland: International Committee of the Red Cross.

Gisel, Laurent, Rodenhauser, Tilman, Dormann, Knut. (2020). Twenty years on International humanitarian law and the protection of civilians against the effects of cyber operations during armed conflicts. International Review of the Red Cross 102(913), 289.

Dinniss, H. H. (2008). The Status and Use of Computer Network Attacks in International Humanitarian Law. (Doctoral Dissertation). Retrieved from https://etheses.lse.ac.uk/2527/1/U615476.pdf.

McGuinness, Damien. (2017). How a cyber attack transformed Estonia. Retrieved on May 20, 2021 from https://www.bbc.com/news/39655415.

David, Hollis. (2011). Cyberwar Case Study: Georgia 2008. Small Wars Journals, 2.

Swanson, Lesley. (2010). The Era of Cyber Warfare: Applying International Humanitarian Law to the 2008 Russian-Georgian Cyber Conflict. Loy. L.A. Int'l Comp. L. Rev. 32(2), 303.

Tikk, E., Kaska, K., Vihul, L. (2010). International Cyber Incidents: Legal Considerations. Tallinn, Estonia: Cooperative Cyber Defence Centre of Excellence.

Turns, David. (2012). Cyber Warfare and the Notion of Direct Participation in Hostilities. Journal of Conflict and Security Law 17(2), 296.

Beck, L. Doswald. (2002). Some Thoughts on Computer Network Attack and the International Law of Armed Conflict. International Law Studies 76.

International Committee of the Red Cross. (2013). What Limits Does Law of War Impose on Cyber Attacks? Retrieved on May 24, 2021 from https://www.icrc.org/en/doc/resources/documents/faq/130628-cyber-warfare-q-and-a-eng.htm.

Droege, Cordula. (2012). Get Off My Cloud: Cyber Warfare, International Humanitarian Law, and the Protection of Civilians. International Review of Red Cross 94(886), 543.

International Committee of the Red Cross. (2013). Cyber warfare and international humanitarian law: The ICRC's position. Retrieved on May 27, 2021 from https://www.icrc.org/en/doc/assets/files/2013/130621-cyber-warfare-q-and-a-eng.pdf.

International Committee of the Red Cross. (2015). International humanitarian law and the challenges of contemporary armed conflicts. (Report EN 32IC/15/11), 44. Retrieved on May 27, 2021 from file:///D:/32ic-report-on-ihl-and-challenges-of-armed-conflicts.pdf.

International Committee of the Red Cross. (2016). International Humanitarian Law and the Challenges of Contemporary Armed Conflicts. International Review of the Red Cross 97, 1427-8.

Healey, Jason. (2012). Beyond Attribution: Seeking National Responsibility for Cyber Attacks. Washington, Atlantic Council, Issue Brief. Retrieved on May 29, 2021 from https://www.atlanticcouncil.org/in-depth-research-reports/issue-brief/beyond-attribution-seeking-national-responsibility-in-cyberspace/.

Assumpcao, Clara. (2020). The Problem of Cyber Attribution Between States.

Retrieved on June 2, 2021 from https://www.e-ir.info/pdf/83271.

Rid, Thomas, Buchanan, Ben. (2015). Attributing Cyber Attacks. Journal of Strategic Studies 38(1), 5-6.

Jastram, Kate, Quintin, Anne. (2011). The Internet in Bello: Cyber War Law, Ethics Policy. Seminar Summary Report, 10. Retrieved on June 2, 2021 from https://www.law.berkeley.edu/wp-content/uploads/2015/04/cyberwarfare-seminar-summary-complete.pdf.

Singer, P. W., Friedman, Allan. (2014). Cyber Security and Cyberwarfare. Oxford, U.K.: Oxford University Press, 73.

McConnell, Mike. (2020). How to Win the Cyberwar We're Losing. Retrieved on June 5, 2021 from https://www.washingtonpost.com/wp-dyn/content/article/2010/02/25/AR2010022502493_pf.html.

Tsagourias, Nicholas. (2013). Cyber Attacks, Self Defence and the Problem of Attribution. Journal of Conflict and Security Law 17, 229-44.

Waxman, Mathew C. (2011). Cyber-Attacks and the Use of Force. Yale Journal of International Law 36, 421-59.

Roscini, Macro. (2014). Cyber Operations and The Use of Force in International Law. Oxford, U.K.: Oxford University Press, 33-40.

Healey, Jason. (2013). A Fierce Domain: Conflict in Cyberspace, 1986 to 2012. Cyber Conflict Studies Association, 265.

Lin, Herbert. (2012). Cyber Conflict and International Humanitarian Law. International Review of the Red Cross 94(886), 515, 522.

Spaight, J.M. (1924). Air Power and War Rights. London, UK: Longmans Green Co., 31.

