JIMMA UNIVERSITY

COLLEGE OF LAW AND GOVERNANCE

SCHOOL OF LAW

THE APPLICATION OF INTERNATIONAL HUMANITARIAN LAW TO CYBER WARFARE: CRITICAL ANALYSIS

BY: YIHEYIS K/MARIYAM

June 2018

THE APPLICATION OF INTERNATIONAL HUMANITARIAN LAW TO CYBER WARFARE: CRITICAL ANALYSIS

BY: Yiheyis K/Mariyam

Advisor

Nega Ewunetie (Asst. Professor)

Co-advisor

Kassaye Muluneh (LLB, LLM)

A Thesis Submitted in Partial Fulfillment of the Requirements for the Masters of Law (LL.M) in Human Rights and Criminal Law

DECLARATION

I, Yiheyis K/mariyam, hereby declare that this research paper is original and has never been presented in any other institution. To the best of my knowledge and belief, I also declare that all referred materials are duly acknowledged.

Name: Yiheyis K/mariyam

Signature:

This thesis has been submitted for examination with my approval as University advisor.

Advisor: Nega Ewunetie (Asst. Professor)

Signature:

Acknowledgments

I would like to express my deepest and sincere gratitude to my thesis advisor Mr. Nega Ewunetie for his unreserved and persistent advice throughout the work of this paper. Had it not been for his constructive and insightful comments, the realization of this work would have been very difficult.

I must also express my very profound gratitude to my families and friends for providing me with unfailing support and continuous encouragement throughout my years of study and through the process of writing this paper. This accomplishment would not have been possible without them. Thank you.

Acronyms

AP I	Additional Protocol I
AP II	Additional Protocol II
CNA	Computer Network Attack
CND	Computer Network Defense
CNE	Computer Network Exploitation
IAC	International Armed Conflict
ICJ	International Court of Justice
ICRC	International Committee of Red Cross
ICTY	International Criminal Tribunal for the former Yugoslavia
IHL	International Humanitarian Law
NIAC	Non-International Armed Conflict

Contents

Abstract

Contemporarily it is axiomatic that individuals, organizations and states rely on the cyber space and its tools for their everyday activities ranging from sending an email to controlling critical system and infrastructure. Alongside such extensive utilization there arises a great risk that such systems and infrastructures may became the target of malicious cyber-attacks by the adversary during armed conflict. This raises a question whether and, if so, how the existing rules of IHL apply to cyber warfare cases. In this respect there is a general consensus that cyber-attacks that amount to or carried out in the context of an armed conflict are subjected to the existing rules and principles of IHL. The controversy lies on how to transpose the existing rules of IHL to a warfare conducted in cyberspace through cyber means and methods, if they are meant to achieve the objective of protecting victims of armed conflict. By following a consequence based interpretation of armed conflict and attack this paper argues that for the most part the existing rules of IHL seems to provide sufficient protection to victims of armed conflict. However, given the unique features of the cyber space there are some problems that require the evolvement of the existing rules of IHL.

CHAPTER ONE
Introduction

1.1.Background of the Research

International Humanitarian Law (IHL), which is sometimes referred to as *jus in bello* or the law of armed conflict, is a branch of public international law which "seeks to moderate the conduct of armed conflict and to mitigate the suffering which it causes."[1] The Four Geneva Conventions[2] and their two Additional Protocols[3], the Regulations annexed to the Fourth Hague Convention[4] and several treaties prohibiting or restricting the use of certain weapons[5] currently constitute the main part of this branch of public international law.[6] These treaties, with the aim of limiting the effect of armed conflict, provide protection to victims of armed conflict and restrict the means and method of warfare.[7]

But the flexibility of these laws to accommodate changes has been challenged with the development of new technologies which have altered the nature of warfare.[8] Among such technological advancement the invention and proliferation of the cyber space, which has changed not only the means and method of warfare but also the battle itself, has posed a serious challenge to the existing rules of IHL.[9]

---

[1] Hilaire Mccoubrey, *International Humanitarian Law: Modern Developments in the Limitation of Warfare* (2nd ed. 1998) 1

[2] Geneva Convention for the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field (1949) 75 U.N.T.S. 31 (GC. I); Geneva Convention for the Amelioration of the Condition of Wounded, Sick and Shipwrecked Members of Armed Forces at Sea (1949) 75 U.N.T.S. 85 (GC. II); Geneva Convention relative to the Treatment of Prisoners of War (1949) 75 U.N.T.S. 135 (GC. III); Geneva Convention relative to the Protection of Civilian Persons in Time of War (1949) 75 U.N.T.S. 287 (GC. IV)

[3] Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflict (1977) 1125 U.N.T.S. 7 (Protocol I); Protocol Additional to The Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of Non-International Armed Conflicts (1977) 1125 U.N.T.S. 609 (Protocol II)

[4]Regulations concerning the Laws and Customs of War on Land, annexed to Hague Convention [No. IV] Respecting the Laws and Customs of War on Land, (1907)

[5] This includes among other things: Convention on the Prohibition of Development, Production and Stockpiling of Bacteriological and Toxin weapons and their Destruction (1972); Convention on Prohibitions or Restrictions on the Use of Certain Conventional Weapons which may be deemed to be excessively injurious or to have indiscriminate effects (1980); Convention on the prohibition of the development, production, stockpiling and use of chemical weapons and on their destruction (1993); Convention on the prohibition of the use, stockpiling, production and transfer of anti-personnel mines and on their destruction (1997)

[6] Nils Melzer (n 6) 21

[7] Dan-Iulian Voitaşec, 'Applying International Humanitarian Law to Cyberattacks' (2015) CKSPL 552

[8] For a detailed analysis of IHL and technology see Michael N. Schmitt, 'War, Technology and the Law of Armed Conflict' (2016) 82 ILS

[9] See Michael N. Schmitt, 'The Law of Cyber Warfare: Quo Vadis' 25 Stan. L. & Pol'y Rev. 269 (2014)

As a result of unprecedented advancement and proliferation of information communication technologies, the world has witnessed increased reliance on cyberspace[10]since the end of the 20th century. As such, contemporarily individuals, organizations, and states utilize the cyberspace and its tools for their everyday activities ranging from sending an email, to controlling critical systems and infrastructures such as power plants, nuclear plants, dams, water treatment and distribution systems, oil refineries, gas and oil pipelines, banking systems, hospital systems, railroads, and air traffic control system.[11]

Alongside such extensive utilization, there is a concern in knowing that the cyberspace is susceptible to infiltration and manipulation through cyber-attacks.[12] Cyber-attacks are:

> *computer operations, which involve the development and dispatch of computer code from one or more computers to target computers or computer systems, that aims at infiltrating a computer system either to collect, export, destroy, change, or encrypt data, or to trigger, alter, or otherwise manipulate processes controlled by the infiltrated system.*[13]

Even though such attacks are conducted in a virtual world they have a potential to cause serious human suffering in a physical world. For instance, a cyber-attack directed against computer systems controlling the operation of critical infrastructures could potentially result in catastrophic consequences such as collisions between aircraft, the release of radiation from nuclear plants, the release of toxic chemicals from chemical plants, or the disruption of vital infrastructure and services such as electricity or water.[14] Thus in the contemporary world where almost anything is

[10] US Joint Chiefs of Staff, 'Department of Defense Dictionary of Military and Associated Terms' (2001), p. 41: defines cyberspace as: "global domain within the information environment consisting of the interdependent network of information technology infrastructures, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers"

[11] Cordula Droege, 'Get off my cloud: cyber warfare, international humanitarian law, and the protection of Civilians' (2012) 94 IRRC 538

[12] Sandra Song, The Laws of War: Do they Apply in Cyberspace? (2013) http://natoassociation.ca/the-laws-of-war-do-they-apply-in-cyberspace/ (Accessed November 7, 2018); The term cyber-attack in this sentence is only used in its descriptive sense, not as an attack provided under Art.49 of AP-I

[13] Eitan Diamond, 'Applying International Humanitarian Law to Cyber Warfare' (2014) INSS 67

[14] Cordula Droege (n 11) 539; A. Hathaway, R. Crootof et al., 'The law of cyber-attack' (2012) CLRV 7: by citing different literature the authors stated that cyber-attack scenarios ranges "from a virus that scrambles financial records or incapacitates the stock market, to a false message that causes a nuclear reactor to shut off or a dam to open, to a blackout of the air traffic control system that results in airplane crashes."

attached to the cyber space, cyber-attack appears as a favorable tool to utilize especially during armed conflict.[15]

Cognizant of such risk of vulnerability and its potential effects on the civilian population, states are now building a technological capacity not only to defend their critical infrastructures from cyber-attack but also to be able to launch cyber operations against their adversaries during armed conflict.[16] This has made the cyberspace a new, artificial and the fifth domain of warfare in addition to traditionally recognized domains of land, sea, air and outer space.[17]

Such development raises the question whether and, if so, how the existing rules of IHL apply to cyber warfare i.e. cyber-attacks that amount to or carried out in the context of an armed conflict. In such respect, although there is no cyber-specific provision under the existing rules of IHL it doesn't mean that cyber warfare operates in a void normative framework. A considerable amount of literature has recognized the applicability of rules of IHL to cyber operations that amount to or carried out in the context of armed conflict.[18]

This conclusion is, among other things, supported by the Martens clause which provides that in cases not covered by international agreement "civilians and combatants remain under the protection and authority of the principles of international law derived from established custom, from the principles of humanity and from the dictates of public conscience."[19] Thus all activities occurring in the armed conflict are subject to humanitarian law principles. Furthermore, the obligation imposed by Article 36 of AP I[20] which require review of newly developed weapons, means and method of warfare in light of IHL rules shows that the rules of IHL are meant to be

[15] Ibid

[16] *See* for example Scott Shane, 'Cyberwarfare emerges from shadows of public discussion by US officials' (2012) http://www.nytimes.com/2012/09/27/us/us-officials-opening-up-on-cyberwarfare.html (Accessed January 12, 2018)

[17] Nils Melzer (n 6) 3

[18] See for e.g. Knut Dörmann, 'Applicability of the Additional Protocols to Computer Network Attack' (2004) Dinstein, Yoram, 'The Principle of Distinction and Cyber War in International Armed Conflicts'(2012) Journal of Conflict and Security Law; Cordula, 'Get off my cloud: Cyber warfare, international humanitarian law, and the protection of civilians' (2012) IRRC; Michael N. Schmitt, 'Rewired warfare: Rethinking the law of cyber-attack', (2014) IRRC; Iben Yde, 'The Law of Cyber Armed Conflicts: Translating Existing Norms of International Humanitarian Law into Cyber Language' (2013)

[19]Hague Convention IV Respecting the Laws and Customs of War on Land, Oct. 18,1907, pmbl. And Protocol Additional (I) to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflicts, art. 1(2), Dec. 12, 1977, 1125 U.N.T.S. 3

[20]The provision provides that "in the study, development, acquisition or adoption of a new weapon, means or method of warfare, a High Contracting Party is under an obligation to determine whether its employment would, in some or all circumstances, be prohibited by this Protocol or by any other rule of international law applicable to the High Contracting Party."

applicable to subsequent warfare technologies. This has also been affirmed by the International Court of Justice (ICJ), in its Nuclear Weapons Advisory Opinion which held that "Established principles and rules of humanitarian law applicable in armed conflicts…applies to all forms of warfare and to all kinds of weapons, those of the past, those of the present and those of the future."[21]

Accordingly, if cyber operations amount to or carried out in the context of armed conflict they will be governed by the rules and principles of IHL. Once this hurdle has been passed there comes the issue of how to apply the fundamental rules and principles of IHL to cyberwarfare. This may appear as a simply task of transposing the rules of IHL to a new means and method of warfare. However, the unique nature of cyberwarfare, which will be explained in the statement of the problem part, have made adapting the existing rules of IHL to cyberwarfare a difficult endeavor. This research, therefore, seeks to critically analyze the effect of regulating cyberwarfare with the existing rules and principles of IHL.

1.2.Statement of the problem

Although there is a prima facie case for the application of IHL to cyberwarfare cases adapting the existing rules that are designed to apply to the means and method of warfare involving the use of kinetic force in the physical world, to cyberwarfare is not an easy task. The unique features of cyberwarfare have made rules of IHL difficult to be applied with their full effect as they apply to the traditional means and method of warfare.

Among other things, the anonymous nature of cyber operation has made attribution, the central element in determining the existence of armed conflict, a daunting task. The whole structure of the existing IHL rules is premised on the assumption that the parties to the armed conflict are known and identifiable.[22] However, in cyber operation, it is usually impossible to trace their originator.[23] In such instances the very application of IHL to the operation becomes questionable.

Furthermore, in contrast to conventional hostilities which involve the use of kinetic force many cyber operations produce a non-violent effect. As such cyber operations rather than physically

[21] ICJ, Legality of the Threat or Use of Nuclear Weapons, Advisory Opinion, (1995) para. 86
[22] Cordula Droege (n 11) 541; In conventional hostilities, the deployment of troops and artilleries makes it easy to identify the parties in the conflict
[23] Ibid

destroying or damaging the targeted system, they could simply hamper its functioning.[24] In elaborating this point Cordula Droege notes that "[…] an electrical grid might be left untouched physically but nonetheless be put out of commission by a computer network attack. Similarly, a country's banking system might be manipulated without any of the infrastructure being damaged physically."[25]

Whether such non-lethal cyber operation rises to the level of armed conflict (especially in cases where they are the only hostile operation conducted against the adversary) or, once there is an armed conflict, whether they are subjected to the rules on the conduct of hostilities has been the subject of an ongoing debate in the literature. In such respect the prevailing view in literature provides that it is only when cyber operations cause an equivalent effect to that of kinetic force, namely injury or death to persons or damage or destruction to property that they constitute an armed conflict under the Geneva conventions.[26] Others, on the other hand, contend that cyber operations which lead to disruptions and interference without causing physical damage or destruction can also constitute an armed conflict within the meaning of the Geneva conventions.[27]

Most importantly, the dual-use nature of cyber infrastructures and the interconnectivity of the cyberspace have posed a serious challenge in applying the core principles of IHL, i.e., distinction, proportionality, and precaution, to cyberwarfare. Almost the entire infrastructures in the cyber space (computers, servers, and cables) are dual-use objects i.e. serving both civilian and military purposes.[28] Thus it is to a large extent impossible to differentiate between civilian and military infrastructures in the cyberspace. This runs counter to the assumption that lies behind the existing IHL rules on the conduct of hostilities, which is civil and military objects are for the most part distinguishable.[29]

[24] Eitan Diamond (n 13)73
[25] Cordula Droege (n 11) 546
[26] See, e.g., Michael N. Schmitt, 'The Law of Cyber Targeting' (2015) 7 TP 4; Nils Melzer (n 6) 23-25
[27] Knut Dörmann, Applicability of the Additional Protocols to Computer Network Attacks, (2004) can be accessed on: http://www.icrc.org/eng/resources/documents/misc/68lg92.htm.
[28] Geiss, R., and Lahmann, H., Cyber warfare: applying the principle of distinction in an interconnected space, (2012) 45 Israel Law Review 383
[29] Cordula Droege (n 11) 541

In light of the aforementioned unique features of cyber warfare, this paper mainly aims to critically analyze how to best interpret and apply the existing rules and principles of IHL to cyberwarfare, if they are meant to achieve the objective of limiting the effect of armed conflict.

1.3.Objective of the Research

1.3.1. General Objective

The general objective of this research is to critically analyze how cyber operations that amount to or carried out in the context of armed conflict are regulated under the existing rules and principles of IHL. In doing so it will try to map out the existing contending arguments in the literature and points out a way forward for challenges that can't be accommodated by interpretation.

1.3.2. Specific Objectives

In particular, the research attempts:

- To examine whether cyber operations in and of themselves can constitute an armed conflict within the meaning of the Geneva Conventions,
- To probe what types of cyber operations are subjected to IHL rules on the conduct of hostilities,
- To critically analyze how the existing fundamental principles of IHL can be interpreted and applied to cyberwarfare if they are meant to achieve their humanitarian purpose, and
- To assess the potential challenges in applying the existing rules of IHL to cyberwarfare and the possible way forward.

1.4.Research Questions

The central question that this research aims to address is that: how to best interpret and apply the existing rules and principles of IHL in cyber warfare cases, if they are meant to provide sufficient protection to the civilian population. In doing so the research deals with the following specific questions:

- Can cyber operations in and of themselves constitute an armed conflict?
- What type of cyber operations are subject to IHL rules on the conduct of hostilities?
- How should the existing fundamental principles of IHL be interpreted and applied to cyberwarfare?
- What are the challenges in applying existing fundamental principles of IHL to cyberwarfare and the possible way forward?

1.5.Literature Review

There are several literatures that have touched and addressed the *jus in bello* aspect of cyber warfare. However, with the exception of some of them, the discussion in most of the literatures is not comprehensive.[30] They are either limited to addressing some aspects of the issues involved[31] or attempted to address the whole issues in scanty manner.[32]

Furthermore, despite their consensus on the general application IHL to cyber warfare cases, the arguments under the existing literatures on how to interpret and apply the existing rules and principles of IHL in the cyber realm, in such a way it provides sufficient protection to the civilian population, varies greatly. This variation among other things can be attributed to the unique features of the cyber space and the absence of clear state practice on the issue. Thus it seems necessary to appreciate the issues involved and the contending arguments of authors under existing literatures to have a clear picture of the discussion under this paper.

In such respect most authors rely on effect based interpretation of computer operations to analyze the adequacy or otherwise of the existing IHL rules in the cyber realm. For instance Michael Schmitt a leading expert on cyberwarfare issues argues that cyber operations constitute an armed conflict or once there is an armed conflict can amount to attack under the meaning of the Geneva conventions only when they cause an equivalent effect to that of kinetic force, namely injury or death to persons or damage or destruction to property.[33]

Accordingly, cyber operations that do not injure or kill persons or cause damage or destruction to property (hence not attack) do not trigger the applicability of the restraints imposed by IHL on the conduct of hostilities.[34] Thus they can be directed directly at a civilian infrastructure without any regard to their adherence to the principles of distinction, proportionality and precaution. Schmitt contends that although this line of interpretation expands the rage of targetable objects and results

[30] The Tallinn Manual on the International Law Applicable to Cyber Warfare is considered to be the most comprehensive literature that have tried to interpret the LOAC (both jus ad bellum and jus in bello) to cyber warfare: - Michael N. Schmitt, *Tallinn Manual on the International Law Applicable to Cyber Warfare*, (CUP, 2013)

[31] See for e.g. Eric T. Jensen, Cyber Attacks: Proportionality and Precautions in Attack, (2013) 89 INT'L L. STUD. 198; Jeffrey T.G. Kelsey, 'Hacking into International Humanitarian Law: The Principles of Distinction and Neutrality in the Age of Cyber Warfare' (2008) 106 MLR 1427; Noam Lubell, Lawful Targets in Cyber Operations: Does the Principle of Distinction Apply? (2013) 89 INT'L L. STUD. 252.

[32] Eitan Diamond (n 13)

[33] Michael N. Schmitt, 'Wired Warfare: Computer Network Attack and the Jus in Bello' () 76 ILS

[34] ibid

in the expansion of war's impact on civilian population, it is the only legitimate interpretation of the law as it stands now.[35]

He further claims that the dual use of cyber infrastructures coupled with the interconnectivity of the cyberspace poses a new and sometimes troubling quandaries. However, for the most part "humanitarian law in its present form generally suffices to safeguard those it seeks to protect from the effects of computer network attack."[36]

On the other hand, Cordula Droege in his article "Get off my cloud: cyber warfare, international humanitarian law, and the protection of civilians"[37] asserts that cyber operation that has disrupted the function of vital infrastructure can constitute an armed conflict even if no death or injury to persons or physical damage or physical destruction to property has ensued. Corollary once there is armed conflict such type of cyber operation would amount to attack thus subject to the restraints imposed by IHL on the conduct of hostilities. Therefore, they cannot be directed directly against civilian infrastructure and if directed against military objectives their effect on civilian infrastructure must be taken into consideration in proportionality assessment and precaution.

In concluding his discussion Deroge provides that the existing IHL rules can provide sufficient protection to the civilian population in cyber warfare cases only if they are interpreted expansively (as shown above). But even then considering the potential weakness of the existing IHL principles and the absence of sufficient knowledge on cyber capabilities "it cannot be excluded that more stringent rules might be necessary."[38]

In contrast to Deroge's argument, Gary D. Brown in his article "International Law Applies to Cyber Warfare: Now What"[39] argues against such expansive interpretation of the law. He contends that expanding the concept of attack to the extent of covering nondestructive cyber operations is a risky endeavor that stretches the law to its breaking point. The gist of his argument is that since such expansive interpretation wouldn't be limited to cyber activities and extends to kinetic

[35] Ibid 195 and Michael N. Schmitt, 'The Law of Cyber Warfare: Quo Vadis' (2014) 25 Stan. L. & Pol'y Rev. 296
[36] Michael N. Schmitt (n 32) 209
[37] Cordula Droege (n 11)
[38] Ibid 578
[39] Gary D. Brown, International Law Applies to Cyber Warfare: Now What, (2017) 46 Sw. L. Rev. 355

activities with similar effects it would make humanitarian law difficult and less effective to apply in conventional (kinetic) warfare.

Nils Melzer in his article "cyber warfare and international law"[40] takes somehow a different approach on the issue. Rather than indulging into effect based analysis of cyber operations he relies on the concept of 'hostility' to approach cyber warfare issues. He argues that cyber operations can amount to armed conflict or once there is an armed conflict trigger the rules on the conduct of hostilities if they constitute part of 'hostilities' within the meaning of IHL.[41] For Melzer cyber operations are said to constitute part of hostilities not only if they resulted in death, injury or destruction (although a predominant form of conducting hostility) but also if they adversely affect enemy's military operations or military capacity.

Thus non-destructive cyber operations that have adversely affected enemy's military operation or military capacity would amount to armed conflict or once there is an armed conflict trigger the rules on the conduct of hostilities. In elaborating this point, he asserts that

> *cyber operations aiming to disrupt or incapacitate an adversary's computer-controlled radar or weapons systems, logistic supply or communication networks may not directly cause any physical damage, but would certainly qualify as part of the hostilities and, therefore, would have to comply with the rules and principles of IHL governing the conduct of hostilities.*[42]

But his argument fails to provide an answer for the most contentious issue namely, whether non-destructive cyber operation that disrupt purely a civilian infrastructure without causing either military harm or death, injury or destruction is subject to the rules on the conduct of hostilities. In this respect Melzer only refers "to the dilemma between adopting either a too restrictive or a too permissive interpretation of the law."[43]

Be that as it may, the discussion under the aforementioned literatures makes it clear that there is no consensus among authors on how to best interpret and apply the existing rules and principles

[40] Nils Melzer (n 6)
[41] Ibid 27
[42] Ibid 28
[43] Ibid

of IHL in cyber warfare cases. Thus this research by critically appraising and analyzing the existing arguments in light of the object and purpose of IHL tries to contribute to the ongoing debate.

1.6.Research Methodology

In order to achieve its objectives, the research will employ a doctrinal research method. As such relevant available literature on the subject will be reviewed and analyzed. In particular, the research will consult and examine conventions, cases, books, journal articles and documents that have relevance to the topic.

1.7.Scope of the Research

This research is limited to examining the *jus in bello* aspect of cyber warfare, and will not discuss other bodies of law that may be applicable to cyberwarfare. Accordingly, it will explore how the existing rules and principles of IHL can be interpreted to make sense in the cyber realm. But due to the broadness of issues involved the research mainly focuses on how to best interpret and apply the fundamental principles of IHL i.e. distinction, proportionality and precaution to cyberwarfare and to point out a way forward for challenges that cannot be accommodated by interpretation.

1.8.Significance of the Research

As it has been pointed out under statement of the problem part of this paper cyber warfare involves unique features that seem awkward to fit into the existing rules of IHL. This has ignited a considerable debate, which is still unabated, in the literature on how to best interpret and apply the existing rules of IHL in the cyber realm if they are meant to achieve their humanitarian purpose. In such context the paper tries to contribute to the debate. Furthermore, by mapping out and analyzing the existing arguments and current developments the research provides an updated understanding of the issue. This in turn will likely induct others to carry out more extensive studies in the area.

1.9.Organization of the Research

In general, the research has the following components. Under chapter one, introduction about the research has been already discussed. Chapter two, as a base for the discussion under chapter three identifies and discusses the evolution, current legal basis and core principles and rules of IHL. Chapter three, as the main part of the research, critically analyzes how cyber operations that amount to or carried out in the context of armed conflict are regulated under the existing rules and

principles of IHL. Finally, the conclusion and recommendation part provides a succinct summary of the main findings of the research and suggests the possible way forward in order to enhance the regulation of cyber warfare.

Chapter Two
Evolution, Legal Basis and Core Principles of IHL

In order to answer the ultimate question of this work, which is whether the existing rules and principles of IHL provide sufficient protection to civilians in cyber warfare cases, it is necessary to appreciate first the evolution, current legal basis and core principles and rules of IHL. Accordingly, as a base for the upcoming discussion of the paper this chapter articulates and discuss in details the aforementioned issues.

2.1. The Concept and Development of IHL

International Humanitarian Law, could be regarded as a body of rules within international law that seek, for humanitarian reason, to limit the effect of armed conflict.[44] It owes its inspiration to a feeling for humanity and focuses on the protection of the individual.[45] As such, it regulates the conduct of parties to an armed conflict with the view of ameliorating the plight and suffering of human beings affected or likely to be affected by the conflict.[46] IHL tries to achieve this humanitarian objective basically by providing protection to persons who are not or no longer participating in hostilities and by restricting belligerents' choice of means and method of warfare.[47]

Historically, IHL traces its origin back to antiquity. As Solis noted it "there were rules attempting to limit armed combat virtually from the time men began to fight in organized groups."[48] A cursory reading into history books reveals that in different societies and periods, as early as 3000 B.C, there were customary rules and bilateral agreements which provide protection to certain categories of victims of armed conflict or limit the use of certain means and method of warfare.[49] Accordingly, except for small cases of bilateral agreements, the conduct of parties to the conflict was mostly regulated by customary rules.

But this started to change in the middle of 19th century propelled by three important events. The first of such event was the adoption of Instructions for the Government of Armies of the United

[44] Hilaire Mccoubrey (n 1)
[45] J. Pictet, 'The principles of international humanitarian law' (1966) 66 IRRC 455
[46] Abdulrashid L. Haruna, 'Tracing Humanity in Warfare: An Exposition of the Evolutionary Trend of International Humanitarian Law' (2014) 2 GJPLR 41
[47] Dan-Iulian Voitaşec, 'Applying International Humanitarian Law to Cyberattacks' (2015) CKSPL 552
[48] Gary D. Solis, *The Law of Armed Conflict: International Humanitarian Law in War* (CUP 2010) 3
[49] Marco Sassoli & Antoine A. Bouvier, *How Does Law Protect in War: Cases, Documents and Teaching Materials on Contemporary Practice in International Humanitarian Law* (2nd ed., 2006) 121; The authors noted that "in spite of their humanitarian importance these customs and agreements only have a limited applicability (apply to specific region and specific war). Furthermore, their implementation was under the sole responsibility of the belligerents."

States in the Field (Lieber code) in 1863.[50] The code was issued for the union soldiers during the American Civil War and represented the first attempt to codify the existing laws, customs and usages of war into one document.

The second and most important event is the adoption of the First Geneva Convention in 1864, which marked the beginning of modern IHL. The Convention is the first international treaty on the conduct of armed conflict and comprises a set of ten articles that are designed to ensure that all soldiers wounded on the battlefield were taken care of without distinction.

The third important event was the adoption of the first multilateral treaty banning the use of, in time of war, Certain Explosive Projectiles (The St. Petersburg Declaration) in 1868. The Declaration was "the first international agreement in which the use of a weapon developed through advances in technology was banned on humanitarian grounds."[51]

Since then IHL experienced a striking evolution and development in many aspects. Among other things, the law has constantly enlarged the category of persons protected under it.[52] Starting with wounded, sick and shipwrecked combatants the protection extended to prisoners of war[53] and the civilian population.[54] Furthermore, since St. Petersburg Declaration restriction on the means[55] and methods of warfare[56] has been dramatically expanded. Contemporarily, the Four Geneva

[50] Instructions for the Government of Armies of the United States in the Field (24 April 1863)
[51] Gary D. Solis (n 48) 50
[52] The 1864 Geneva Convention gives protection only to wounded or sick combatants on the battlefield and to civilians and medical personnel who assist them.
[53] The 1929 Geneva Convention II Relative to the Treatment of Prisoners of War and later Geneva Convention relative to the Treatment of Prisoners of War (1949) 75 U.N.T.S. 135 (GC. III)
[54] Geneva Convention relative to the Protection of Civilian Persons in Time of War (1949) 75 U.N.T.S. 287 (GC. IV)
[55] The rules of IHL regulating the means of warfare have been in the process of constant update parallel to technological advancements and innovation of new weapons. The 1925 Geneva Protocol for the prohibition of the use in war of asphyxiating, poisonous or other gases and of bacteriological methods of warfare; 1972 Convention on the prohibition of the development, production and stockpiling of bacteriological (biological) and toxic weapons and on their destruction; 1980 Convention on prohibitions or restrictions on the use of certain conventional weapons which may be deemed to be excessively injurious or to have indiscriminate effects (CCW) with its protocols; The 1993 Convention on the prohibition of the development, production, stockpiling and use of chemical weapons and on their destruction; The 1995 Protocol relating to blinding laser weapons (Protocol IV [new] to the 1980 Convention); 1996 Revised Protocol on prohibitions or restrictions on the use of mines, booby traps and other devices (Protocol II [revised] to the 1980 Convention); 1997 Convention on the prohibition of the use, stockpiling, production and transfer of anti-personnel mines and on their destruction; the 2008 Cluster Munitions Convention.
[56] The restriction on methods of warfare (Tactics employed in conflict vis a vis an enemy) has also evolved extensively. The most important instruments with regard to the restriction on methods of warfare are the 1899 and 1907 Hague Conventions. Latter the restrictions were elaborated and incorporated under the GC. I-IV and their two APs.

Conventions of 1949 and their two Additional Protocols of 1977, which contain almost 600 articles, constitute the main instruments of IHL.[57]

2.2. Scope of Application

IHL applies exclusively in situations of armed conflict. Under the Geneva Conventions there are two recognized types of armed conflict i.e. international armed conflict (IAC) and non-international armed conflict (NIAC), which trigger the application of the rules of IHL.

As a matter of treaty law the difference between these two types of conflicts are significant. Among other things, the level of regulation prescribed by the Geneva conventions differs greatly based on the characterization of the conflict. As such in comparison to IAC which triggers the application of the whole body of Geneva rules, the existence of NIAC triggers the application of only the basic elements of the Geneva Conventions, such as the humane treatment of those who are not taking part in combat, and the obligation to take care for the sick and the wounded provided under Common Article 3 of the 1949 Geneva Conventions.[58]

But, as a matter of customary law there exists a progressive convergence between rules governing international and non-international conflict. The jurisprudence of ICTY has made it clear that some rules and principles that were designed to regulate IAC have gradually been extended to apply to internal conflicts under customary international law, thereby blurring the distinction between IAC and NIAC.[59] According to the tribunal, customary rules which regulate NIAC include:

> *protection of civilians from hostilities, in particular from indiscriminate attacks, protection of civilian objects, in particular cultural property, protection of all those who do not (or no longer) take active part in hostilities, as well as prohibition of means of warfare proscribed in international armed conflicts and ban of certain methods of conducting hostilities.*[60]

[57] ICRC, *International Humanitarian Law: Answers to your Questions* (2002) 11
[58] Common Article 3 to the 1949 Geneva Conventions
[59] *Prosecutor v Tadic*, Decision on the Defence Motion for Interlocutory Appeal on Jurisdiction, 2 October 1995, Case No. IT-94-1-AR72, para. 97-127
[60] Ibid, para 128

However, despite such progressive convergence of norms that regulate international and non-international armed conflicts, "the fundamental framework, structure, and application of the law remains rooted in the binary differentiation found in in the positive law."[61]

2.2.1. International Armed Conflict (IAC)

An international armed conflict (IAC) is a classic form of armed conflict which involves two or more states as parties on opposing sides. The generally accepted criteria for the existence of IAC is provided under Common Article 2 of the 1949 Geneva Conventions. The provision provides that:

> *The present Convention shall apply to all cases of declared war or of any other armed conflict which may arise between two or more of the High Contracting Parties, even if the state of war is not recognized by one of them.*[62]

Thus, for an IAC to exist, the act must constitute an "armed conflict" and must arise between two or more of the High Contracting Parties.[63] Furthermore, the provision has excluded a formal declaration of war or recognition of the situation as such from being a determinative criterion and provides that, even in the absence of declaration of war or recognition of the situation as such, the *de facto* occurrence of armed conflict triggers the application of IHL.

Additional Protocol I extended the definition of IAC by including "armed conflicts in which peoples are fighting against colonial domination, alien occupation or racist regimes in the exercise of their right to self-determination."[64] Thus for states party to Additional Protocol I the occurrence of armed conflict between the government and national liberation movements constitute an IAC.

2.2.1.1. Armed Conflict

As provided under Common Article 2 of the 1949 Geneva Conventions the existence of IAC, among other things, depends on the existence of armed conflict. However, what amounts to armed conflict has not been defined under any IHL treaty. In this regard, the official ICRC commentary defines armed conflict as:

---

[61] David Wallace et.al, 'Trying to Make Sense of the Senseless: Classifying The Syrian War Under the Law of Armed Conflict' (2017) 25 MSIL Rev 577

[62] Common Article 2 of the 1949 Geneva Conventions

[63] Gary D. Solis (n 48) 150 provides that because all states, countries, have ratified the 1949 Conventions, all states are "High Contracting Parties."

[64] Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflict (1977) 1125 U.N.T.S. 7 (Protocol I) Article 1, para. 3-4

> *any difference arising between two States and leading to the intervention of members of the armed forces is an armed conflict within the meaning of Article 2, even if one of the Parties denies the existence of a state of war. It makes no difference how long the conflict lasts, how much slaughter takes place, or how numerous are the participating forces.*[65]

Similarly, the ICRC Commentary to Additional Protocol I provides:

> *Humanitarian law […] covers any dispute between two States involving the use of their armed forces. Neither the duration of the conflict, nor its intensity, play a role: the law must be applied to the fullest extent required by the situation of the persons and the objects protected by it.*[66]

According to the language of the commentaries, the employment of armed forces seems to be a decisive criterion to characterize the situation as armed conflict. But the majority of authors in the literature posit to the view that armed conflict requires the existence of hostilities between states (nothing less nothing more).[67] Thus, as long as an act of hostility is attributable to a state it can constitute an armed conflict within the meaning of Common Article 2 of the Geneva Conventions. The reference to armed forces in the commentaries should be understood as a form of shorthand referring to hostilities.[68] The actor-based analysis of armed conflict was espoused under the commentaries because at the time the relevant instruments were drafted, armed forces were the entities that engage in hostilities.[69]

Passing the hurdle discussed in the above paragraph does not settle the matter conclusively because there is no agreement as to what constitutes hostilities in the literature. Relatively, there seems to exist a consensus that an act of violence which caused or intended to cause death, injury, damage or destruction, constitutes an act of hostility capable of triggering the application of IHL. The

---

[65] Jean Pictet ed., *Commentary to Geneva Convention III Relative to The Treatment of Prisoners of War* (1960) 23 (emphasis added)

[66] Yves Sandoz, Christophe Swinarski and Bruno Zimmermann (eds), *Commentary on the Additional Protocols of 8 June 1977 to the Geneva Conventions of 12 August 1949*, (1987) para 62 (emphasis added)

[67] It should be noted that an armed conflict can exist even in the absence of hostilities. For instance, a formal declaration of war and cases of partial or total occupation triggers the application of IHL even in the absence of hostilities. *See*: Common Article 2 of the four 1949 Geneva Conventions which extends the applicability of IHL to "all cases of partial or total occupation of the territory of a High Contracting Party, even if the said occupation meets with no armed resistance.

[68] Michael N. Schmitt, 'Wired Warfare: Computer Network Attack and the Jus in Bello' () 76 ILS 191

[69] Ibid

troublesome issue is whether non-destructive actions can qualify as an act of hostilities.[70] In this regard, some authors argue that some non-destructive actions could amount to an act of hostilities within the meaning of the Geneva Conventions.

Moreover, there is also a controversy as to the threshold of the requisite hostility. In this regard, the widely accepted position provides that any use of force (an act of hostility) by one state against another state, irrespective of its scope, intensity, and duration, triggers the existence of an IAC between those states.[71] On the other hand, there are authors who espouse to the view that IAC only comes into effect when the hostility between states reaches a certain level of intensity. Thus according to this view relatively small-scale hostility between States do not trigger an IAC and that only hostility to a greater extent, duration, or intensity can qualify as an armed conflict.[72] This view risks creating a legal vacuum i.e. victims in relatively small-scale hostilities do not enjoy the protection of IHL according to this line of argument. This is inconsistent with the object and purpose of IHL which strives to avoid legal lacunas in the protection of victims of armed conflict.[73]

2.2.1.2. International

In addition to being armed, under Common Article 2 of the Geneva Conventions, the conflict must also be of an "international" nature to qualify as IAC. The conflict is said to be international if it involves two or more states as parties on opposing sides (inter-state warfare).[74] In this regard as discussed in the above section the situation would amount to IAC if an act of hostility which is attributable to a state is directed against another state. This will obviously be the case if the hostility is carried out by the state organs i.e. armed forces, intelligence or law enforcement agencies.[75]

Moreover, hostility carried out by a person or entity not an organ of the state can be attributable to the state if they are "empowered by the law of that State to exercise elements of the governmental authority, provided that the person or entity is acting in that capacity in the particular instance"[76] Furthermore, an act of hostility carried out by unauthorized person or group (which is not militarily

[70] This was not such an issue until very recently. Because the conventional armed conflict involves the use of kinetic force which is destructive or injurious or at least employs a lethal means.
[71] Jean Pictet (n 65) and Yves Sandoz and others (n 66)
[72] Dapo Akande, 'Classification of Armed Conflicts. Relevant Legal Concepts' in Elizabeth Wilmshurst (ed.), *International Law and The Classification of Conflicts* (2012) 41
[73] Hans-Peter Gasser, International humanitarian law and the protection of war victims, ICRC (Nov. 30, 1998) Available at: https://www.icrc.org/eng/resources/documents/misc/57jm93.htm.
[74] S. Neff, *War and the Law of Nations, A General History*, (2005) 250
[75] Michael N. Schmitt, Classification of Cyber Conflict' (2013) 89 INT'L L. STUD. 241
[76] Draft article on state responsibility Art.5

organized) can be attributed to the state if specific instructions to commit such act of hostility is issued by that state.[77] But if an act of hostility is carried out by an organized armed group it can be attributed to the state if that state exercises an overall control over the group, even in the absence of issuance of a specific instruction to that effect.[78] An overall control is deemed to exist when:

> [*a] State (or, in the context of an armed conflict, the Party to the conflict) has a role in organizing, coordinating or planning the military actions of the military group, in addition to financing, training and equipping or providing operational support to that group*.[79]

2.2.2. Non-International Armed Conflict (NIAC)

The second recognized type of armed conflict which triggers the applicability of IHL is a Non-International Armed Conflict (NIAC). Common Article 3 of the Geneva Conventions defines NIAC in negative terms as "armed conflict not of an international character occurring in the territory of one of the High Contracting Parties."[80] As elaborated by the ICTY in *Tadic* case armed conflict not of an international character exists when there is "protracted armed violence between governmental authorities and organized armed groups or between such groups within a State."[81] A Similar definition of Non-International Armed Conflict (NIAC) has also been adopted by other international tribunals and the Rome Statute.[82] The definition espoused by the international tribunals shows that a conflict to constitute NIAC, it must reach a certain level of intensity and the groups fighting against government forces or against each other must have a certain level of organization.

---

[77] Prosecutor v. Tadić, Case No. IT-94-1-A, Appeals Chamber Judgment, (Int'l Crim. Trib. for the former Yugoslavia July 15, 1999) para. 132: "Where the question at issue is whether a single private individual or a group that is not militarily organized has acted as a *de facto* State organ when performing a specific act, it is necessary to ascertain whether specific instructions concerning the commission of that particular act had been issued by that State to the individual or group in question."

[78] Ibid para 137

[79] Ibid

[80] Common Article 3 of the 1949 Geneva Conventions

[81] Tadic (n 59) para. 70

[82] *Prosecutor v. Akayesu*, Case No. ICTR-96-4-T, Judgment, (Sept. 2, 1998) para 619*; Prosecutor v. Rutaganda*, Case No. ICTR-96-3-T, Judgment, (Dec. 6, 1999) para 92; *Prosecutor v. Fofana*, Case No. SCSL-2004-14-AR73, Decision on Appeal Against "Decision on Prosecution's Motion for Judicial Notice and Admission of Evidence," (May 16, 2005) para 32; *Prosecutor v. Lubanga*, Case No. ICC-01/04-01/06, Decision on Confirmation of Charges, (ICC Jan. 29, 2007) para 233; *Prosecutor v. Bemba Gombo*, Case No. ICC-01/05-01/08, Decision on Confirmation of Charges, (June 15, 2006) para 229; Rome Statute of the International Criminal Court (17 July Rome Statute of the International Criminal Court (17 July 1998) UN Doc A/CONF.183/9 of 17 July 1998, entered into force (July 2002) Article 8(2)(f)

2.2.2.1. Intensity

Unlike IAC where the occurrence of hostility irrespective of its intensity constitutes an armed conflict, for NIAC to exist the hostility must reach a certain threshold of intensity. Thus situations of internal disturbances and tensions, such as riots, isolated and sporadic acts of violence and other acts of a similar nature does not constitute an armed conflict within the meaning of Common Article 3 of the Geneva Conventions.[83]

To determine whether the hostility has reached the required level of intensity to trigger the existence of NIAC several indicative factors have been suggested by the international tribunals.[84] Recently the Independent International Commission of Inquiry on the Syrian Arab Republic in concluding that the conflict in Syria has reached the required threshold of intensity to constitute a NIAC, have taken factors such as the employment of heavy weapons by the government, the deployment of armed forces to contain the situation, the use of methods akin to military operation, the need to increase government forces to deal with the situation and the rise of armed clashes which have resulted in considerable human causalities and property damage.[85]

2.2.2.2. Organization

For NIAC to exist the hostility must involve at least one non-state organized armed group as a party to the conflict. Thus the armed group party to the hostility must have some form of organization to characterize the situation as NIAC. But the extent of organization of the group is not required to reach the level of a conventional military unit.

To determine whether the organization threshold has been met, the international criminal tribunals have taken several factors into consideration. For instance, the ICTY in *Limaj* case concluded that the Kosovo Liberation Army (KLA) has met the required Organization threshold for NIAC by taking into consideration factors such as:

---

[83] ICRC, 'How is the Term "Armed Conflict" Defined in International Humanitarian Law?' (2008) Opinion paper, 3: Although this is provided under Article 1(2) of APII it also applies to common Article 3 of the 1949 Geneva Conventions.

[84] Michael N. Schmitt (n 75) 248: The author by referring to the ICTY decision in *Haradinaj* case provides that "factors such as the gravity of the attacks, the collective character of the hostilities, the need to increase forces to deal with the situation, the time over which the hostilities have taken place, and whether the United Nations Security Council has addressed the matter were taken into account in determining whether the hostility has reached the required level of intensity."

[85] Louise Arimatsu et.al, 'The Legal Classification of the Armed Conflicts in Syria, Yemen and Libya' (2014) 15

> *the organization and structure of the armed group; the adoption of internal regulations; the nomination of a spokesperson; the issuing of orders, political statements and communiqués; the establishment of headquarters; the capacity to launch coordinated action between the armed units; the establishment of a military police and disciplinary rules; the ability to recruit new members; the capacity to provide military training; the creation of weapons distribution channels; the use of uniforms and various other equipment; and the participation by members of the group in political negotiations.*[86]

Furthermore, in *Boskoski* case, the ICTY provided that in addition to the preceding factors the group must have the capacity to implement the basic obligation of IHL.[87] This requirement does not expect the group to actually enforce IHL, but its structure must be of a nature to allow such enforcement.[88]

2.2.3. NIAC under Additional Protocol II

The definition of NIAC under Additional Protocol II is more restrictive than the notion of NIAC under Common Article 3 of the 1949 Geneva Conventions and the jurisprudence of international criminal tribunals. Article 1(1) of AP II defines NIAC as an armed conflict:

> [*which] take place in the territory of a High Contracting Party between its armed forces and dissident armed forces or other organized armed groups which, under responsible command, exercise such control over a part of its territory as to enable them to carry out sustained and concerted military operations and to implement this Protocol*.[89]

This definition among other things, provides the requirement for organized armed groups (OAGs) to control a territory which will enable them to carry out a sustained and concerted military operation. Furthermore, it restricts the scope of application of the protocol to NIACs occurring between state armed forces on the one hand and dissident armed forces or other organized armed

[86] Michael N. Schmitt (n 28) 245-246; see also: *Prosecutor v. Limaj*, Case No. IT-03-66-T, Judgment, (Int'l Crim. Trib. For the former Yugoslavia Nov. 30, 2005) para.94-129

[87] ICTY, *Prosecutor v. Boskoski*, IT-04-82-T, Trial Chamber Judgement of 10 July 2008, para 202; For NIAC under Additional Protocol II this requirement is expressly provided under Article 1(1) of AP II

[88] Tallin manual (n 30) 89

[89] Protocol Additional to The Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of Non-International Armed Conflicts (1977) 1125 U.N.T.S. 609 (Protocol II) Article 1(1)

groups on the other hand. Thus an armed conflict occurring only between organized armed groups does not trigger the application Additional Protocol II.

2.3. Fundamental Principles of IHL

Once the application of IHL is triggered the parties to the conflict, in the conduct of their hostilities, are required to adhere to certain rules flowing from three core principles of IHL i.e. the principle of distinction, proportionality, and precaution.

2.3.1. The Principle of Distinction

The principle of distinction requires parties to the armed conflict to distinguish between civilians and civilian objects on the one hand and combatants and military objective on the other hand and accordingly to direct their operation only against combatants and military objectives. This principle was formulated, even though vaguely, for the first time under the Saint Petersburg Declaration of 1868 which indicated that "the only legitimate object which States should endeavor to accomplish during war is to weaken the military forces of the enemy."[90]

The substantive content of the principle of distinction is elaborately provided under Article 48 of AP I which reads that:

> *The Parties to the conflict shall at all times distinguish between the civilian population and combatants and between civilian objects and military objectives and accordingly shall direct their operations only against military objectives*.[91]

This principle is now generally considered as being part of customary international law in both international and non-international armed conflict and has been labeled by the ICJ in its Nuclear Weapons Advisory Opinion as one of two "cardinal" principles of IHL.[92]

The principle of distinction as formulated under Article 48 of AP I has two aspects one relating to the individual and the other relating to objects.[93] The individual aspect of the principle of distinction requires the parties to the conflict to distinguish at all times between civilians and combatants and to direct their operations only against combatants. Thus applied to persons the

[90] Gary D. Solis (n 48) 251
[91] AP I (n 17) Article 48
[92] ICJ, Legality of the Threat or Use of Nuclear Weapons, Advisory Opinion, (1995) para 78
[93] Gary D. Solis (n 48) 251

principle of distinction prohibits direct and deliberate attacks against civilians[94] and the civilian population.[95] This has been affirmed under subsequent rules which operationalize the principle.[96]

The object aspect of the principle of distinction requires the parties to the conflict to distinguish at all times between civilian objects and military objectives and to direct their operations only against military objectives. Thus applied to objects the principle of distinction prohibits attacks or reprisal against civilian objects.[97] Under IHL civilian objects are defined in negative terms as all objects which are not military objectives.[98] Military objectives are in turn defined under Article 52 (2) of AP I as:

> *objects which by their nature, location, purpose or use make an effective contribution to military action and whose total or partial destruction, capture or neutralization, in the circumstances ruling at the time, offers a definite military of advantage.*[99]

Accordingly, an object[100] has to fulfill two cumulative criteria in order to qualify as a military objective. Firstly, the object by its nature,[101] location,[102] purpose[103] or use[104] must make an effective contribution to military action; and secondly, its destruction capture or neutralization, in the circumstances ruling at the time, must offer a definite military advantage. It is only when the

[94] AP I (n 64) Article 50(1) defines civilians as: "persons who do not belong to one of the categories of persons referred to in Article 4(A)(1), (2), (3) and (6) of Geneva Convention (III) as well as in Article 43 of the Protocol." And in case of doubt as to the status of a person, that person shall be considered to be a civilian.
[95] Ibid Article 50(2): defines the civilian population as comprising "all persons who are civilians."
[96] Ibid Article 51(2) and AP II (n 89) Article 13(2) provides that "The civilian population as such, as well as individual civilians, shall not be the object of attack. Acts or threats of violence the primary purpose of which is to spread terror among the civilian population are prohibited." The parties to the conflict are also prohibited from attacking civilians and the civilian population by way of reprisal. (Article 51(6) of AP I)
[97] AP I (n 64) Article 52(1)
[98] Ibid
[99] Ibid
[100] Yves Sandoz and others (n 66) para 2007-8: describes object as something visible and tangible.
[101] Yoram Dinstein, *The Conduct of Hostilities under the Law of International Armed Conflict* (CUP 2004) 88 provides that the term "Nature" refers to the intrinsic character of the object. Further notes that although no list of military objectives by nature has been compiled in a binding manner it includes, among other things, fixed military fortifications, bases, barracks, installations and emplacements, including training and war-gaming facilities and weapon systems, military equipment and ordnance, armor and artillery, and military vehicles of all types.
[102]The term 'location' normally refers to a geographical area which has a particular military importance. See Yves Sandoz and others (n 66) para.2021
[103] Yves Sandoz and others (n 66) para 2022: "Purpose" refers to the intended future use of the object.
[104] Ibid: The term "use" refers to the present function of the object. Thus although an object is civilian by its nature it may qualify as a military objective when it is used for military ends.

two criteria are simultaneously fulfilled that the object qualifies as a military objective in the sense of Article 52(2) of AP I.[105]

It is now generally agreed that an object by its nature, location, purpose or use is said to make an effective contribution to military action if it contributes to the execution of the enemy's military operation or directly supports the enemy's military activities.[106] As such only war-fighting or war-supporting objects could qualify as a military objective. In contrast to this generally held view, the US Commander's Handbook on the Law of Naval Operations expanded the definition of military objective to include war-sustaining objects.[107] In elaborating this position the Handbook provides that economic targets of the enemy that indirectly but effectively support and sustain the enemy's war-fighting capability may also be attacked.[108] This expansive interpretation of military objective creates an unacceptable risk of characterizing almost every object in which civilian activities are carried out as indirectly sustaining the war effort.

Furthermore, to qualify as a military objective the destruction, capture or neutralization of the object, in the circumstances ruling at the time, must offer a definite military advantage. Thus if an attack on the object is expected to offer only a potential or indeterminate military advantage or any other advantage than a military one such object would not qualify as a military objective.[109]

2.3.1.1. Specifically protected objects

The military character of an object is not always conclusive in legitimizing an attack against it. Despite such general rule under Art. 52(2) of AP I there are some objects which are entitled to special protection under IHL. These are objects which are immune from attack except in extraordinary situations. For instance, facilities such as dams, dikes and nuclear electrical generating stations are immune from attack, even when they qualify as a military objective, if such attack might "cause the release of dangerous forces and consequent severe losses among the civilian population."[110] Military medical units are also protected from attack "unless they are used

[105] Ibid para 2018
[106] Tallinn Manual (n 30) 130
[107] US Department of the Navy, *Annotated Supplement to the Commander's Handbook on the Law of Naval Operations* (1997) para 8.1.1
[108] Ibid
[109] Yves Sandoz and others (n 66) para 2024
[110] AP I (n 64) Article 56 (1)

to commit, outside their humanitarian duties, acts harmful to the enemy."[111] Objects which are indispensable to the survival of the civilian population, such as foodstuffs, agricultural areas for the production of foodstuffs, crops, livestock, drinking water installations and supplies and irrigation works, are immune from attack, even when they qualify as a military objective, if such attack is expected to leave the civilian population with such inadequate food or water as to cause its starvation or force its movement.[112]

2.3.1.2. Indiscriminate attack

Civilians and civilian objects are protected not only against direct and deliberate attacks but also against indiscriminate attack.[113] Thus the parties to the conflict are proscribed from conducting an attack in an indiscriminate manner and from employing indiscriminate method or means of warfare.[114] The method or means of warfare is said to be indiscriminate if it cannot be directed at a specific military objective or generate uncontrollable effects.[115]

2.3.2. The Principle of Proportionality

Directing attacks only against military objectives does not guarantee the full protection of civilians and civilian objects. Usually, attacks against military objectives inevitably result in death or injury of civilians and the destruction of civilian objects. This is so because among other things civilians may work inside the military objective or they may reside in the vicinity of the military objective.[116] Furthermore, due to technical or human error, an attack directed against military objective may instead hit civilians or civilian objects. In the past, this was accepted as a legitimate collateral damage.[117]

However, contemporarily the principle of proportionality imposes a restriction on lawful attacks directed against military objectives. As it is provided under Article 51(5)(b) of Additional Protocol I, an attack is precluded if it "may be expected to cause incidental loss of civilian life, injury to civilians, damage to civilian objects, or a combination thereof, which would be excessive in relation to the concrete and direct military advantage anticipated."[118] This principle is generally

[111] For instance, see: Geneva Convention for the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field (1949) 75 U.N.T.S. 31 (GC. I) Article 19 and 21; AP II (n 40) Article 11
[112] AP I (n 64) Article 54(3) (b) and AP II (n 40) Article 14
[113] Yoram Dinstein (101) 116
[114] AP I (n 64) Article 51(4) (a-c)
[115] Ibid and also see: Michael N. Schmitt, 'The Law of Cyber Targeting' (2015) 7 TP 16
[116] Yoram Dinstein (n 101) 119
[117] Ibid
[118] AP I (n 64) Article 51(5)(b)

accepted as being part of customary international law applicable both in international and non-international armed conflicts.[119]

Thus an attack is prohibited if it is expected to inflict excessive collateral damage to civilians and civilian objects in relation to the concrete and direct military advantage anticipated. Carrying out an attack knowing that it will inflict collateral damage to civilians and civilian objects in relation which is clearly excessive to the concrete and direct overall military advantage anticipated, is a war crime under Article 8(2)(b)(iv) of the Rome Statute of the International Criminal Court.[120]

Regarding the collateral damage that must be factored in the proportionality calculus there is a controversy on whether to count injury or death to civilians/ damage to civilian objects, only where it is expected to directly result from the attack, or also to count the harm that is expected to arise as an indirect result of the attack. The generally held view in this regard is that the collateral damage that should be factored in the proportionality calculus encompasses both direct effects and indirect effects that are reasonably expected to ensue from the attack.[121] This line of argument is consistent with the phrase "may be expected to cause" in Article 51(5)(b) of API. Thus as long as the indirect effects are not too remote and can be reasonably foreseen they should be factored in the proportionality calculus.

Moreover, the principle of proportionality provides that the anticipated military advantage that should be measured against the expected collateral damage of the attacks must be concrete and direct. According to the ICRC Commentary, the term concrete and direct implies a "substantial and relatively close military advantages."[122] As such, military advantages which are hardly perceptible and those which would only appear in the long term should be disregarded.[123]

Be that as it may, the principle of proportionality as formulated under Article 51(5)(b) and suffers from one major problem i.e. determining what is excessive. The determination of whether the expected collateral damage is excessive in relation to the anticipated military advantage is a subjective assessment of the person planning the attack. As such it depends on the circumstance

[119] Jean-Marie Henckaerts and Louise Doswald-Beck, *Customary International Humanitarian Law*, vol. I (OUP, 2005) Rule 14 and Yves Sandoz and others (n 66) Para. 4772
[120] Rome Statute (n 82) Article 8(2)(b)(iv)
[121] Ian Henderson, *The Contemporary Law of Targeting* (MNP, 2009) 207-11
[122] Yves Sandoz and others (n 66) para. 2209
[123] Ibid

of the individual and the information available to him. But the final decision as to the proportionality of the attack is measured against a reasonable man standard. The ICTY elaborated this equation under the *Galic* case by stating that:

> *In determining whether an attack was proportionate it is necessary to examine whether a reasonably well-informed person in the circumstances of the actual perpetrator, making reasonable use of the information available to him or her, could have expected excessive civilian casualties to result from the attack*.[124]

However, the problem is determining what a reasonable person could regard excessive, is extremely difficult because dissimilar factors i.e. suffering and damage v. military advantage, are being compared against each other in the absence of a common system of valuation.[125] For instance, in an attack against electrical grid line, it is extremely difficult to determine how much civilian suffering is deemed excessive in reference to the anticipated military advantage of blocking enemy's military communication.[126] In this regard, the ICRC Commentary espouses to the view that extensive collateral damages are considered as excessive.[127] In contrast to such assertion, the generally held view provides that an extensive collateral damage is lawful (not excessive) if the anticipated military advantage is so substantial.[128]

2.3.4. The Principle of Precaution

The principle of precaution as formulated under Article 57(1) of AP I requires parties to the armed conflict to take constant care in conducting their military operation with a view of sparing the civilian population, civilians and civilian objects.[129] This principle, as operationalized under subsequent rules, has two aspects: precautions in attack and precaution against the effects of the attack.

---

[124] *Prosecutor v Galic*, (Trial Chamber) Case No IT-98-29-T (5 December 2003) para 58
[125] Michael N. Schmitt (n 21) 203
[126] ICTY, Final Report to the Prosecutor by the Committee Established to Review the NATO Bombing Campaign Against the Federal Republic of Yugoslavia (hereinafter Final Report to the Prosecutor), 13 June 2000, para. 19. In ex post facto assessment of the proportionality of NATO's attack on Pancevo industrial complex and petroleum refinery which resulted in the release of some 80,000 tons of crude oil into the soil and of many tones of other toxic substances, during the war in Kosovo in 1999, the Committee stated that "it is difficult to assess the relative values to be assigned to the military advantage gained and harm to the natural environment, and the application of the principle of proportionality is more easily stated than applied in practice."
[127] Yves Sandoz and others (n 66) para 1980
[128] Yoram Dinstein, 'The Principle of Distinction and Cyber War in International Armed Conflicts' (2012) 17 JCSL 272
[129] AP I (n 64) Article 57(1)

Precautions in attack among other things require those who plan or decide upon an attack to do everything feasible to verify that targets are military objectives and also are not subject to some other form of protection.[130] The standard of care that must be exercised by those who plan or decide upon an attack in this case is provided as doing everything feasible i.e. "precautions which are practicable or practically possible taking into account all circumstances ruling at the time, including humanitarian and military considerations.".[131] This standard dictates the commander to make a reasonable effort to discover pertinent information about the target before making a decision.[132]

Even though it appeared that the target is a military objective and can be attacked without violating the principle of proportionality, Article 57(2)(a)(ii) requires the commanders to take all feasible precautions in the choice of means and methods of warfare with a view of avoiding and in any event minimizing incidental harm to civilians.[133] Furthermore, Article 57(3) of AP/I stipulates that when a choice is possible between several military objectives procuring similar military advantage the one expected to cause the least incidental civilian losses and damage should be selected.

It further requires them to cancel or suspend an attack if it becomes apparent that it will entail a breach of the principle of proportionality.[134]

It further imposes an obligation to give effective advance warning unless the circumstance dictates otherwise.[135] The ICRC in elaborating this provision provides that giving a warning may be inconvenient when the element of surprise in the attack is a condition of its success.[136] For instance, if the target is movable object giving an advance warning of the attack may be inconvenient, as it would propel the enemy to relocate it. Thus unless in such cases the principle of precaution dictates giving an advance warning.

---

[130] AP I (n 64) Article 57(2)(a)(i)
[131] Protocol on Prohibitions or Restrictions on the Use of Mines, Booby Traps and Other Devices (Protocol II) Annexed to the Convention on Prohibitions or Restrictions on the Use of Certain Conventional Weapons Which May be Deemed to be Excessively Injurious or to Have Indiscriminate Effects (3 May 1996), Article 3(4)
[132] Peter Barber, 'Scuds, Shelters and Retreating soldiers: The Laws of Aerial Bombardment and the Gulf War' (1993) XXXI No.4 ALR 689
[133] Ibid Article 57(2)(a)(ii)
[134] Ibid Article 57(2)(b)
[135] Ibid Article 57(2)(c)
[136] Yves Sandoz and others (n 66) para 2223

The second aspect of the principle i.e. precautions against the effects of attacks requires parties to the armed conflict, to the maximum extent feasible, to keep their military objectives apart from civilians and civilian objects[137] and to take other necessary precautions to protect civilians and civilian objects under their control against the dangers resulting from military operations.[138]

[137] Ibid Article 58 (a & b)
[138] Ibid Article 58 (c)

Chapter Three

Cyberwarfare and IHL

Contemporarily it is axiomatic that individuals, organizations and states rely on the cyber space and its tools for their everyday activities ranging from sending an email to controlling critical system and infrastructure. Alongside such extensive utilization, there arises a great risk that such systems and infrastructures may become the target of malicious cyber operation by the adversary. Accordingly, this part of the paper critically analyzes how much the existing rules and principles of IHL protect these systems and infrastructures from malicious cyber-attacks in armed conflicts.

3.1. Defining cyber warfare

Cyber warfare refers to "a means and methods of warfare that consist of cyber operations amounting to, or conducted in the context of, an armed conflict, within the meaning of IHL."[139] This raises a question what cyber operation can amount to or will be conducted in the context of armed conflict. In its broadest sense cyber operation generally refers to any reduction of information to electronic format and its passage between physical elements of cyber infrastructure.[140] As such any activity in the cyber space which involves the movement of computer codes through data stream is a computer operation.

However, in the context of malicious cyber activities, computer operation can then be subdivided into three categories: computer network exploitation (CNE), computer network attack (CNA), or computer network defense (CND).

CNE or cyber exploitation, refers to "enabling operations and intelligence collection to gather data from target or adversary automated information systems or networks."[141] Among other things, cyber exploitation includes cyber propaganda and cyber espionage activities. Thus activities such as defacement of websites[142] and stealing sensitive information from computers[143] fall under this category of cyber operations. This type of cyber operations is not prohibited under IHL. Hence, it

[139] ICRC, 'Cyber warfare and international humanitarian law' (2013)
[140] US Department of Defense, The National Military Strategy for Cyberspace Operations, 2006, GL-1
[141] Ibid
[142] During the conflict between Georgia and Russia in 2008 the websites of Georgia's Ministry of Foreign Affairs and the National Bank of Georgia were defaced and replaced with a series of photos of the Georgian President Mikheil Saakashvili with Adolf Hitler and other twentieth-century dictators.
[143] IWM, Tracking GhostNet: Investigating a cyber-espionage network, (2009): In 2009, a cyber-spy network called "GhostNet" accessed confidential information belonging to both governmental and private organizations in over 100 countries around the world. GhostNet was reported to originate in China, although that country denied responsibility.

cannot amount to armed conflict or if there is an armed conflict it will not be subjected to IHL rules on the conduct of hostilities.

CNA or cyber-attacks, in turn, refers to cyber operations that go beyond exploitation and aims "to disrupt, deny, degrade, or destroy information resident in computers and computer networks, or the computers and networks themselves."[144] This includes cyber-attacks that damage information resident in computer or networks [145] and attacks that incapacitate[146] or disrupt[147] a computer or computer networks. The Manual on International Law Applicable to Air and Missile warfare reformulates this definition of CNA to include cyber operations that are designed to gain control of a computer network in order to manipulate a physical object.[148]

CND or counter cyber-attack, refers to "actions taken to protect, monitor, analyze, detect, and respond to unauthorized activity within… information systems and computer networks."[149] They are pre-programmed counter cyber-attacks, in response to hostile cyber operation (cyber exploitation or attack) from the outside.

Accordingly, the term cyber warfare or cyber-attack in the subsequent part of this paper should be understood as referring to cyber-attacks or counter cyber-attacks discussed above.

---

[144] Ibid

[145] For instance, in 2003 in the 'Titan Rain' incident terabytes of data were deleted forevermore from U.S. Department of Defense facilities, NASA labs, Lockheed Martin and other systems. (Chinese sources were alleged to have been behind this operation. Miranda Grange, *Cyber Warfare and The Law of Armed Conflict*, (2014) 7 Research Paper

[146] The most employed method to incapacitate a computer or computer networks in recent years is Distributed Denial of Service attack (DDoS). In this type of attack thousands of compromised computers (bot nets) are made to flood the targeted computer network with communication requests, in order to overload and incapacitate it. For instance, in 2007 Estonia suffered from massive DDOS attack after controversially moving a Soviet-era war memorial. At the time Estonia was densely wired and many services were carried out online. The attack by targeting the websites of banks, ministries, newspapers, and broadcasters has led to severe disruption of media, government and banking systems. (Russia is allegedly behind the perpetration of the attack). Similar attacks were also carried out against Georgia in 2008. *See*: Jeffrey T.G. Kelsey, 'Hacking into International Humanitarian Law: The Principles of Distinction and Neutrality in the Age of Cyber Warfare' (2008) 106 MLR 1429

[147]John Richardson, 'Stuxnet as Cyberwarfare: Applying the Law of War to the Virtual Battlefield' (2011) 29 J. Marshall J. Computer & Info. L. 3: For instance, the stuxnet virus which was directed against Iran's nuclear facility in Natanz has disrupted the operation of gas centrifuges and "succeeded in damaging or destroying more than nine hundred centrifuges, setting back Iran's uranium enrichment program by several years." A similar cyber-attack to Stuxnet was reported in Illinois in 2012 where criminal attackers caused a water pump to burn out by turning the pump on and off repeatedly. See also Miranda Grange (n 7) 8

[148] HPCR, Manual on International Law Applicable to Air and Missile warfare, (2009) Rule 1. This includes cyber-operations that are designed to gain control of an opposing party's missile system and cause it to fire upon itself, or a cyber-operation designed to open a dam and unleash a flood.

[149] US Department of Defense (n 2)

3.2. Armed Conflict in the Cyber Space

As noted under Chapter Two of this paper, there are two recognized type of armed conflict under IHL which trigger its application i.e. international and non-international armed conflict. While IAC exists when there is an act of hostility between two or more states, NIAC involves a protracted hostility between a state and an organized armed group or between two or more organized armed groups. Unless the situation qualifies as one of the aforementioned hostilities IHL is inapplicable and other branch of laws such as international human right laws and domestic laws regulate the situation.

3.2.1. IAC in the Cyber Space

Common Article 2 of the 1949 Geneva Conventions defines IAC as an armed conflict involving two or more states as parties on opposing side. Similarly, the ICTY defined IAC as "a resort to armed force between States."[150] Reduced into its basics the existence of IAC requires a resort to armed force and the involvement of two or more states as parties on opposing side.

3.2.1.1. Cyber Armed Conflict

What amounts to armed conflict or resort to armed force is not defined under any IHL treaty. As noted under Chapter Two of this paper, a look at the ICRC commentaries creates an impression that the involvement of members of armed force is the decisive criterion. But, contemporarily an armed conflict is generally understood as a situation involving an act of hostility. The problem is there is no agreement in the literature on the exact meaning of hostility either.

In conventional armed conflict, hostility involves the collective employment of kinetic force which is physically destructive or injurious. If cyber-attack is conducted in the context of such an ongoing conventional armed conflict, it seems uncontroversial that it will be governed by the same IHL rules as that conflict. The controversy lies on whether cyber-attacks in and of themselves can constitute an armed conflict in the absence of parallel conventional hostilities. In other words, the question is if cyber-attacks are the only hostile operations directed against the adversary can they amount to an act of hostility capable of triggering the application of IHL?

According to M. Schmitt providing an answer to such question requires a look into the object and purpose of IHL.[151] A review of IHL instruments makes it clear that protecting persons who do not

[150] *Prosecutor v. Tadić,* Case No. IT-94-1, Decision on the Defence Motion for Interlocutory Appeal on Jurisdiction, (Int'l Crim.Trib. For the Former Yugoslavia Oct. 2, 1995) para. 70

[151] Michael N. Schmitt, 'Wired Warfare: Computer Network Attack and the Jus in Bello' () 76 ILS 191

or are no longer participating in hostilities and their properties lies at the heart of the purpose of IHL. As to the protection given to these entities it is framed in terms of injury or death, or in the case of property, damage or destruction. Thus, any measure which is intended to cause injury, death, damage, or destruction or if such consequences are foreseeable from the act, it can constitute an armed conflict within the meaning of the Geneva conventions. This is so, even if kinetic force is not employed and cyber-attacks are the only hostile operations.[152]

Accordingly, cyber-attacks that are intended to "destroy oil pipelines by surging oil through them after taking control of computers governing flow, causing the meltdown of a nuclear reactor by manipulation of its computerized nerve center, or using computers to trigger a release of toxic chemicals from production and storage facilities constitute an armed conflict."[153] However, most of cyber-attacks do not produce such analogous effect to that of a kinetic force. Cyber-attacks will frequently be resorted to in order to incapacitate the computer network without causing physical damage or destruction. Whether such non-destructive cyber-attacks can amount to armed conflict or not, is difficult to inquire due to lack of state practice on the issue.[154]Different approaches have been espoused in the literature in providing an answer to such question. The most restrictive approach provides that cyber-attacks which do not produce analogous effect to that of kinetic force (injury, death, damage or destruction) can not constitute an armed conflict. Although, such non-destructive cyber-attacks may produce a wide spread and sever effects, extending the definition armed attack to incorporate such scenarios stretches the concept of armed conflict beyond its object and purpose.[155]

The second approach, which clashes head-on to the above approach, considers non-destructive cyber-attacks as capable of constituting armed conflict.[156] Among other things, the object and purpose of IHL, is to avoid lacuna in the protection of victims of armed conflict. This can be deduced from the absence of violence threshold for the existence of IAC. Following this purposive

[152] Ibid 192

[153] Ibid and see also: Cordula Droege, 'Get off my cloud: cyber warfare, international humanitarian law, and the protection of Civilians' (2012) 94 IRRC 546 "if a computer network attack causes airplanes or trains to collide, resulting in death or injury, or widespread flooding with large-scale consequences, there would be little reason to treat the situation differently from equivalent attacks conducted through kinetic means or methods of warfare."

[154] ICRC, International Humanitarian Law and The Challenges of Contemporary Armed Conflicts (2011) Report 37: The report noted that whether or not cyber-attacks that disable an object, without causing a physical damage, can constitute an armed conflict will probably be determined in a definite manner only through future state practice.

[155] Gary D. Brown (n 39) 363

[156] Michael N. Schmitt, 'The Law of Cyber Targeting' (2015) 7 TP 6 and Cordula Droege (n 11) 547

interpretation of the law favors an extensive definition of armed conflict to the extent of incorporating cyber-attacks which incapacitate the function of an object.[157]

There are also authors who have tried to strike the balance between the above two extreme positions. They provide that cyber-attacks which incapacitate the function of critical infrastructures such as electricity and water supply system can constitute an armed conflict if they lasted for a certain period of time.[158] Such instances will inevitably lead to sever hardships, albeit not death or injury, from which IHL seeks to protect the civilian population.[159]

Although the third approach is cogent, it somehow introduces a violence threshold by requiring the cyber-attack on critical infrastructures to last for a relatively longer period of time. But the absence of violence threshold for IAC and the importance states attach to the protection of their critical infrastructures, coupled with IHL's purpose of avoiding legal lacuna in the protection of victims of armed conflict militate in favor of considering non-destructive cyber-attacks against critical infrastructure as constituting armed conflict even if they have lasted for a short period of time. As the debate is still ongoing the approach that will be endorsed by states will probably be determined in a definite manner only through future state practice.[160]

3.2.1.2. Attribution in Cyber Conflict

As provided under Common Article 2 of the Geneva Conventions, for the existence of IAC a situation in addition to being armed conflict must involve two or more states as parties on opposing sides. Thus, unless the parties to the armed conflict are identified as two or more states it is impossible to classify the situation as IAC. In this regard, as noted under Chapter Two of this paper, an act of hostility which is attributable to a state can constitute an IAC if it is directed against

[157] Ibid

[158] Cordula Droege (n 11) 548-549

[159] Ibid; This approach, for instance, has been accepted by the Dutch government as it has endorsed a report which states that: "if an organized cyber-attack (or series of attacks) leads to the destruction of or substantial or long-lasting damage to computer systems managing critical military or civil infrastructure, it could conceivably be considered an armed conflict and international humanitarian law would apply. The same is true of a cyber-attack that seriously damages the state's ability to perform essential tasks, causing serious and lasting harm to the economic or financial stability of that state and its people. An example would be a coordinated and organized attack on the entire computer network of the financial system (or a major part of it) leading to prolonged and large-scale disruption and instability that cannot easily be averted or alleviated by normal computer security systems." Government Response to the AIPICAVV Report on Cyber Warfare, RUKSOVERHEID (April 26, 2012)

[160] ICRC (n 154)

another state. An act of hostility will be attributable to a state if it is carried out by its *dejure* or *defacto* agents.

Accordingly, cyber-attacks perpetrated by state organs (armed forces, intelligence or law enforcement agencies), or by persons or entities exercising elements of governmental authority,[161] or by persons or groups operating under a specific instruction from the state and by organized armed groups over which the state exercises an overall control[162] can constitute an IAC if directed against another state.

In conventional hostilities, as it involves the deployment of troops and artilleries, identifying the author of an attack is relatively easy. However, in cyber-attack identification of the author and attribution of the act is particularly difficult. The existence of IP spoofing[163] and the use of botnets[164], among other things, have made it easy to disguise the origin of cyber-attacks. Besides, even where the origin is revealed it does not ensure revealing the identity of the author. Whether the cyber-attack is carried out by the *defacto* or *dejure* agents of the state remains a puzzle even though it is determined that the attack has originated from government cyber infrastructure of a particular state. This is why states frequently deny that they are responsible for the attack or blame it on a group of independent individuals.

To overcome such factual uncertainty some authors have proposed a legal presumption.[165] For instance, in light of the proscription under international law that states should not allow their territory to be used for the purpose harming another state,[166] if a cyber-attack originated from the government infrastructure of a particular state, a presumption should be drawn that the operation is attributable to the state.[167] However, the existing rules of international law do not support such a presumption. Under the existing rules of international law, if a state claims that it is the victim

[161] An example would be a private corporation that a State authorizes by law to conduct cyber operations on its behalf, so long as the operations in question are of the sort for which said authorization was granted.
[162] Tadic case para 137: the state is said to have an overall control over the group mounting a cyber-attack if it has a role in organizing, coordinating or planning the cyber-attack in addition to financing, training or equipping the group with software or hardware necessary to conduct the attack.
[163] "IP spoofing" refers to the creation of Internet Protocol (IP) packets with a forged source address with the purpose of concealing the identity of the sender or impersonating another computing system.
[164] A "botnet" is an interconnected series of compromised computers used for malicious purposes. A computer becomes a "bot" when it runs a file that has bot software embedded in it.
[165] Cordula Droege (n 11) 543
[166] International Court of Justice (ICJ), Corfu Channel case (*United Kingdom v. Albania*), Judgment of 9 April 1949, p. 22; see also: Tallinn Manual (n 30) Rule 5
[167] Cordula Droege (n 11) 543

of international wrongful act attributable to a certain state, the invoking state bears the burden of proving the same.[168] Furthermore, given the difficulty of shielding computer infrastructure from manipulation and the ease with which one can remotely control a computer and pose under a different identity in cyber space, it would be placing a very high burden on governments to hold them accountable for all operations originating from their computers without any further proof.[169]

Notwithstanding the above mentioned evidentiary difficulty, if the cyber-attack is attributable to a state and amounts to an act of hostility it can constitute an IAC, if it is directed against another state.

3.2.2. NIAC in the Cyber Space

As provided under Common Article 3 of the 1949 Geneva Conventions and the jurisprudence of international criminal courts, a non-international armed conflict (NIAC) exists whenever there is a "protracted armed violence between governmental authorities and organized armed groups or between such groups within a State."[170] Reduced into its basics for the existence of a NIAC a situation must reach a certain level of intensity and the groups fighting against government forces or against each other must have a certain level of organization.

As noted under Chapter Two of this paper, several indicative factors have been suggested by the international criminal tribunals to facilitate the determination whether a given situation and a given group has met the required intensity and organization threshold, respectively, for the existence of NIAC. If cyber-attacks are carried out by a group meeting the organization threshold and parallel to conventional hostilities meeting the intensity threshold for NIAC, it seems uncontroversial that they will be governed by the same IHL rules as that conflict. In other words, if cyber-attacks are carried out in the context of an ongoing NIAC they will be subjected to the same IHL rules governing that conflict.

---

[168] ICJ, Oil Platforms case (*Islamic Republic of Iran v. United States of America*), Judgment of 6 November 2003, para. 57

[169] Tallin Manual (n 30) Rule 7: "The mere fact that a cyber-operation has been launched or otherwise originates from governmental cyber infrastructure is not sufficient evidence for attributing the operation to that State but is an indication that the State in question is associated with the operation." See also: Cordula Droege (n 11)

[170] *Prosecutor v. Tadić*, Decision on the Defence Motion for Interlocutory Appeal, 2 October 1995, IT-94-1, para. 70

The difficulty lies in considering whether cyber-attacks in and of themselves can meet the intensity threshold and whether groups organized entirely online can meet the organization threshold for the existence of NIAC.

3.2.2.1. Virtual Groups as Parties to NIAC

The organization criterion requires an act of hostility to be carried out by a group having some form of organization (capable of being identified as party to the conflict). This would certainly exclude cyber-attacks conducted by individual hackers from the notion of armed conflict.[171] As noted under Chapter Two of this paper, several indicative factors have been suggested by the international criminal tribunals to facilitate the determination whether the organizational threshold has been met by a given group.

Among other things, factors such as having an established command structure, adopting internal regulations, the ability to launch coordinated attack, ability to recruit new members and providing military training were adopted by the ICTY, in *Limaj* case, in determining whether the Kosovo Liberation Army (KLA) has meet the required Organization threshold for NIAC.[172] Most importantly, as it is provided under *Boskoski* case the group must also have the capacity to comply with and enforce IHL to meet the necessary organizational threshold.[173] This requirement is provided expressly for NIAC under Additional Protocol II.[174] It is important to note that what has been required from this requirement is not the actual enforcement of IHL by the group but the group's organization must be of a nature to allow the compliance and enforcement of the law.[175]

In context of cyber-attacks this raises a question whether groups organized entirely online can meet the organization threshold for the existence of NIAC. As noted by Michael Schmitt:

> *The members of virtual organizations may never meet nor even know each other's actual identity. Nevertheless, such groups can act in a coordinated manner against the government (or an organized armed group), take orders from a virtual leadership and be highly organized. For example, one element of the group might*

[171] Nils Melzer (n 6) 24
[172] *Prosecutor v. Limaj*, Case No. IT-03-66-T, Judgment, (Int'l Crim. Trib. For the former Yugoslavia Nov. 30 2005) para.94-129
[173] *Prosecutor v. Boskoski*, IT-04-82-T, Trial Chamber Judgement of 10 July 2008, para 202; For NIAC under Additional Protocol II this requirement is expressly provided under Article 1(1) of AP II
[174] Article 1(1) of the protocol.
[175] Tallin Manual (n 30) 89 and Yves Sandoz (n 66) para.4470

be tasked to identify vulnerabilities in target systems, a second might develop malware to exploit those vulnerabilities, a third might conduct the operations and a fourth might maintain cyber defenses against counter-attacks.[176]

Although such group seems to fulfill most of the factors provided under the *Limaj* case, the primary obstacle to the characterization of the group as organized would be its inability to enforce compliance with international humanitarian law.[177] Since there would be no means to enforce compliance of the law with regard to individuals with whom there is no contact, groups which are organized virtually do not meet the organization threshold.

3.2.2.2. The Intensity Threshold in Cyber Conflict

In contrast to IAC where the mere existence of hostility regardless of its intensity constitute an armed conflict, in the case of NIAC there is a higher threshold whereby a situation must reach a certain level of intensity. In this regard what has been clear so far is not when the intensity threshold is deemed to be met but rather when it is not. As such situations of internal disturbances and tensions, such as riots, isolated and sporadic acts of violence and other acts of a similar nature do not constitute an armed conflict within the meaning of Common Article 3 of the Geneva Conventions.[178]

To facilitate the determination whether a certain situation has met the required threshold of hostility several factors has been suggested by the international criminal tribunals. Among other things, factors such as the employment of heavy weapons by the government, the deployment of armed forces rather than the police to control the situation, the use of methods similar to military operation and the infliction of considerable human causalities and property damage as a result of the confrontation were taken to concluded that a given situation has meet the required intensity threshold for NIAC.[179]

Most of the aforementioned factors, as indicators of the fulfilment of intensity threshold, presuppose kinetic confrontation in the physical world. This raises a question whether cyber-attacks in and of themselves, in the absence of kinetic force, could meet the required threshold of

[176] Michael N. Schmitt, 'Classification of cyber conflict' (2012) 17 JCSL 256
[177] Ibid
[178] ICRC, 'How is the Term "Armed Conflict" Defined in International Humanitarian Law?' (2008) Opinion paper, 3: Although this is provided under Article 1(2) of APII it also applies to common Article 3
[179] ICTY, *Prosecutor v. Limaj*, paras 135–170; ICTY, *Prosecutor v. Haradinaj*, para. 49; ICTY, *Prosecutor v. Boskoski*, paras 177–178

intensity for the existence of NIAC. As noted in the discussion of IAC, to constitute an act of hostility cyber-attacks must either cause analogous effects to that of kinetic force or must incapacitate the function of critical objects. Accordingly, cyber-attacks which disrupt computer networks to cause damage to objects (like stuxnet virus)[180], or that opened the floodgates of dams inevitably causing injury or death to persons and damage and destruction of property, or cyber-attacks which incapacitate the function of air traffic control system thereby causing aircrafts to collide, would meet the intensity threshold, provided that they are not merely sporadic. This is a high threshold which would exclude many cyber-attacks from qualifying the intensity threshold. Thus except for some exceptional circumstances cyber-attacks directed by an organized armed group do not meet the intensity threshold for the existence of a NIAC.[181]

3.3. Fundamental principles of IHL and Cyber-attacks

Once the application of IHL is triggered the parities to the conflict, in the conduct of their hostilities are required to adhere to certain rules flowing from three core principles of IHL, i.e., the principle of distinction, the principle of proportionality, and the principle of precaution. It is through these rules that the law tries to provide protection for civilian victims of armed conflict.

These rules which operationalize the three principles are formulated in terms of "attack." For instance, rules operationalizing the principle of distinction provides that "the civilian population as such, as well as individual civilians, shall not be the object of attack"[182]; "civilian objects shall not be the object of attack"[183]; "indiscriminate attacks are forbidden"[184]; and "attacks shall be limited strictly to military objectives"[185]. Rules which operationalizes the principle of proportionality prohibits "an attack which may be expected to cause incidental loss of civilian life, injury to civilians, damage to civilian objects, or a combination thereof, which would be excessive in relation to the concrete and direct military advantage anticipated."[186] The same applies to the

[180] See footnote 147
[181] Robin Geiss, 'Cyber Warfare: Implications for Non-International Armed Conflicts' (2013) 89 INT'L L. STUD. 634
[182] AP I (n 64) Article 51(2)
[183] Ibid Article 52(1)
[184] Ibid Article 51(4)
[185] Ibid Article 52(2)
[186] Ibid Article 51(5)(b)

rules operationalizing the principle of precaution "precautions in attack"[187] and "precautions against the effects of attack."[188]

As it is apparent from the reading, the aforementioned rules deciphering the meaning of "attack" is particularly important before embarking on analyzing the principles.

3.3.1. Cyber-attack as "an Attack"

Article 49 of AP I defines "attacks" as "acts of violence against the adversary, whether in offence or in defense."[189] The ICRC Commentary in elaborating this provision provides that acts of violence refers to a physical force.[190] Thus, acts such as dissemination of propaganda, embargoes or other non-physical means of psychological, political or economic warfare are excluded from the notion of "attack".[191]

According to the text of Article 49 of AP I and the commentary, only acts involving the employment of physical force seems to qualify as an "attack". However, it is now generally agreed that attack within the meaning of Article 49 of AP I implies not a violent act but a violent consequence.[192] Thus, even though the means employed is not violent an act can qualify as an attack if it produces a violent consequence. This 'consequence based' interpretation of attack is supported by subsequent articles of AP I. Attack in these rules is framed, not in terms of the means employed but, in terms of violence ensuing from it. For instance, civilians are protected against "*dangers* arising from military operations."[193] An attack is said to be disproportionate if it produces excessive "*loss* of civilian life, *injury* to civilians, *damage* to civilian objects."[194] These provisions reflect the drafters' intention to follow the consequential harm approach to qualify as an "attack." Furthermore, despite their non-kinetic nature, acts employing biological or chemical weapons have been always characterized as attacks because of their harmful or lethal consequence.[195]

[187] AP I (n 64) Article 57
[188] Ibid Article 58
[189] Ibid Article 49, AP I
[190] Yves Sandoz and others (n 66) Para. 1880
[191] Ibid
[192] Michael N. Schmitt, 'Cyber Operations and the Jus in Bello: Key Issues' (2011) 87 INT'L LAW STUD 93; Michael N. Schmitt, wired warfare, p.194; Yoram Dinstein (n 101) 84; Zen Chang, 'Cyberwarfare and International Humanitarian Law' (2017) 9 CICLJ 34
[193] AP I (n 64) Article 51(1) and Article 58(c)
[194] Ibid Article 51(5)(b) and see also Article 57 (2)(iii); Article 57(2)(b)
[195] Michael N. Schmitt (192) 94; Tadic Case (n 32) para. 120, 124

Corollary, cyber-attacks although they do not involve the use of kinetic force, can constitute an "attack" if they produce violent consequences. As such for instance cyber-attacks which disrupt computer networks to cause damage to objects (like stuxnet virus)[196] or that opened the floodgates of dams, inevitably causing injury, or death to persons and damage, or destruction of property, or cyber-attacks which incapacitate the function of air traffic control system thereby causing aircrafts to collide, would qualify as "attacks" within the meaning of Article 49 of AP I. Thus, if the cyber-attack is intended to cause such violent consequences or if such violent consequences are foreseeable, such cyber-attack will qualify as an "attack" in IHL terms.

The controversy arises when one considers cyber-attacks that do not cause violent consequences (injury, death, damage or destruction) but rather incapacitate or disrupt the function of an object without causing physical damage. In this regard there are two competing approaches. The narrow approach provides that "[a] cyber operation, like any other operation, is an attack when resulting in death or injury of individuals, whether civilians or combatants, or damage to or destruction of objects, whether military objectives or civilian objects."[197] According to this approach damage to objects refers to physical damage and cyber-attacks that do not cause such physical damage to an object do not constitute as "attack".[198] This narrow approach is criticized as being under inclusive because both physical damage and cyber incapacitation will ultimately render the object useless. Thus once the object is rendered useless it would not make sense to create a distinction based on the manner that was achieved.[199]

The alternative broader approach, to which the author of this paper also espouses, provides that cyber-attacks which incapacitates the function of an object qualify as an "attack" even if no physical damage has been caused to the object.[200] The proponents of this approach basis their argument on Article 52(2) of AP I. The provision defines military objectives as objects "…whose total or partial destruction, capture or *neutralization*, in the circumstances ruling at the time, offers

[196] See footnote 147
[197] Michael N. Schmitt (n 192) 94
[198] The ardent proponent of this view Michael N. Schmitt now proposed a less militant version of this approach by providing that the term damage encompasses operations that, while not causing physical damage, nevertheless break an object, rendering it inoperable, as in the case of a cyber-operation that causes a computer-reliant system to no longer function unless repaired (unless the operating system or any software essential to its operation is reloaded). See Michael N. Schmitt, 'Rewired Warfare: Rethinking the Law of Cyber Attack' (2014) 96 IRRC 202-03, Available at: https://www.icrc.org/en/intemationalreview/article/rewired-warfare-rethinking-law-cyber-attack.
[199] Cordula Droege (n 11) 558
[200] Knut Dormann, 'Applicability of the Additional Protocols to Computer Network Attacks' (2004) ICRC 4

a definite military advantage."[201] The reference to neutralization under the provision shows that "attack" may not only lead to destruction of the object but also may incapacitate the function of an object without necessarily destroying it.[202] Furthermore, damage to an object was provided as one effect of "attack" from which IHL wants to protect civilians.[203] The dictionary meaning the term damage is different from destruction and it refers to a "harm impairing the value or usefulness of something."[204] Thus cyber-attack which impairs the use of an object without destroying it will qualify as an "attack".

However, it must be noted that the loss of functionality has to be in relation to an object existing in the physical world. Several infrastructures rely on computer networks and systems for their operation. For instance, most critical national infrastructures including power, energy, water, banking, transportation, telecommunication and vital enterprises such as pipelines, manufacturing plants rely on supervisory control and data acquisition (SCADA) systems for their operation.[205] As such, cyber-attacks by disrupting, incapacitating or gaining control of the SCADA system may disable the function of such critical infrastructures and vital enterprises. If the cyber-attack is designed to cause such effect or if it is reasonably foreseeable that such effect will transpire from the cyber-attack such cyber-attack qualifies as an "attack" within the meaning of Article 49 of AP I.

In contrast, cyber-attacks causing a harm below what has been provided under the above paragraph do not qualify as an "attack". As such, unless expressly prohibited,[206] can be directed against civilians and civilian objects. For instance, cyber-attacks that block an email or social network communications, or online booking or shopping systems, or websites do not qualify as "attack". Therefore, they can be directly directed at civilians and civilian objects. In traditional conflicts, achieving such effects require physical destruction of communication towers, which obviously qualifies as an "attack". Hence, directing them against civilians and civilian objects will be

[201] AP I (n 64) Article 52(2) (emphasis added)
[202] Knut Dormann (n 200) 4
[203] For instance, Article 51(5)(b) of AP I prohibits an attack "which may be expected to cause incidental loss of civilian life, injury to civilians, *damage* to civilian objects […]"
[204] Oxford dictionary, Available at: https://en.oxforddictionaries.com/definition/damage
[205] Bonnie Zhu, Anthony Joseph, Shankar Sastry, 'A Taxonomy of Cyber Attacks on SCADA Systems' (2011) 380-388, (Conference Paper)
[206] For instance, military establishments and object indispensable for survival are protected not only from attacks but also from harms that fall below such threshold. See the discussion under section 3.3.2.1. of this paper

prohibited the principles of IHL. However, non-destructive cyber-attacks, because they may not amount to "attack" as in the above examples, expand the possibility of targeting otherwise protected persons and objects. This illustrates how IHL, while very useful in a traditional kinetic situation, fails to provide the same level of protection for civilians who might be victims in cyber war.

Another issue which arises, unique to cyber-attacks, is that whether cyber-attacks which are designed to damage data resident on computer or computer networks can amount to "attack" in the sense of Article 49 of AP I. The ICRC commentary to the Additional Protocols provides that the term object refers to something which is "visible and tangible."[207] Hence damage to data does not amount to "attack". This interpretation of object as something visible and tangible would have sufficed at the time when the instruments were drafted. At that particular point of time it is unlikely that the drafters would have contemplated the possibility of destroying data without physically damaging the storage method, such as paper files.[208]

However, in contemporary cyber reliant world data resident on computer and computer networks can be destroyed through cyber-attacks, without any damage is done to the computer or computer networks. As such, applying the prevailing interpretation to such cases results in absurd consequence. As Noam noted it, while kinetic attack that results in the setting on fire of five hundred mailbags is an "attack", and a cyber-operation that permanently deletes five million e-mails is not an attack.[209] The existence of back up data and its retrievability can be posed against considering data as an object. But there are some data that are directly transformable into tangible objects, such as banking account data that are directly transformable into money, and data that have intrinsic value, like digital arts. In such situations destroying the data corresponds to the destruction of an object.[210] Thus, the law should evolve to accommodate at least the cyber destruction of such kind of data into the concept of "attack".

3.3.2. The Principle of Distinction in the Cyber Space

The principle of distinction as formulated under Article 48 of AP I requires parties to the armed conflict to distinguish between civilians and civilian objects on the one hand, and combatants and

[207] Yves Sandoz and others (n 66) para 2007-8
[208] Noam Lubell, 'Lawful Targets in Cyber Operations: Does the Principle of Distinction Apply?' (2013) 89 INT'L L. STUD. 267
[209] Ibid
[210] Michael N. Schmitt (n 192) 96

military objectives on the another hand and to direct their operation only against combatants and military objectives.[211] This principle is generally considered as reflective of customary international law applicable in both IAC and NIAC[212]and has been labeled by the ICJ as one of the two cardinal principles of IHL.[213]

Accordingly, the principle of distinction prohibits direct and deliberate attacks against civilians and civilian objects.[214] As such applied to cyber-attack cases the principle prohibits cyber-attacks that are designed to deliberately cause injury or death of civilians and damage or destruction of purely civilian objects, either by opening floodgates of dams or by disrupting air traffic control system that caused a civilian airliner to crash. Whether such consequences are achieved by cyber-attacks or by firing a missile makes no difference for the purpose of IHL.

As noted under Chapter Two of this paper, in order to qualify as a military objective an object by its nature, location, purpose, or use must make an effective contribution to military action; and its destruction, capture or neutralization, in the circumstances ruling at the time, must offer a definite military advantage. Objects which by their nature are considered as making effective contribution to military action includes "materials and buildings that are usually owned or controlled by the military for use by the military."[215] In the context of cyber-attacks, this includes cyber infrastructures of the armed force such as command and control facility and computer components of weapon or weapon systems.[216] Apart from military cyber infrastructures, the most likely military objectives in the cyber context are objects which qualify by the use and purpose criteria. According to these criteria, even though the object is civilian by its nature it will became a military objective when it is used or intended to be used for military ends.

In the context of cyber-attacks, almost the entire international cyber infrastructures serve both civilian and military purposes. When objects are used for both civilian and military purposes they are labeled as dual use objects and became a legitimate military objective. The problem is in cyber context almost all infrastructures in the cyber space i.e. computers, routers, cables, and satellites

[211] AP I (n 64) Article 48
[212] Jean-Marie Henckaerts and Louise Doswald-Beck, *Customary International Humanitarian Law*, vol. I (OUP 2005) Rule 1
[213] ICJ, Legality of the Threat or Use of Nuclear Weapons, Advisory Opinion, (1995) para 78
[214] Article 51(2), 52(1) of AP I and AP II, Article 13(2)
[215] Ian Henderson, *The Contemporary Law of Targeting*, (MNP 2009) 54
[216] Michael N. Schmitt, The law of Cyber Targeting (2015) 7 TP 10 and Yoram Dinstein, 'The Principle of Distinction and Cyber War in International Armed Conflicts' (2012) 17 JCS 263

are used for both civilian and military purposes. For instance, it is reported that 98 percent of US government communications use civilian owned and operated networks.[217] Accordingly, almost the entire international cyber infrastructures qualify as a legitimate military objective by use.

Furthermore, the problem is exacerbated by the fact that not only the current use of an object for military purpose makes it military objective but also its intended future use (the purpose criterion).[218] In elaborating the purpose criterion the Air and Missile Warfare Manual (AMWM) provides that "the purpose criterion recognizes that an attacker need not wait until a civilian object is actually used for military ends before being allowed to attack it as a military objective."[219] Thus, if it is established that the enemy has a real intention to use a certain civilian object for military purpose such object will qualify as a military objective by purpose.

Applying this criterion in the cyber context implies that, if it is established that the enemy is going to carry out a cyber-attack a wide range of cyber infrastructures, namely, servers, routers, cables, or satellites, that such attack might pass through will qualify as a legitimate military objectives.[220]The problem is given the systematic interconnectedness of cyber infrastructures it is impossible to exactly determine the network over which such attack might pass through, thereby rendering the entire network a legitimate military objective.

Thus on the basis of the contemporary definition of military objective the entire cyber infrastructure could possibly qualify as a military objective. In today's world where almost every aspect of civilian life depends on the proper functioning the cyber infrastructures this is a worrying conclusion.[221]

The other point is to qualify as a military objective, the object by its nature, location, purpose or use must make an effective contribution to military action. As noted under Chapter Two of this paper, an object is said to make an effective contribution to military action if it contributes to the execution of the enemy's military operation or directly supports the enemy's military

[217] Eric Talbot Jensen, 'Cyber warfare and precautions against the effects of attacks' (2010) 88 TLR 1534
[218] AP I (n 64) Article 52(2) and Yves Sandoz and others (n 66) para 2020-23 see also Geiss, R., and Lahmann, H. (n 28) 386
[219] PHPCR, 'Commentary on the HPCR Manual on International Law Applicable to Air and Missile Warfare' (2010) 107
[220] Geiss, R., and Lahmann, H. (n 28) 385-386
[221] Ibid 390

activities.[222]Thus, only war-fighting and war-sustaining objects could qualify as military objectives. While the former refers to objects that are used to conduct military operation, the latter refers to objects on which the military operation relies directly such as munition and weapon factories. This raises a question whether IT corporations, such as Microsoft, that produces generic hardware and software not specifically for the military, but which nevertheless are frequently put to military use, qualify as military objectives.[223]

In this regard Eric Talbot Jensen provides that if a civilian computer company produces, maintains, or supports government cyber systems, it qualifies as a military objective, like munition factories, within the meaning of Article 52(2) of AP I.[224] But this analogy between munition factories and corporations producing generic IT tools and systems is faulty. Munition factories produce items that are inherently militaristic, which generic IT tools and systems are not. His argument might have been compellingly convincing if the reference was made to corporations producing malware that will be used to mount a cyber-attack. Corporations producing generic IT tools and systems like corporations producing food items will not qualify as military objectives.[225]

The more troubling issue is in addition to war-fighting and war-supporting objects the US Commander's Handbook on the Law of Naval Operations expanded the definition of military objective to include war-sustaining objects.[226] As such, the Handbook provides that economic targets of the enemy that indirectly but effectively support and sustain the enemy's war-fighting capability may also be attacked.[227] Although arguments in favor and against such expanded approach have persisted before and outside cyber warfare scenarios, the capacity of cyber-attacks

[222] Tallin Manual (n 30) 130
[223] This issue was a subject of controversy between Experts during the preparation of the Tallin Manual but no definite conclusion was reached. See Tallin Manual (n 30) 128-129, commentary no. 9 on Rule 39: "The difficult case involves a factory that produces items that are not specifically intended for the military, but which nevertheless are frequently put to military use. Although all of the Experts agreed that the issue of whether such a factory qualifies as a military objective by use depends on the scale, scope, and importance of the military acquisitions, the Group was unable to arrive at any definitive conclusion as to the precise thresholds."
[224] Eric Talbot Jensen (n 78) 1544 and Eric Talbot Jensen, 'Unexpected Consequences from Knock-on Effects: A Different Standard for Computer Network Operations?' (2003) 18 AUILR 1160 & 1168
[225] Cordula Droege (n 11) 567
[226] US Department of the Navy, *Annotated Supplement to the Commander's Handbook on the Law of Naval Operations* (1997) para 8.1.1
[227] Ibid

to reach and effectively disrupt the function of war-sustaining objects have reinvigorated the debate.[228]

The most compelling and the generally held view in this regard provides that war-sustaining objects could not qualify as military objectives because the connection between this objects and military action is too remote.[229] In other words, since war-sustaining objects do not effectively contribute to military action of the enemy, they could not qualify as military objective within the meaning of Article 52(2) of AP I. Furthermore, the expansive interpretation of military objective creates unacceptable risk of characterizing almost every object in which civilian activities are carried out as indirectly sustaining the war effort. Moreover, the restrictive approach is consistent with the very object and purpose of the principle of distinction, which is that "innocent civilians must be kept outside hostilities as far as possible and enjoy general protection."[230]

Jeffrey T.G. Kelsey contends that although the definition of military objective as it stands now doesn't accommodate war-sustaining objects, it should evolve to do so.[231] He bases his argument on the fact that cyber-attacks against war-sustaining objects such as banks and media could neutralize the targets and hasten the completion of the war without any physical injury to the civilians or physical damage to properties. Traditionally, IHL protected these objects because "a conventional attack would cause substantial civilian casualties and greatly affect civilian lives and property, while serving only an indirect military."[232] Thus, since that risk is nonexistent in cyber-attack cases the law should evolve to accommodate war-sustaining objects into potential military objectives.[233]

Although this argument seems very appealing it is incompatible with the very purpose and object of the principle of distinction mentioned in the above paragraph. The fault of Kelsey's argument lies on contending that a cyber-attack against war-sustaining objects should be permitted not

[228] Michael N. Schmitt (n 215) 12: In explaining the effectiveness of cyber-attacks against war-sustaining objects the author notes that "While kinetic attacks against banks would be highly disruptive, given the limitations of kinetic weaponry and the number of potential targets falling into this category, creating strategic effects capable of undermining the sustainability of the war effort is unlikely. However, cyber-attacks that would, for instance, render the cyber infrastructure upon which the banking system relies dysfunctional could bring the entire system down."
[229] Tallin Manual (n 30) 130-131, commentary no. 16 on Rule 38
[230] Yves Sandoz and others (n 66) para. 1923
[231] Jeffrey T.G. Kelsey (n 8) 1446
[232] Ibid 1440
[233] Ibid

because such objects effectively contribute to military action but because such attacks produce non-destructive effects. If such objects do not effectively contribute to enemy's military action, they remain as civilian objects and the fact that cyber-attacks will produce a non-destructive effect will not change such character. Regarding the claim that such attack will hasten the completion of the war it has been noted that "under no circumstances would military necessity justify any encroachment upon that general prohibition against attacks on civilians and civilian objects."[234]

Regarding the second definitional element of military objectives under Article 52(2), an object in addition to making effective contribution to military action its destruction, capture or neutralization, in the circumstances ruling at the time, must offer a definite military advantage. Thus, if an attack on the object is expected to offer only a potential or indeterminate military advantage or any other advantage than a military one such object would not qualify as a military objective. This holds true in cases where cyber-attacks are used as a means.

What is peculiar in the cyber-context is that because of the technological nature of cyber space it is relatively easy to provide an example where the second definitional element is missing while the first element of making effective contribution is satisfied. The cyber space is resilient, meaning that if certain communication cyber infrastructure is destroyed the communication will find another way in the interconnected cyber space.[235] Thus even though a certain segment of civilian cyber infrastructure by its use or intended future use makes an effective contribution to enemy's military action its destruction or neutralization may not hamper enemy's ability to conduct cyber-attack.[236] As such, since such destruction would not offer a definite military advantage such segment of the civilian cyber infrastructure do not qualify as a military objective within the meaning of Article 52(2) of AP I.

3.3.2.1. Cyber-attacks Against Specifically Protected Objects

In addition to the general rule prohibiting attacks against civilian objects, certain objects, which today are highly dependent on computer control, enjoy special protection under IHL. These objects are immune from attack except in extraordinary situations. For instance, medical units and establishments are protected from attack "unless they are used to commit, outside their

[234] Guenael Mettraux, *International Crimes and the Ad Hoc Tribunals*, (OUP, 2005) 120, citing *Prosecutor v. Galic´*, IT-98-29-T (5 Dec. 2003)
[235] Geiss, R., and Lahmann, H (n 28) 388
[236] Ibid

humanitarian duties, acts harmful to the enemy."[237] As such for instance, it is prohibited to mount cyber-attacks which are designed to shut down an electricity generating system that is exclusively used by hospitals.[238]

Furthermore, the law places not only an obligation not to attack medical units and establishments but also to respect and protect them.[239] According to the ICRC Commentary the term respect and protect implies an obligation not to harm them in any way and not to interfere with their work.[240] In context of cyber-attacks this prohibits cyber-attacks which are designed to destroy or manipulate patients' data as they would interfere with the hospital's work.

Similarly, Article 54 of AP I proscribes to "attack, destroy, remove or render useless objects indispensable to the survival of the civilian population […]"[241] Among such objects drinking water pipeline systems, purification plants and crop irrigation systems rely on computer system for their function. Thus, cyber-attacks which are designed to incapacitate or manipulate these systems are prohibited under this provision. Even when these objects qualify as a military objective, if the cyber-attack is expected to leave the civilian population with such inadequate food or water as to cause its starvation or force its movement it is prohibited.[242]

Works and installations containing dangerous forces such as dams, dykes and nuclear electrical generating stations are immune from attack, even when they qualify as a military objective, if such attack might "cause the release of dangerous forces and consequent severe losses among the civilian population."[243] As such cyber-attacks which are designed to open floodgates of dams thereby causing severe losses among civilian population are prohibited. However, cyber-attacks which shut down the function of such objects without causing the release of dangerous forces are not prohibited, provided that the objects constitute a military objective in the sense of Article 52(2) of AP I.[244]

---

[237] For instance, see: Geneva Convention for the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field (1949) 75 U.N.T.S. 31 (GC. I) Article 19 and 21; AP II (n 40) Article 11
[238] Knut Dormann (n 200) 6
[239] Art. 19 of GC I, Article 18 of GC IV, Art 12 of AP I and Article 11 of AP II
[240] Jean S. Pictet (ed.), *Commentary: I Geneva Convention for the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field*, (1952) 196
[241] AP I (n 64) Article 54
[242] Ibid Article 54(3) (b) and AP II, Article 14
[243] AP I (n 64) Article 56 (1)
[244] Yves Sandoz and others (n 66) para 2153

3.3.2.2. Indiscriminate Cyber-attack

As noted under Chapter Two of this paper, civilians and civilian objects are protected not only against direct and deliberate attacks but also against indiscriminate attack.[245] This rule has been stated under Article 51(4) which proscribes parties to the armed conflict from attacking in indiscriminate manner and from employing indiscriminate method or means of warfare.[246]

The attack is said to be carried out in an indiscriminate manner if it is not directed at a specific military objective and consequently, is of a nature to strike military objectives and civilians or civilian objects without distinction.[247] Applied in cyber context for instance, if a malware that is designed to damage the computer downloading it, is posted on public website that is open to both civilians and combatants alike such cyber-attack would qualify as indiscriminate attack.[248] It is so, not because the means (the malware) was indiscriminate but because it has been employed indiscriminately.

An attack is also indiscriminate if it employed a means and method of warfare which cannot be directed at a specific military objective and consequently, is of a nature to strike military objectives and civilians or civilian objects without distinction.[249] Applied in the cyber context this rule prohibits cyber-attack where it is impossible to predict whether such attack will strike specific military objective rather than civilian computer and computer systems.[250]

Most importantly, an attack is indiscriminate if it employed a means and method of warfare generating uncontrollable effects and consequently, is of a nature to strike military objectives and civilians or civilian objects without distinction.[251] In this case the means and method of warfare is capable of being directed at a specific military objective but its effect cannot be limited.[252] Biological weapon is a prime example this form of indiscriminate means of warfare because an attacker employing them cannot control their spread.[253] Applied in the cyber context viruses directed against a specific military objective violate this rule if they have a nature of replicating

[245] Yoram Dinstein, *The Conduct of Hostilities under the Law of International Armed Conflict*, (CUP 2004) 116
[246] AP I (n 64) Article 51(4) (a-c)
[247] Ibid Article 51(4)(a)
[248] Tallin Manual (n 30) 156-157, comment no.3 on Rule 49
[249] AP I (n 64) Article 51(4)(b)
[250] Tallin Manual (n 30) 145, comment no.3 on Rule 43
[251] AP I (n 64) Article 51(4)(c)
[252] Yves Sandoz and others (n 66) para. 1963
[253] Michael N. Schmitt (n 216) 16

themselves and transmitting from computer to computer free from the control of their creators.[254] Given the interconnectedness of the cyber space such virus will inevitably pass to civilian network and systems in a way that cannot be controlled by the attacker.[255]

However, to apply the restrictions on indiscriminate attacks discussed above, it must be noted that the effect of cyber means or method of warfare must raise to the level of harm that would amount to attack in the sense of Article 49 of AP I (see the discussion under section 3.3.1. of this paper) or with regard to specifically protected objects the level of harm, discussed under the above section of this paper. As such, if the virus spreads uncontrollably infecting several computers but without causing any harmful effect or causing simple inconvenience the restriction under Article 51(4)(c) of AP I will not apply. For instance, the stuxnet virus, which was directed against Iran's nuclear facility in Natanz, although infected several computers caused no damage outside the targeted system of nuclear facility.[256] Thus it does not violate the rule under Article 51(4)(c) of AP I.

3.3.3. The Principle of Proportionality in the Cyber Space

While the principle of distinction prohibits direct and deliberate attack against civilians and civilian objects, the principle of proportionality prohibits attacks against military objective if the expected collateral damage against civilians and civilian objects is excessive in relation to the concrete and direct military advantage anticipated.[257] This principle is generally considered as being part of customary international law applicable in both IAC and NIAC.[258]

Given the dual use nature of most of cyber infrastructures and the interconnectedness of the cyber space there is a serious concern that many civilian infrastructures will be affected by cyber-attacks in armed conflicts. Thus the principle of proportionality plays a paramount role in providing protection to civilians and civilian objects in the cyber context.

As one can understand from the reading Article 51(5)(b) of AP I, in determining the proportionality or otherwise of an attack there are two factors that must be compared against each other, namely the expected collateral damage to civilians and civilian objects and the concrete and direct military advantage anticipated. In this regard, while the collateral damage that must be factored in the

[254] Michael N. Schmitt (n 13) 201
[255] Tallin Manual (n 30) 146, comment no.4 on Rule 43
[256] John Richardson (n 147) 24-25
[257] AP I (n 64) Article 51(5)(b) and Article 57(2)(a)(iii)
[258] Jean-Marie Henckaerts and Louise Doswald-Beck, *Customary International Humanitarian Law*, vol. I (OUP, 2005) Rule 14 and Yves Sandoz and others (n 66) Para. 4772

proportionality calculus it is framed in terms of "loss of civilian life, injury to civilians and damage to civilian objects"[259] concrete and direct military advantage implies a substantial and relatively close military advantages."[260]

As discussed under Section 3.3.1 of this paper, the term damage refers to not only to physical damage of the object but also loss of its functionality. As such, if cyber-attacks are expected to cause death or injury to civilians or physical damage or loss of functionality of an object such effects will be factored in proportionality calculus. However, there is a controversy whether the rule requires to consider such effects when they directly result from the cyber-attack or also when they are indirect or reverberating effects. The generally held view in this regard provides that the collateral damage that should be factored in the proportionality calculus encompasses both direct effects and indirect effects that are reasonably expected to ensue from the attack.[261] Thus as long as it is reasonably foreseeable that the cyber-attack will directly or indirectly results in death or injury to civilians or physical damage or loss of functionality of an object, such effects has to be factored in the proportionality calculus. This line of argument is consistent with the phrase "may be expected to cause" in Article 51(5)(b) of API and was echoed by ICTY in *Galic* case.[262]

But, unfortunately, due to the novelistic character of the cyber space and its complexity, it seems unreasonable to expect a military commander to foresee the direct and reverberating effects of a cyber-attack. To curb this difficulty, Schmitt argues that throughout the mission planning process of a cyber-attack "computer experts will have to be available to assess potential collateral and incidental effects."[263] This is a compellingly convincing position to hold in light of the likelihood that a great number of civilian systems could possibly be affected. The ICTY, in the Galic case mentioned above, has made it clear that information upon which the commander basis his determination must be available. Furthermore, as it would be discussed under the principle of precaution, the commander is required to do everything feasible to verify the potential incidental effects of the proposed attack. This requirement can be extended to cyber-attack cases as requiring an assessment report of computer experts on the potential effects of the attack.

[259] AP I (n 64) Article 51(5)(b)
[260] Yves Sandoz and others (n 66) para. 2209
[261] Ian Henderson, *The Contemporary Law of Targeting* (MNP, 2009) 207-11
[262] *Prosecutor v Galic*, (Trial Chamber) Case No IT-98-29-T (5 December 2003) para 58
[263] Michael N. Schmitt, 'Wired Warfare: Computer Network Attack and the Jus in Bello' () 76 ILS. 204

However, the principle of proportionality is inherently weak. Because determining what is excessive is difficult as the rule requires dissimilar factors i.e. suffering and damage versus military advantage, to be compared against each other in the absence of a common system of valuation.[264] Although this controversy is not peculiar to cyber-attack cases the nondestructive nature of such attacks complicates the matter.

3.3.4. Precaution in the Cyber Space

The principle of precaution, by setting out the standards of care that must be exercised by those planning, deciding, or carrying out attacks, operationalizes the principles of distinction and proportionality. As such, the principle of precaution dictates the commander who plans or decides on an attack to gather pertinent information about the target and the potential incidental effect of the attack before making a decision. By doing so, if it is determined that the target is not a military objective or even if it is a military objective an attack against it will produce excessive collateral damage to the anticipated military advantage, the commander must refrain from launching the attack.[265]

Applied in the context of cyber-attacks, this rule requires, among other things, to do everything practically possible to verify that the targeted cyber infrastructure or system is a military objective and to determine the incidental effects of the proposed cyber-attack is not excessive. This compellingly requires the involvement of computer experts to analyze the target network and the systems with which it is interconnected as best possible.[266] If the nature of the proposed target or the incidental effect of the proposed cyber-attack is not clear even after such expert analysis, the commander must refrain from mounting the attack.[267] Conducting a feasible precaution should not be used to justify a cyber-attack carried out in such circumstances.

However, computer network defense attack or counter cyber-attacks in response to hostile cyber operation from the outside will be pre-programmed to simply target back computers from which the hostile operation originates.[268] In such instances there is no preliminary inquiry as to the nature

[264] Ibid 203
[265] AP I (n 64) Article 57(2)(a)(i) and Article 57(2)(a)(iii)
[266] Eitan Diamond (n 13) 80
[267] Eric Talbot Jensen, 'Cyber Attacks: Proportionality and Precautions in Attack' (2013) 89 INT'L L. STUD. 210
[268] Cordula Droege (n 11) 574

of the target or the incidental effects of the counter cyber-attacks. Thus, states should evaluate the legality of such counter cyber-attacks in light of the principle of precaution under IHL.

Even though it is determined that the proposed target is a military objective and the proposed attack will not result in excessive incidental damage to civilians and civilian objects, the principle of precaution obliges the attacker to choose a means or method of warfare which will likely cause the least collateral damage.[269] In this regard, the availability of cyber-attack expands the options for minimizing collateral damage. For instance, instead of kinetically attacking an electrical grid line the principle of precaution requires the employment of non-destructive cyber-attacks which simply turn off the system without causing physical damage.

The second aspect of the principle i.e. precautions against the effects of attacks requires parties to the armed conflict, to the maximum extent feasible, to keep their military objectives apart from civilians and civilian objects.[270]In cyber context this rule requires states to keep their military and civilian cyber infrastructures apart., This obligation entails, among other things, the establishment of closed military networks and segregating certain highly sensitive civilian infrastructures from outside networks.[271] However, in light of the high amount of cost involved in carrying out such segregation, it is unlikely that states will find it feasible. In contrast, states seem to be moving in the exact opposite direction and co-locating their military cyber infrastructure with civilian infrastructure.[272] For instance, states are moving their military data to cloud i.e. data centers which are primarily used for civilians to store information.[273]

In addition to segregation, the principle of precaution under Article 58(c) of AP I requires states to take necessary precautions to protect civilians and civilian objects under their control against the dangers resulting from military operations. The ICRC commentary to this provision provides examples of measures that states could take to fulfill their obligation under this rule, including providing well-trained civil defense forces, systems for warnings of impending attacks, and responsive fire and emergency services.[274] Applied in the context of cyber-attacks, this rule can be

[269] AP I (n 64) Article 57(2)(a)(ii) of AP I
[270] Ibid Article 58 (a & b)
[271] Cordula Droege (n 11) 575
[272] Eric Talbot Jensen (128) 213
[273]DOD, 'Defense Department to Move to Cloud Computing' (2017) Available at: https://www.defense.gov/News/Article/Article/1402556/defense-department-to-move-to-cloud-computing/ (Accessed April 19, 2018)
[274] Yves Sandoz and others (n 66) para. 2257-58

interpreted as requiring "the provision of protective software products, monitoring networks and systems and providing warnings of impending or ongoing attacks, and providing technical assistance to repair networks or reroute them to alternative systems that continue to maintain functionality."[275]

[275] Eric Talbot Jensen (128) 211

Conclusion

As far as IHL is concerned cyber warfare does not operate in void normative framework but it is subjected to the existing rules and principles. However, transposing the existing rules and principles of IHL to this new form of warfare poses certain difficulties and raises a number of questions. While most of these difficulties and questions can be surpassed and resolved through interpretation, some require the evolvement of the existing IHL rules. But the worrisome issue is that even for issues that can be resolved through interpretation there are considerable competing views and choosing one doesn't settle the matter conclusively. Thus, any argument with regard to the relationship between cyber warfare and IHL, no matter how convincing, is inconclusive.

To begin with quandaries that can be resolved through interpretation, whether non-destructive cyber-attacks could amount to armed conflict, or once there is an armed conflict whether they could constitute an attack in the sense of IHL lies at first place. In this regard, the existing IHL rules on conflict characterization and the conduct of hostilities rest on the assumption that hostilities involve the use of kinetic forces which are either destructive or injurious. While cyber-attacks have the potential to cause destructive or injurious effects, analogous to that of kinetic forces, they also have the potential to cause non-destructive but devastating effects. Whether such non-destructive cyber-attacks in and of themselves could constitute armed conflict, or once there is an armed conflict whether they could amount to an attack, is the subject of an ongoing debate. However, as it has been shown in this paper, non-destructive cyber-attack could constitute armed conflict or once there is an armed conflict, it could amount to an attack only when they incapacitate the function of physical infrastructures. Extending this interpretation to other non-destructive cyber-attacks is beyond the object and purpose of IHL.

As shown in the paper, by following such consequence based analysis of cyber-attacks in relation to the existing rules of IHL, one can conclude that for the most part the existing rules and principles of IHL provide sufficient protection to civilians and civilian objects. However, certain peculiar features of the cyber space have made some rules and principles of IHL objectively difficult to be applied with their full effect as they apply to the traditional means and method of warfare. For instance, much of the existing cyber infrastructures are dual-use objects and as such can be lawfully targeted. Thus, the principle of distinction which was designed to protect civilians and civilian objects from attack is largely devoid of its value in the context of cyber-attacks. Any IHL protection that civilian cyber infrastructure might enjoy will be derived from the principles of

proportionality and precaution. However, due to the inherent weakness of the principles and the complex nature of the cyber space, the protection that is said to be afforded by these principles is precarious. In a world where many aspect of civilian life hinged on the proper functioning of the entire cyber infrastructure this is a worrisome conclusion.

Furthermore, according to the prevailing view, the term object under the existing IHL instruments is understood as referring something visible and tangible. Thus, data resident in computers and computer networks do not enjoy the protection given to objects under IHL. As the rules were drafted at the time where cyber space and cyber operations were science fictions, it is understandable that the drafters could not have contemplated the destruction of data separately from the storage media, such as paper. However, in light of the current technological advancement the prevailing view that object is something visible and tangible is unlikely to survive. Thus, IHL should assuredly evolve to meet the need of protecting civilian virtual data in contemporary world.

Recommendations

In light of the aforementioned problems, it is recommendable that states should adopt a new, comprehensive and cyber specific IHL treaty. Among other things, the adoption of such treaty will alleviate the existing fog of uncertainty as to the precise scope and application of IHL in cyber warfare cases. IHL treaties are mainly criticized for being one war behind reality. Rather than regulating the conduct of parties to the conflict proactively, the treaties so far pop up following a horrific incident in certain war. The advent of this new form of warfare presents states with an opportunity to change the so far regrettable paradigm and to proactively shape the future.

If adopting a new, comprehensive and cyber specific IHL treaty appeared as a utopian proposition, states can amend some rules of the existing treaties to accommodate features peculiar to the cyber space. For instance, the list of specifically protected objects under Article 56 of AP I could be amended to include major Internet exchange nodes or central servers on which millions of important civilian functions rely on. Dams, dykes and nuclear electrical generating stations are specifically protected under this provision because attacking them would cause the release of dangerous forces and consequent severe losses among the civilian population. Similarly, given the reliance of several important civilian functions on major Internet exchange nodes or central servers, an attack against such critical cyber infrastructures would result in severe and wide spread devastating effects. Thus rather than leaving the protection of such objects on inherently weak principles, incorporating them under Article 56 of AP I will enhance their protection.

Furthermore, given the importance of virtual data in this digital age the term object under the existing IHL rules should evolve to accommodate them.

In the meantime, as it is shown in this paper, the existing rules and principles of IHL should be interpreted broadly in such a way that they provide sufficient protection to civilians and civilian properties, despite their limitation.

Bibliography
Books and Journal Articles

- Abdulrashid L. Haruna, 'Tracing Humanity in Warfare: An Exposition of the Evolutionary Trend of International Humanitarian Law' (2014) 2 GJPLR
- Bonnie Zhu, Anthony Joseph, Shankar Sastry, 'A Taxonomy of Cyber Attacks on SCADA Systems' (2011) Proceedings of the International Conference on Internet of Things and 4th International Conference on Cyber, Physical and Social Computing
- Bonnie Zhu, Anthony Joseph, Shankar Sastry, 'A Taxonomy of Cyber Attacks on SCADA Systems' (2011)
- Cordula, 'Get off my cloud: Cyber warfare, international humanitarian law, and the protection of civilians', International Review of the Red Cross (IRRC) (2012)
- Dan-Iulian Voitaşec, 'Applying International Humanitarian Law to Cyberattacks' (2015) CKSPL
- Dan-Iulian Voitaşec, Applying International Humanitarian Law to Cyberattacks, (2015) CKSPL
- Dapo Akande, 'Classification of Armed Conflicts. Relevant Legal Concepts' in Elizabeth Wilmshurst (ed.), *International Law and The Classification of Conflicts* (2012)
- Yoram Dinstein, 'The Principle of Distinction and Cyber War in International Armed Conflicts' (2012) 17 JCS
- Eitan Diamond, Applying International Humanitarian Law to Cyber Warfare, ()
- Eric Talbot Jensen, 'Cyber Attacks: Proportionality and Precautions in Attack' (2013) 89 INT'L L. STUD.
- Eric Talbot Jensen, 'Cyber warfare and precautions against the effects of attacks' (2010) 88 TLR
- Eric Talbot Jensen, 'Unexpected Consequences from Knock-on Effects: A Different Standard for Computer Network Operations?' (2003) 18 AUILR
- Gary D. Solis, *The Law of Armed Conflict: International Humanitarian Law in War* (CUP 2010)
- Geiss, R., and Lahmann, H., Cyber warfare: applying the principle of distinction in an interconnected space, (2012) 45 Israel Law Review

- Guenael Mettraux, *International Crimes and the Ad Hoc Tribunals*, (OUP, 2005)
- Hans-Peter Gasser, International humanitarian law and the protection of war victims, ICRC (Nov. 30, 1998)
- Hathaway, R. Crootof et al., 'The law of cyber-attack' (2012) CLRV
- Hilaire Mccoubrey, International Humanitarian Law: Modern Developments in the Limitation of Warfare (2nd ed. 1998)
- Ian Henderson, *The Contemporary Law of Targeting* (MNP, 2009)
- Iben Yde, The Law of Cyber Armed Conflicts: Translating Existing Norms of International Humanitarian Law into Cyber Language, (2013)
- ICRC, International Humanitarian Law and The Challenges of Contemporary Armed Conflicts (2011)
- ICRC, 'Cyber warfare and international humanitarian law' (2013)
- ICRC, 'How is the Term "Armed Conflict" Defined in International Humanitarian Law?' (2008) Opinion paper
- IWM, Tracking GhostNet: Investigating a cyber-espionage network, (2009)
- J. Pictet, 'The principles of international humanitarian law' (1966) 66 IRRC
- Jean Pictet ed., *Commentary to Geneva Convention III Relative to The Treatment of Prisoners of War* (1960)
- Jean S. Pictet (ed.), *Commentary: I Geneva Convention for the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field, ICRC, Geneva*, (1952)
- Jean-Marie Henckaerts and Louise Doswald-Beck, *Customary International Humanitarian Law*, vol. I (OUP 2005)
- John Richardson, 'Stuxnet as Cyberwarfare: Applying the Law of War to the Virtual Battlefield' (2011) 29 J. Marshall J. Computer & Info. L.
- Knut Dormann, 'Applicability of the Additional Protocols to Computer Network Attacks' (2004) ICRC
- Knut Dörmann, Applicability of the Additional Protocols to Computer Network Attack,
- Louise Arimatsu et.al, 'The Legal Classification of the Armed Conflicts in Syria, Yemen and Libya' (2014)

- Marco Sassoli & Antoine A. Bouvier, *How Does Law Protect in War: Cases, Documents and Teaching Materials on Contemporary Practice in International Humanitarian Law* (2nd ed., 2006)
- Michael N. Schmitt, 'Rewired warfare: Rethinking the law of cyber-attack', International Law Review of the Red Cross (IRRC) (2014)
- Michael N. Schmitt, 'The Law of Cyber Targeting' (2015) 7 TP
- Michael N. Schmitt, 'Wired Warfare: Computer Network Attack and the Jus in Bello' () 76 ILS
- Michael N. Schmitt, Classification of Cyber Conflict' (2013) 89 INT'L L. STUD.
- Michael N. Schmitt, Tallinn Manual on the International Law Applicable to Cyber Warfare, (CUP, 2013)
- Michael N. Schmitt, War, Technology and the Law of Armed Conflict, () 82 ILS
- Miranda Grange, *Cyber Warfare and The Law of Armed Conflict*, (2014)
- Nils Melzer, 'Cyberwarfare and International Law' (2011) UNIDIR
- Noam Lubell, 'Lawful Targets in Cyber Operations: Does the Principle of Distinction Apply?' (2013) 89 INT'L L. STUD.
- Peter Barber, 'Scuds, Shelters and Retreating soldiers: The Laws of Aerial Bombardment and the Gulf War' (1993) XXXI No.4 ALR
- Program on Humanitarian Policy and Conflict Research, 'Commentary on the HPCR Manual on International Law Applicable to Air and Missile Warfare' (version 2.1, March 2010)
- Robin Geiss, 'Cyber Warfare: Implications for Non-International Armed Conflicts' (2013) 89 INT'L L. STUD.
- S. Neff, *War and the Law of Nations, A General History*, (2005)
- US Department of Defense, The National Military Strategy for Cyberspace Operations, (2006)
- US Joint Chiefs of Staff, 'Department of Defense Dictionary of Military and Associated Terms' (2001)
- Yoram Dinstein, *The Conduct of Hostilities under the Law of International Armed Conflict* (CUP 2004)

- Yves Sandoz, Christophe Swinarski and Bruno Zimmermann (eds), *Commentary on the Additional Protocols of 8 June 1977 to the Geneva Conventions of 12 August 1949*, (1987)

Internet sources

- Kirthi Jayakumar, 'Cyberwar and international humanitarian law' (2013) http://www.transconflict.com/2013/03/cyber-war-and-international-humanitarian-law-213/
- Scott Shane, 'Cyberwarfare emerges from shadows of public discussion by US officials' (2012)http://www.nytimes.com/2012/09/27/us/us-officials-opening-up-on-Cyberwarfare.html
- Sandra Song, The Laws of War: Do they Apply in Cyberspace? (2013) http://natoassociation.ca/the-laws-of-war-do-they-apply-in-cyberspace/
- Oxford dictionary, Available at: https://en.oxforddictionaries.com/definition/damage

International Legal Instruments

- Convention on Prohibitions or Restrictions on the Use of Certain Conventional Weapons which may be deemed to be excessively injurious or to have indiscriminate effects (1980)
- Convention on the Prohibition of Development, Production and Stockpiling of Bacteriological and Toxin Weapons and their Destruction (1972)
- Convention on the prohibition of the development, production, stockpiling and use of chemical weapons and on their destruction (1993)
- Convention on the prohibition of the use, stockpiling, production and transfer of anti-personnel mines and on their destruction (1997)
- Geneva Convention for the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field (1949) 75 U.N.T.S. 31 (GC. I)
- Geneva Convention for the Amelioration of the Condition of Wounded, Sick and Shipwrecked Members of Armed Forces at Sea (1949) 75 U.N.T.S. 85 (GC. II)
- Geneva Convention relative to the Protection of Civilian Persons in Time of War (1949) 75 U.N.T.S. 287 (GC. IV)

- Geneva Convention relative to the Treatment of Prisoners of War (1949) 75 U.N.T.S. 135 (GC. III)
- Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts (Protocol I) (Adopted on 8 June 1977, entry into force 7 December 1979)
- Protocol Additional to The Geneva Conventions of 12 August 1949, And Relating to The Protection of Victims of Non-International Armed Conflicts (Protocol II), (Adopted On 8 June 1977)
- Regulations concerning the Laws and Customs of War on Land, annexed to Hague Convention [No. IV] Respecting the Laws and Customs of War on Land, October 18, 1907, annex, 36 Stat. 2277, 1Bevans 631
- Rome Statute of the International Criminal Court (17 July Rome Statute of the International Criminal Court (17 July 1998) UN Doc A/CONF.183/9 of 17 July 1998, entered into force (July 2002)

Cases

- ICC, *Prosecutor v. Bemba Gombo,* Case No. ICC-01/05-01/08, Decision on Confirmation of Charges, (June 15, 2006)
- ICC, *Prosecutor v. Lubanga,* Case No. ICC-01/04-01/06, Decision on Confirmation of Charges, (ICC Jan. 29, 2007)
- ICJ, Corfu Channel case (*United Kingdom v. Albania*), Judgment of 9 April 1949
- ICJ, Legality of the Threat or Use of Nuclear Weapons, Advisory Opinion, (1995)
- ICJ, Oil Platforms case (*Islamic Republic of Iran v. United States of America*), Judgment of 6 November 2003
- ICTR, *Prosecutor v. Akayesu,* Case No. ICTR-96-4-T, Judgment, (Sept. 2, 1998)
- ICTR, *Prosecutor v. Rutaganda,* Case No. ICTR-96-3-T, Judgment, (Dec. 6, 1999)
- ICTY, *Prosecutor v. Limaj*, Case No. IT-03-66-T, Judgment, (Int'l Crim. Trib. For the former Yugoslavia Nov. 30 2005)
- ICTY, *Prosecutor v. Tadić,* Case No. IT-94-1, Decision on the Defence Motion for Interlocutory Appeal on Jurisdiction, (Int'l Crim.Trib. For the Former Yugoslavia Oct. 2, 1995)

- SCSL, *Prosecutor v. Fofana*, Case No. SCSL-2004-14-AR73, Decision on Appeal Against "Decision on Prosecution's Motion for Judicial Notice and Admission of Evidence," (May 16, 2005)