Cyber Warfare and International Humanitarian Law: Evaluating the Need for A Dedicated Legal Framework

Submitted in partial fulfillment of the requirements of the Bachelor of Laws Degree, Strathmore University Law School

By

Bertha Akinyi Ochieng

139175

Prepared under the supervision of

Allan Mukuki

February 2025

Word count 14271

Declaration

I, BERTHA AKINYI OCHIENG, do hereby declare that this research is my original work and that to the best of my knowledge and belief, it has not been previously, in its entirety or in part, been submitted to any other university for a degree or diploma. Other works cited or referred to are accordingly acknowledged.

Signed:

Date: 25/02/2025

This dissertation has been submitted for examination with my approval as University Supervisor.

Signed:.....

Allan Mukuki

Date: 27/2/2025

Abstract

Cyber operations have become a significant aspect of modern warfare, yet they still depend on general international humanitarian law principles to safeguard civilians. This study examines the current legal framework governing cyber warfare and analyses recent cases where the application of IHL to cyber operations has been questioned. It argues for establishing a dedicated legal framework within IHL to specifically address cyber warfare, ensuring that the objectives of IHL, such as the protection of civilians and military necessity, are fully met. The study draws on legal positivism and realism in international relations to assess the need for this specialized framework. By interpreting existing laws and literature on cyber operations, it highlights the inadequacies of the current framework, particularly challenges in applying the definition of an attack and the principle of distinction to cyber operations. In conclusion, it proposes a dedicated framework under IHL that clarifies key principles and definitions, addressing ambiguities and limiting varied interpretations in the context of cyber warfare.

ACKNOWLEDGEMENT

I would like to express my sincere gratitude to my supervisor who guided my throughout the process of writing this dissertation, and assisted me in completion of the same. I would as well like to thank my friends who offered valuable insights, without which I would not have been able to complete this dissertation. To my parents, who's support and constant encouragement was the pivotal to my success throughout this challenging process, I am eternally grateful.

I. List of cases

New Zealand v France

The Corfu Channel Case (U.K V Albania)

II. List of legal instruments

The Geneva conventions of 1949

The additional protocols of 1977

III. List of abbreviations

CO- Cyber Operation

DDoS- Distributed Denial of Services

EU- European Union

FBI- Federal Bureau of Investigation

ICCPR- International Convention on Civil and Political Rights

ICJ- International Court of Justice

ICRC- International Committee of the Red Cross

IHL- International Humanitarian Law

UDHR- Universal Declaration of Human Rights

UN- United Nations

UNC- United Nations Charter

US- United States of America

VCLT- Vienna Convention on the Law of Treaties

TABLE OF CONTENTS

CHAPTER 1

INTRODUCTION

1.1 Introduction

In 2023, there were 2365 cyber breaches with 343,338,964 victims, forming a 72% increase from 2021.[1] According to the ICRC, cyber warfare is, "the means and methods of warfare that rely on information technology and are used in situations of armed conflict."[2] Cyber warfare includes operations on or targeting a computer system targeting a computer system via a data network with the intent to infiltrate, gather, exfiltrate, alter, encrypt, or destroy data, as well manipulating processes managed by the compromised system.[3]

As would be any novel weapon or delivery system, used in armed conflict by or on behalf of parties to the conflict ,cyber means are subject to IHL in the same way.[4] However, principles under IHL may be compromised due to the attempted application of general IHL to a specific field, such as cyber operations(COs) and differences in the interpretation of the principles to the same, especially in instances where are challenging to fit into existing definitions.

This research aims to determine whether there is need for a dedicated legal framework for cyber warfare. It will explore the relationship between IHL and cyber warfare, highlighting areas in which the current legal framework may fall short in achieving the objectives of IHL. It will analyse instances involving the application of cyber warfare to attempt to understand how COs have been dealt with in the current legal context. The research will then evaluate the challenges that result from applying the existing framework and provide recommendations.

---

[1] Identity Theft Resource Centre, *ITRC Annual Data Breach Report*, 10 September 2024, 6.

[2] https://casebook.icrc.org/a_to_z/glossary/cyber-warfare on 10 September 2024.

[3] International Committee of the Red Cross and the Red Cresent, *How Does Law Protect in War*, 10 September 2024, 56.

[4] International Committee of the Red Cross and the Red Cresent, *How Does Law Protect in War*, 10 September 2024, 56.

1.2 Background

Technological advancements have led to the rise and potential continued rise in the use of COs in armed conflict. In Article 36, the commentary to the additional protocols of the Geneva Convention, the parties are under the obligation to determine whether employment of the new weapon or means of warfare would be in contravention of the protocol or any other rule of IHL.[5] This leaves room for a highly contrasting party to determine whether the means they seek to employ fall under existing regulations and protocols under IHL. Cyber-based means of warfare are governed by IHL, just as any new weapon or delivery system has been when employed in armed conflict .The challenge posed in applying means of warfare through cyber technology to IHL is that principles or rules of IHL are challenging to use in the context of COs for multiple reasons. These include, for example, the interconnectivity of military and civilian systems and networks [6] as well as difficulty in attributing responsibility for an attack and the inability to define data as an object as is given under the Additional protocols.[7]

The challenges above show that the current IHL may not fully address the intricacies of cyber warfare, thus requiring a study to conclude whether a separate and dedicated framework is truly needed for cyber warfare to be adequately regulated under IHL.

1.3 Statement of the problem

Even though COs are a generally new development under modern means of warfare, multiple international bodies and states, have stated that the charter of the UN, along with general IHL principles, these include, the principles of distinction and proportionality, apply to cyber warfare.[8]

---

[5] https://ihl-databases.icrc.org/en/ihl-treaties/api-1977/article-36?activeTab= on 5 September 2024.

[6] International Committee of the Red Cross and the Red Cresent, *How Does Law Protect in War*, 10 September 2024, 56.

[7] Huang Z and Ying Y, 'The application of the principle of distinction in the cyber context: A Chinese perspective' International Review of the Red Cross, March 2020 https://international-review.icrc.org/articles/principle-of-distinction-cyber-context-chinese-perspective-913#footnote149_5dif7ti on 8 September 2024.

[8] International Committee of the Red Cross and the Red Cresent, International Humanitarian Law and the challenges of contemporary armed conflicts in 2015, 10 September 2024, 55. f

However, applying the same does not and will not produce the best outcomes in warfare in the future. This is because cyber warfare is a 'sui generis' battlefield.[9] This is seen in the difficulty and somewhat impossibility of applying some principles, such as the principle of distinction due to the interconnectedness of civilian and military objects as well as the difficulty in defining key aspects of IHL under cyber warfare. These include attempting to qualify a cyber object as an object under IHL, even though current literature places an object as a physical thing. There is also difficulty attributing attacks under the current definition, as COs are subject to anonymity at many a times. [10]

As such, this dissertation intends to assess the connection between IHL and the increasingly growing cyber warfare and the degree to which the current legal framework offers guidance regarding the same. It will explore whether there is a need for a specialised legal framework to ensure that IHL is effective in the context of COs while still ensuring and upholding adherence to core IHL principles.

1.4 Justification of the study

There has been discourse in recent years over the inadequacies arising from applying the principles in the Geneva Convention to cyber warfare. However, in most instances, this has ended in the conclusion that IHL can be adequately applied to fit the context as opposed to having a separate framework enacted defining precisely the ambit of IHL in cyber warfare and the extent to which the principles apply, despite considerable ambiguities and inadequacies in the same.

In remaining with a system riddled with inadequacies, the aims of IHL, including the most important, that is, civilian protection in times of warfare, will eventually fail as the use of cyber

[9] Mavropoulou E, 'Targeting in the Cyber Domain: Legal Challenges Arising from the Application of the Principle of Distinction to Cyber Attacks' Journal of Law and Cyber Warfare ,2015, 23 - https://www.jstor.org/stable/26441253?seq=3 on 15 September 2024.

[10] International Committee of the Red Cross and the Red Cresent, *How Does Law Protect in War*, 10 September 2024, 57.

warfare grows. This is because, through cyber means, various targets can be destroyed or disrupted. These include industries, infrastructure and telecommunication systems, among other targets. These potential effects are of great humanitarian concern.

This research is vital in identifying and compiling where IHL falls short and specific and practical circumstances in which IHL has fallen short regarding COs and civilian protection.

1.5 Statement of aims and objectives

The research aims to establish whether a legal framework dedicated to cyber warfare is needed to achieve the goals of IHL. It also aims to provide an understanding of the correlation between IHL and the current legal framework and highlight possible areas in which the current framework may fall short.

To do so, the objectives of the dissertation are to:

1. Examine the applicability of existing International Humanitarian laws to cyber operations

2. Analyse instances of COs in situations of armed conflict

3. Evaluate challenges and limitations in applying the existing legal framework to cyberwarfare

1.6 Research questions

1. Is existing IHL applicable to the context of cyber operations?

2. How have instances of cyber operations been addressed under current legal frameworks?

3. What are the challenges and limitations of applying the existing legal framework to cyber warfare?

1.7 Hypothesis

The existing IHL framework needs to be revised to effectively regulate cyber warfare. A dedicated legal framework is necessary to address cyber operations' unique challenges in armed conflict.

1.8 Theoretical framework

This dissertation draws on three main theoretical frameworks: deontology, legal positivism, and constructivism, to critically analyse the need for a dedicated framework on cyber warfare. Deontology emphasises the moral duty to protect civilians, as outlined in the Geneva Conventions and highlights cyber warfare's challenge in differentiating between civilian and military targets. Constructivism underscores the evolving nature of legal norms, suggesting that international law must adapt to the realities of cyber warfare through state interactions and the creation of new norms. Together, these frameworks support the analysis of the need for a dedicated legal framework for cyber warfare in order to ensure legal clarity and responsive regulation. Legal positivism stresses the importance of codifying clear and specific laws for COs, as existing IHL lacks the specificity needed to cater to modern cyber conflicts adequately.

Deontology, as one of the foundations of this study, makes use of rules to distinguish right from wrong.[11] This theory contemplates whether an action in itself is wrong or right.[12] Immanuel Kant was of the belief that ethical actions act in accordance with universal moral laws for example, do not kill and do not cheat.[13] Deontology also considers intention in action; that is, if

[11] Ethics Unwrapped, 'Deontology', McCombs School of Business, University of Texas, 2024 <https://ethicsunwrapped.utexas.edu/glossary/deontology> on 10 October 2024.

[12] Viva Press, 'Deontology: Pros & Cons', Open Educational Resource, 2024, <https://viva.pressbooks.pub/phi220ethics/chapter/deontology-pros-cons> on 10 October 2024.

[13] Ethics Unwrapped, 'Deontology', McCombs School of Business.

you intend good, then the action is good, but if you intend harm, then the action is bad.[14] In applying this to COs, if the intention of the operation was harm, then the action is morally wrong. This study will use a deontological application of the Geneva Conventions and its additional protocols. The Geneva Conventions establish principles such as distinction, which call for making distinctions between military and civilian objectives in armed conflict so as to be able to ensure civilian protection. However, COs blur the boundary between civilian and military objectives, therefore making application of the principles difficult and somewhat subjective. The current framework does not explicitly address these complexities thus bringing about the need for a dedicated framework to uphold the moral duty to protect civilians as well as maintain Article 31 of the VCLT, calls for the interpretation of treaties 'in good faith and following the normal meaning of the terms.'[15]

Sarina Theys describes constructivism as a theoretical framework that goes beyond material reality and includes the effects of ideas and beliefs on politics. She states that it suggests that reality is constantly being constructed, creating opportunities for change.[16] Fredrich Kratochwil describes international law not only as a system of rules but also one of social norms. [17] Katzenstein defines social norms under constructivism as, "a standard of appropriate behaviour for actors with a given identity". [18] Iain Johnston provides that norms are a result of discursive state practices. He also states the role and importance of communication and dialogue in forming norms. He uses non-coercive communication to develop new understandings and eventually brings states to view specific actions as reasonable and appropriate. Johnston also provides that norms are not static and evolve through state interaction. He offers that the dynamic nature of norms brings about the contestation, reinterpretation and transformation of norms.[19]

[14] Viva Press, 'Deontology: Pros & Cons', 2024.

[15] Article 31, Vienna convention on the law of treaties, 23 May 1969, 1155 UNTS 331.

[16]Theys S, 'Introducing Constructivism in International Relations Theory' E-International Relations, 2018, 1.

[17]Klabbers J, Kratochwil,'The Status of Law in World Society: Meditations on the Role and Rule of Law' *European Journal of International Law*, 2014,1195— https://doi.org/10.1093/ejil/chu082 on 9 February 2025.

[18]Katzenstein P, 'Cultural Norms and National Security: Police and Military in Postwar Japan' Cornell Studies in Political Economy, 1996,5- https://www.jstor.org/stable/10.7591/j.ctv5rdzdm on 15 September 2024.

[19]Johnston A, 'Treating International Institutions as Social Environments', 45 *International studies quarterly* 4, 2001, 7—<https://www.jstor.org/stable/pdf/3096058> on 10 October 2024.

Legal positivism also serves as one of the theoretical foundations of this study. Laws are social constructs that must be codified to ensure clarity, predictability, and enforcement. Jeremy Bentham advocates for the restructuring of the process of determining responsibility and punishment. He believed that this would favour the advancement of both the community and the individual.[20] The study will use the importance of codifying laws to ensure clarity and predictability in application or objectivity. Regarding cyber warfare, legal positivism would stress the importance of developing a specific legal framework that regulates COs, as existing IHL may not fully cover the novel forms of warfare, and the subjective application does not ensure the certainty that positive laws would.

Within the context of the international community, international law is socially constructed and evolves based on the values and practices of the global community. It leaves room for the recognition of new challenges, for instsnce, cyber warfare, which may necessitate the development of new legal norms and codified legal norms in matters as sensitive as international welfare.

Theys elaborates that a norm under constructivist theory becomes expected behaviour when a critical mass of state actors adopts and internalise it in their practices. [21] A norm to become expected behaviour under international law is codified under legally binding statutes, for example, under which the ratifying states are bound to act by the norm. As cyber warfare does not possess a specific and dedicated legal framework, the norm applied is the utilisation of principles of IHL. However, this application is entirely subjective. For objective action in cyber warfare, there needs to be specified norms that are codified to ensure the recognition of these new legal norms of action in terms of cyber warfare.

In employing deontology, legal positivism and constructivism, this dissertation will effectively be able to address the moral imperative to protect civilians as well as argue for the codification

[20] Internet Encyclopedia of Philosophy, 'Jeremy Bentham', University of Tennessee at Martin, 2024, <https://iep.utm.edu/jeremy-bentham> on 10 October 2024.

[21] Theys S, 'Introducing Constructivism in International Relations Theory' E-International Relations, 2018, 2.

of clear and specific laws which will ensure predictability and proper enforcement of IHL to the reality of COs.

1.9 Literature review

The increasing prominence of cyber warfare in modern armed conflicts has sparked debate about whether existing IHL is sufficient to regulate these operations. This literature review explores key scholarly debates and analyses whether the current IHL framework is relevant and appropriate to address the distinctive challenges put forward by cyber warfare. At the heart of this discussion is the principle of distinction and its application to cyberspace, given the boundaries between civilian and military objects are increasingly blurred. Scholars such as Elizabeth Mavropoulou have examined the definitions of attacks and military operations under IHL, arguing that current principles are inadequate when applied to COs, leading to ambiguities and inconsistent interpretations. Other authors, including Tilman Rodenhauser, Laurent Gisel, and Knut Dormann acknowledge the recognition of IHL's applicability to cyberspace but point out significant practical challenges in its application, such as the protection of civilian infrastructure and data in case of an attack on military infrastructure. By analysing key case studies, including Stuxnet, the Russia-Georgia war and the NotPetya attack, this review critically evaluates the limitations of existing IHL frameworks and argues for developing a dedicated legal framework to ensure that IHL principles are effectively applied to cyber warfare.

Applicability of Existing International Humanitarian Law to Cyber Operations

Elizabeth Mavropoulou argues that cyberspace should be considered a 'sui generis' battlefield in the study of the law applicable to it. She states the definition of "an attack" in Article 49 of Additional Protocol I and analyses if cyber-attacks meet the threshold of being classified as an attack[22]. The definition of attacks is also mentioned in the paper by Eric Talbot, who also defines military operations as, "any movements, maneuvers or other activities whatsoever carried out by the armed forces to combat."[23] This dissertation shares this view and adds that multiple

[22]Mavropoulou E, 'Targeting in the Cyber Domain: Legal Challenges Arising from the Application of the Principle of Distinction to Cyber Attacks' Journal of Law and Cyber Warfare ,2015, 27- https://www.jstor.org/stable/26441253?seq=3 on 15 September 2024.

[23]Jensen E, 'Cyber Attacks: Proportionality and Precautions in Attack' United States Naval War College, Volume 89, 89 INT'L L. STUD. 198 , 2013, 202

definitions under IHL must fully or adequately cover cyber warfare. Thus, merely applying current principles is inadequate, and this has resulted in ambiguities.

Mavropoulou also discussed the principle of distinction, a fundamental principle under humanitarian law. It requires parties in conflict to distinguish between combatants and civilians. The paper also calls attention to the difficulty in applying the same to COs, especially because cyber-attacks can cause significant interference without physical harm.[24] The paper further discusses the dual use of most assets, which leaves a situation in which IHL is left to question the legality of attacks when an attack on military objectives affects civilian infrastructure.[25] This research shall use the papers by Talbot and Mavropoulou to advance the argument that cyberspace requires a dedicated framework that expands definitions under IHL, such as the definition of an attack, and objectively explains the principles in their application to IHL instead of subjective application in each instance.

The paper by Eric Talbot elaborates on the fact that commanders and individuals party to COs must recognise their legal obligation to exercise constant care in military operations. The paper elaborates on the proportionality principle and that of precautions as crucial in cyber warfare. Still, it highlights the challenges in applying the principles to COs, including the indirect effect on civilian objects. This is seen when seemingly military infrastructure is attacked. However, a large majority of internet cables, servers and routers are civilian infrastructure and the primary means of cyber-attacks.[26] This research will use the paper by Talbot to emphasise the difficulty in applying IHL principles due to the indirect effects on civilians. The dissertation will also advance the argument that civilian and military objects are heavily intertwined; hence the

https://digital-commons.usnwc.edu/cgi/viewcontent.cgi?article=1029&context=ils on 15 September 2024.

[24]Mavropoulou E, 'Targeting in the Cyber Domain: Legal Challenges Arising from the Application of the Principle of Distinction to Cyber Attacks' Journal of Law and Cyber Warfare ,2015, 23- https://www.jstor.org/stable/26441253?seq=3 on 15 September 2024.

[25]Mavropoulou E, 'Targeting in the Cyber Domain: Legal Challenges Arising from the Application of the Principle of Distinction to Cyber Attacks' Journal of Law and Cyber Warfare ,2015, 26- https://www.jstor.org/stable/26441253?seq=3 on 15 September 2024.

[26]Jensen E, 'Cyber Attacks: Proportionality and Precautions in Attack' United States Naval War College, Volume 89, 89 INT'L L. STUD. 198 , 2013, 9
https://digital-commons.usnwc.edu/cgi/viewcontent.cgi?article=1029&context=ils on 15 September 2024.

normal application of the principles of proportionality and distinction would be difficult if not impossible.

The article by Tilman Rodenhauser, Laurent Gisel and Knut Dormann iterates the public acknowledgement by organisations and states on the applicability of current IHL to COs. The article includes commitments made to multilateral discussions, for example, the Paris Call for Trust and Security in Cyberspace, which restates the relevance of IHL in cyberspace. [27] This dissertation will depart from the view that the same is applicable and elaborate that the difficulties pointed out in the paper are not merely difficulties but are the cause of the departure from the efficient application of IHL principles as well as the resulting harm to civilians due to the same.

Case Analysis of Cyber Operations in Armed Conflicts

Elizabeth Mavropoulou elaborates on the Stuxnet attack, which she states targeted the Iranian uranium enrichment facilities in Natanz in 2010. This formed a formative event in cyber warfare in that it demonstrated the capacity of cyber weapons. She elaborates that Stuxnet was a sophisticated virus distributed through thousands of computer systems worldwide before targeting Natanz facilities, where it destroyed more than 900 centrifuges. She then states that there was no collateral damage to civilian systems and that it spontaneously self-destructed when it did not fit into the programmed target profile.[28] This dissertation will further the argument that the principle of distinction is difficult to apply in cyber warfare as civilian and military objects are interconnected. Although direct harm may not be seen to have come upon civilian objects, there is infiltration of the same and indirect damage.

In the paper by John Richardson, he concludes that The Stuxnet virus sparked debates about the definition of cyber warfare and the relevance of existing laws in governing such operations. He

[27]Gisel L, Rodenhauser T and Dormann K, 'Twenty years on: International humanitarian law and the protection of civilians against the effects of cyber operations during armed conflicts' International Review of the Red Cross, 2020, 13 -https://international-review.icrc.org/sites/default/files/reviews-pdf/2021-03/twenty-years-ihl-effects-of-cyber-operations-during-armed-conflicts-913.pdf on 14 September 2024.

[28]Mavropoulou E, 'Targeting in the Cyber Domain: Legal Challenges Arising from the Application of the Principle of Distinction to Cyber Attacks' Journal of Law and Cyber Warfare ,2015, 24-https://www.jstor.org/stable/26441253?seq=3 on 15 September 2024.

indicates that adapting humanitarian law to the evolving cyber landscape is essential for addressing future challenges. Although the Stuxnet virus self-destructed when it did not fit the target profile and as such, is considered as being able to distinguish between military and civilian, the paper by Richardson raises the issue of the definition of an armed attack and its application to cyber warfare. [29] This dissertation will use the paper by Richardson to advance the idea that it is difficult to apply IHL definitions to cyber warfare. It would be simpler and ensure consistency if a specialised framework existed for the same.

Ronald Deibert, Rafal Rohozinski and Masashi Crete-Nishihata write about the Russia-Georgia War. The authors explain that both sides experienced Distributed Denial of Services(DDOS) which were aimed at disrupting their online presence. In the instance of the Georgian government for example, their websites were targeted, leading to disruptions in their ability to communicate and disseminate information. The authors also outline that the war resulted in the severing of fibre optic trench lines, disruption of internet-based communication due to DDoS and effects on key infrastructure. This includes the financial sector of the Georgian government. There were as well consequences to essential services.[30] This research brings to light the harmful effects of cyber warfare and the effects on civilian infrastructure, which are heavily interconnected with military infrastructure. The author brings to light the effects of disruption of military services on civilian infrastructure as the disruption in this instance was to Georgian communication by the government but had vast effects on the civilians as well. Further, it brought to light questions on whether a cyber-attack can be carried out on military infrastructure without directly or indirectly affecting civilians. This study will be essential to the research as it will advance that current notions of the principle of distinction do not apply to cyber warfare and require a dedicated framework outlining the application to prevent civilian harm in times of current warfare.

[29]Richardson J, 'Stuxnet as Cyberwarfare: Applying the Law of War to the Virtual Battlefield' SSRN, 2011, 30—https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1892888 on 15 September 2024.

[30]Deibert R, Rohozinski R,Crete-Nishihata M, 'Cyclones in cyberspace: Information shaping and denial in the 2008 Russia–Georgia war' 43 *Security Dialogue* 1,2012, 8.

The case study carried out by Csaba Krasznay involves the case of the Not Petya attack in 2017. The Not Petya attack constituted malware masquerading as ransomware on Ukraine and later foreign companies with collateral damage in France, the United States, Germany, Italy and Poland, among other countries. The study outlines the attack as having interrupted banking, power, airports and metro services, consequently causing hundreds of millions of dollars in damage. The study also references the case of *Wannacry* where there were indirect deaths caused as a result of non-functioning IT systems in hospitals. Krasznay further references attribution as the first step to the deterrence theory.[31]

This research will use this study to support the idea that attribution of attacks poses a problem in the regulation of cyber warfare. A dedicated framework is needed to deal with the complexities of attribution among other elements of cyber warfare, which are more complex and cannot be fully broken down by the current IHL framework and adequately regulate the same. The study also brings in the element of the attack on civilian infrastructure and the difficulty distinguishing the same when it comes to internet infrastructure. This will be essential for this research as the principle of distinction is one of the major principles of IHL, which cannot adequately guide cyber warfare with the current framework.

Challenges and Limitations of the Current Legal Framework in Addressing Cyber Warfare

Elizabeth Mavropoulou explains that civilian and military infrastructure are interrelated and one and the same thing and therefore poses an obstacle in classifying the object and effectively applying the basic rule of targeting, the principle of distinction. [32] The paper by Gisel, Rodenhauser and Dormann also stresses the interconnectedness of civilian and military objects and the challenges it poses in applying IHL to military operations that inadvertently affect

[31]Krasznay C, 'Case study: The NotPetya campaign' ResearchGate, 2021, 485—https://www.researchgate.net/publication/353072644_Case_Study_The_NotPetya_Campaign .

[32] Mavropoulou E, 'Targeting in the Cyber Domain: Legal Challenges Arising from the Application of the Principle of Distinction to Cyber Attacks' Journal of Law and Cyber Warfare ,2015, 26-https://www.jstor.org/stable/26441253?seq=3 on 15 September 2024.

civilian infrastructure.[33] The paper further discussed the potential for long-delayed cyber-attack effects and gave examples of logic bombs. According to Mavropoulou, this complicates the understanding of when execution occurs and raises questions about accountability and the duration of its effects. The paper further discusses the legal status of persons involved in COs and the criteria for determining 'direct participation' in hostilities. This status is important in distinguishing lawful targets in armed conflict. [34] This research shall use the paper, and challenges pointed out by Elizabeth Mavropoulou to show the impossibility of the consistent application of principles of IHL, such as the principle of distinction. This shall advance the thought that the principles would be required to be specifically interpreted and codified concerning cyber warfare to be correctly understood in the same and objectively and consistently applied in different situations.

The paper by Gisel, Rodenhauser and Dormann discusses the ambiguity surrounding what constitutes a cyber-attack thus complicating the legal framework. The paper also raises concerns about the protection of civilian data from harmful COs.[35] This ambiguity is also stated in the paper by Talbot in that it complicates the application of principles such as the principles of proportionality and the requirement for precaution.[36] It raises debate on whether civilian data should enjoy similar protections as their objects due to data not necessarily fitting the description of objects. This further complicated the legal landscape. The authors express concern that the interpretation of existing IHL could lead to gaps in civilian protection. The author introduces the question of whether new rules would be needed to address the gaps and build on the legal

[33] Gisel L, Rodenhauser T and Dormann K, 'Twenty years on: International humanitarian law and the protection of civilians against the effects of cyber operations during armed conflicts' International Review of the Red Cross, 2020, 8 -https://international-review.icrc.org/sites/default/files/reviews-pdf/2021-03/twenty-years-ihl-effects-of-cyber-operations-during-armed-conflicts-913.pdf on 14 September 2024.

[34]Mavropoulou E, 'Targeting in the Cyber Domain: Legal Challenges Arising from the Application of the Principle of Distinction to Cyber Attacks' Journal of Law and Cyber Warfare ,2015, 23-https://www.jstor.org/stable/26441253?seq=3 on 15 September 2024.

[35]Gisel L, Rodenhauser T and Dormann K, 'Twenty years on: International humanitarian law and the protection of civilians against the effects of cyber operations during armed conflicts' International Review of the Red Cross, 2020,3-https://international-review.icrc.org/sites/default/files/reviews-pdf/2021-03/twenty-years-ihl-effects-of-cyber-operations-during-armed-conflicts-913.pdf on 14 September 2024.

[36]Jensen E, 'Cyber Attacks: Proportionality and Precautions in Attack' United States Naval War College, Volume 89, 89 INT'L L. STUD. 198 , 2013, 3
https://digital-commons.usnwc.edu/cgi/viewcontent.cgi?article=1029&context=ils on 15 September 2024.

framework.[37] To ensure civilian protection, which is one of the main aims of IHL, cyber warfare would require a dedicated framework to streamline and simplify the legal landscape of the same and offer civilian protection where the same would not be possible due to ill-fitting definitions under current IHL.

The paper by Talbot introduces the element of feasibility, which is a subjective element to the obligations of states, thus making objective accountability in COs difficult. The paper also notes the lack of consensus and established norms, which makes the prediction of the interpretation of the laws in the future difficult. [38]This research shall use this paper to further the idea that the lack of consensus prevents the consistent and objective application of IHL and thus makes it difficult to achieve the same aims effectively.

This review has explored the application of IHL to cyber warfare, highlighting the complexities and inadequacies of using existing frameworks to govern this evolving domain. The analysis of scholarly debates and case studies, such as Stuxnet, the Russia-Georgia War, and the NotPetya attack, reveals significant challenges in applying fundamental IHL principles, including distinction, proportionality, and attribution, to COs, principles to which are pivotal in the application of IHL. The blurred lines between civilian and military targets in cyberspace, coupled with the unique characteristics of cyberattacks, underscore the need for a dedicated framework regulating cyber warfare and ensuring the protection of civilians effectively.

1.10 Research methodology

This research shall rely on the use of doctrinal legal research methodology. This research shall make use of primary and secondary sources. The primary sources will be the Geneva Conventions of 1949 and the additional protocols of 1977. Secondary sources include online journals, articles, and thesis and research papers. The research shall analyse the specific legal

[37] Gisel L, Rodenhauser T and Dormann K, 'Twenty years on: International humanitarian law and the protection of civilians against the effects of cyber operations during armed conflicts' International Review of the Red Cross, 2020,15-https://international-review.icrc.org/sites/default/files/reviews-pdf/2021-03/twenty-years-ihl-effects-of-cyber-operations-during-armed-conflicts-913.pdf on 14 September 2024.

[38]Jensen E, 'Cyber Attacks: Proportionality and Precautions in Attack' United States Naval War College, Volume 89, 89 INT'L L. STUD. 198 , 2013, 16 https://digital-commons.usnwc.edu/cgi/viewcontent.cgi?article=1029&context=ils on 15 September 2024.

regulations and principles in place and their applicability to cyber warfare in the modern age. This is the most appropriate methodology in this instance as the problem has overarching influence on the sociopolitical economy, and the methodology would allow for the deep analysis of current doctrinal stands and aid in concluding the need for a dedicated legal framework as opposed to the application of current general rules.

1.11 Limitations

This research is limited to studying existing principles and definitions concerning cyber warfare under IHL. It is concerned with analysing the application of these principles in recent years as well as specific cases related to the conduct of states in instances of conflict involving cyber interfaces. A potential limitation of this study is the absence of precedent in the International Judicial System concerning violations of the principles of war in the context of cyber warfare.

1.12 Chapter breakdown

The introductory chapter lays the foundation. It gives the background of the research and outlines the relevance of IHL to modern conflict and specifically, cyber warfare. It explains the significance of the study with regards to the legal ambiguities surrounding cyber conflict. Chapter one defines the research problem, objectives, and research questions that guide the study. Further, it discusses the theoretical frameworks and the methodology used in the exploration of the topic.

The second chapter examines the applicability of existing IHL to COs. The chapter delves into the extent to which IHL principles and guidelines apply to cyber warfare. It examines key articles of the Geneva Conventions along with other treaties and agreements relevant under IHL to examine whether current laws sufficiently regulate COs in the instance of armed conflict. It discusses potential gaps in the legal framework to as well determine the sufficiency or consequent insufficiency of current laws.

Chapter three analyses real-world cases of armed conflict involving. It reviews instances for example, the Stuxnet attack, the Russia-Georgia war, and the cyber attacks in Albania to evaluate how they were conducted and whether they complied with IHL. The chapter identifies practical as opposed to possible theoretical challenges that could be encountered in the application of current laws to COs. The chapter provides insight into how the case studies illustrate the growing need for legal framework specifically tailored to COs.

The fourth chapter evaluates the challenges and limitations of applying the existing legal framework to cyber warfare. The chapter analyses specific issues arising from the application of IHL to COs for example, attribution and the limits that have arisen in application of the current framework to COs. The chapter will then conclude that a specific and dedicated framework would be necessary deal with the limits placed as a result of the current laws.

The fifth chapter summarizes the research findings and conclusions. It draws on these to argue that the current framework is insufficient and finally makes recommendations for future research and for strengthening the legal framework regarding COs.

CHAPTER TWO

THE APPLICABILITY OF EXISTING INTERNATIONAL HUMANITARIAN LAWS TO CYBER-WARFARE

2.1 Peremptory norms of general international law

A peremptory norm of general international law or jus cogens is a norm accepted and recognised by the global community of States a norm from which no derogation is permitted and which can be modified only by a subsequent norm of general international law having the same character. They reflect and protect the fundamental values of the international community and thus are universally applicable.[39] Jus cogens norms are non-derogable and thus form the highest form of laws in International Law and therefore, IHL as well. Some of these norms that the International Law Commission has in the past referred to as peremptory norms are 'the prohibition of aggression, genocide, crimes against humanity, racial discrimination and apartheid, slavery, torture, self-determination and the basic rules of IHL.' The basic rules of IHL can be drawn from the definition of IHL itself. IHL is referred to as, 'the branch of International Law that limits the use of violence in armed conflict by sparing those who do not or no longer directly participate in hostilities as well as by restricting it to the amount necessary to achieve the aim of the conflict which can weaken the military potential of the enemy.' The basic principles drawn are the principle of distinction between civilians and combatants, the prohibition to attack those hors de combat, the prohibition to inflict unnecessary suffering, the principle of necessity and the principle of proportionality. [40] These principles apply to new methods ,such as cyber warfare, as they apply to traditional forms under IHL.[41]

[39]UN International Law Commission (ILC), *Report of the International Law Commission on the work of its seventy-first session (29 April–7 June and 8 July–9 August 2019)*, UN Doc A/74/10, 2019, https://legal.un.org/ilc/reports/2019/english/chp5.pdf on 1 December 2024.

[40]ICRC, 'Fundamentals of IHL,' https://casebook.icrc.org/law/fundamentals-ihl#footnote2_zq0q4gb on 28 November 2024.

[41] International Committee of the Red Cross, *International Humanitarian Law and the Challenges of Contemporary Armed Conflicts*, 2011, <https://casebook.icrc.org/case-study/icrc-international-humanitarian-law-and-challenges-contemporary-armed-conflicts-2011>on 10 November 2024.

It is, however, difficult to apply some of these principles due to cyber objects not fitting into the ordinary meanings as interpreted under IHL. For example, data, being intangible, would not fit in with the ordinary meaning of an object. Additionally, the ICRC commentary on the additional protocols provides for an object being something visible and tangible and hence data would not qualify. [42]

2.2 The UN charter

Article 2 of the UN Charter (UNC) provides for the general principles of IHL. Article 2(1) provides that the UN is based on the principle of sovereign equality of the members. Article 2(4) states, "members shall refrain from threat or use of force against the territorial integrity or political independence of any state or in any manner inconsistent with the purposes of the United Nations." Article 2(7) further provides, "that nothing in the charter should intervene in matters essentially within the domestic jurisdiction of any state or shall require the members to submit such matters to settlement under the charter. However, the principle shall not prejudice the application of enforcement measures under chapter seven."[43] This article provides for the sovereign equality of states and in the cyber context, implies states control over their cyber data and infrastructure and that within their territory. Any unauthorised attack on state cyber infrastructure could violate the principle of state sovereignty.

Article 51 of the UNC provides 'that nothing in the charter shall impair the inherent right of self-defense if an armed attack occurs against a member of the UN until the security council has taken the measures necessary to maintain international peace and security.' It further requires measures taken by members, in self-defense, be reported to the Security Council and that they do not affect the authority of the Security Council to take action to restore international peace and security.[44]

---

[42] Huang Z and Ying Y, 'The application of the principle of distinction in the cyber context: A Chinese perspective' International Review of the Red Cross, March 2020 https://international-review.icrc.org/articles/principle-of-distinction-cyber-context-chinese-perspective-913#footnote149_5dif7ti on 15 November 2024.

[43] Article 2, Charter of the United Nations, 26 June 1945, 1 UNTS XVI.

[44] Article 51, Charter of the United Nations, 26 June 1945, 1 UNTS XVI.

2.3 The Geneva Conventions and the Additional Protocols

Article 1 of the first Geneva Convention mandates 'respect for the Geneva Conventions in all circumstances.'[45] Article 2 gives the scope of the same as, "applying to all cases of declared war or armed conflict even if the state of war is not recognised by one of them and applies in all cases of occupation of territory even if the occupation is not met with armed resistance." These articles would consequently also apply in the same way to cases of cyber warfare used in these situations.

The Fourth Geneva Convention majorly provides for the protection of civilians in wartime. Article 4 of the same provides for 'persons protected by the convention.' Article 4 states these to be 'those who at any given moment and in any manner find themselves in case of conflict or occupation and in the hands of a party to the conflict or occupying power of which they are not nationals.' Article 4 provides that, "nationals of a state which is not bound by the convention are not protected by it and nationals of a neutral state who find themselves in the territory of a belligerent state shall not be regarded as protected persons while the state of which they are nationals had normal diplomatic representation in the state in whose hands they are."[46] This article defines protected persons and if cyber means used in warfare fall under the criteria of harm to these protected persons, IHL would apply and the civilians would be protected under the same.

Articles 27 and 33 provide for the protection of the civilian population. As outlined in Article 27, 'protected persons are entitled in all circumstances to respect for their persons, honour, family rights, religious convictions and practices and their manners and customs.' The article provides that 'they shall at all times be treated humanely and protected against all acts of violence, threats or insults and public curiosity and without discrimination on grounds of race,

[45] Article 1, Geneva Convention for the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field (1949), 75 UNTS 31.

[46] Article 4, Geneva Convention relative to the Protection of Civilian Persons in Time of War (1949), 75 UNTS 287.

religion or any other grounds.'[47] The provisions in Article 33 provide for the 'prohibition against pillage and reprisals against protected individuals and their property.'[48]

Article 53 of the Fourth Geneva Convention provides "that any destruction by the occupying power of real or personal property belonging to private persons, the state or other public authorities or social or cooperative organisations is prohibited except where destruction is rendered absolutely necessary by military operations."[49] Cyberinfrastructure consists of the hardware, software, computer network and communication.[50] These can be qualified as an individual or state's property and thus would receive protection whereby an attack over a cyber network would lead to the destruction of the same.

Article 19 of the first Geneva Convention as well as article 12 of Additional Protocol I provides for the protection of medical units and transport.[51] Cyberattacks on hospitals, healthcare facilities or medical transport teams, for example, as seen in the case of *Wannacry*, could violate this protection especially if the attack has adverse effects on the ability of these units to function and consequently causes loss of life.

The Geneva Conventions are said to apply to cyber warfare in the same way they do to traditional armed conflict.[52] The additional protocols provide 'that in the study, development, acquisition or adoption of a new weapon, means or method of warfare, a high contrasting party is under the obligation to determine whether employment would be prohibited by the protocol or any other rule of international law.' [53]

[47] Article 27, Geneva Convention relative to the Protection of Civilian Persons.

[48] Article 33, Geneva Convention relative to the Protection of Civilian Persons.

[49] Article 53, Geneva Convention relative to the Protection of Civilian Persons.

[50] Shi X, Huang M, ' Cyberinfrastructure and High-Performance Computing' in Huang B, Comprehensive Geographic Information Systems, Elsevier, United States, 2018, 341.

[51] Article 19, Geneva Convention for the Amelioration of the Condition of the Wounded and Sick.

[52] International Committee of the Red Cross, *International Humanitarian Law and the Challenges of Contemporary Armed Conflicts*, 2011, [https://casebook.icrc.org/case-study/icrc-international-humanitarian-law-and-challenges-contemporary-armed-conflicts-2011] on 10 October 2024.

[53] Art 36, Protocol Additional to the Geneva Conventions of 12 August 1949 (1977)1125.

Additional protocol 1 provides for the rules of an attack in IHL. That is, 'the obligation to direct attacks military and not civilian objects', the 'prohibition of indiscriminate attacks and attacks which would be expected to cause excessive incidental civilian casualties or damages', 'the requirement to take precautions to ensure the first two rules are respected', in particular the 'requirement to minimise incidental civilian damage' and the 'obligation to abstain from attacks if such damage is likely to be excessive to the value of the military objective to be attacked.'[54] It is submitted that these rules operate in the same way whether the attack is carried out using traditional weapons or by reliance on a computer network.

Article 49 of Additional Protocol 1 defines an attack as "a means of violence against the adversary whether it is done in offence or defence." It states that these provisions apply to land, air or sea warfare which may affect the civilian population. Further, it states that it does not affect the rules of international law applicable in armed conflict at sea or in the air.[55] Article 49 provides for the definition of an attack which, if cyber attacks fall under the purview, would determine whether the law of armed conflict would apply to COs. COs that do not result in acts of violence, for example, those aimed at gathering intelligence do not fall under the definition under article 49 under the traditional approach.

Article 51 provides for 'the protection of civilians from military operations.' The same prohibits indiscriminate attacks which could be defined as "attacks not directed toward a specific military objective, those which use a method of combat which cannot be directed at a specific military objective or a method whose effects cannot be limited."[56] This therefore can be concluded as, attacks which are of a nature to strike military objectives and civilians without distinction are prohibited. The article also provides for incidental attacks to be 'those expected to cause incidental loss of civilian life, damage to civilian objects or both which could be considered excessive in relation to the expected military advantage'.[57]

[54] Art 51, Protocol Additional to the Geneva Conventions.
[55] Art 49, Protocol Additional to the Geneva Conventions.
[56] Art 51, Protocol Additional to the Geneva Conventions.
[57] Art 51, Protocol Additional to the Geneva Conventions.

Article 56 of additional protocol 1 provides that 'works or installations containing dangerous forces, namely dams, dykes and nuclear electrical generating stations, shall not be made the object of attack, even where these objects are military objectives, if such attack may cause the release of dangerous forces and consequent severe losses among the civilian population.' Further, it states that 'other military objectives in the same vicinity are not to be made the object of attack if the attack may cause the release of dangerous forces from the works or installations and as a result cause severe losses among the civilian population.'[58]

Article 58 provides for precautions that are to be taken against the effects of attacks. It provides that 'parties undertake to remove civilians and civilian objects from the vicinity of military objectives and take any other necessary precautions to protect the civilian population or objects under their control against the danger that may result from military operations.'[59] This article places an obligation on states to segregate military from civilian objects and for those it cannot segregate the responsibility to protect civilians and their objects from anticipated effects of the attacks.

2.4 The Hague Convention

The Hague Peace Conference adopted 'the convention of land warfare' which was revised in the conference of 1907. The provisions of the conventions serve as the rules of customary international law and therefore binding on states which are not formally parties to the same.[60] This convention is officially known as 'The Convention Respecting the Laws and Customs of War on Land' and the subsequent Regulations concerning the same.

Article 25 of the Hague Convention prohibits attacks on undefended towns and villages which could extend to protecting civilian digital infrastructure from cyber attacks.[61] The convention also contains rules of conduct for belligerents, including the requirement to adhere to the laws

[58] Art 56, Protocol Additional to the Geneva Conventions.

[59] Art 58, Protocol Additional to the Geneva Conventions.

[60] https://ihl-databases.icrc.org/en/ihl-treaties/hague-conv-iv-1907?activeTab= on 4th December 2024.

[61] Art 25, Convention Respecting the Laws and Customs of War on Land, 1907.

and customs of war. This could be interpreted to apply to cyber warfare and therefore suggest that COs should comply with established IHL.

2.5 The Budapest Convention on Cyber Crime

This convention deals with criminal offences carried out over a computer network. This convention deals with cyber crimes committed by parties, including, "illegal access and interception, data or system interference, misuse of devices, computer-related forgery, computer-related fraud and content-related offences."

This convention does not make specific references to the legal regulation of warfare conducted through cyber systems. However, it does not exclude the possibility of being applied to cyber conflict. Since the Budapest Convention establishes a framework for addressing cybercrime, it can, by default, be interpreted to apply to cyber warfare in scenarios where the activities meet the thresholds of criminal conduct outlined in the convention, such as unauthorized access, disruption, or damage to critical systems.

Article 23 of the Budapest Convention provides for the principles of cooperation between parties. It provides for the application of international instruments on international cooperation in, 'criminal matters, arrangements agreed on the basis of uniform or reciprocal legislation and domestic laws for the widest extent, for the purposes of investigation or proceedings concerning criminal offences related to computer systems and data or for the collection of evidence in electronic form of a criminal offence.'[62] This principle could be interpreted to ensure that even if cyber attacks are state-sponsored, the convention should still promote cooperation to address the attacks under the framework of combating cybercrime.

Article 25 of the Convention outlines the 'general principles of mutual assistance', requiring parties to fully cooperate in investigating criminal offenses related to computer systems and data.[63] Article 25 is relevant to the context of cyber warfare as it is in other forms of cybercrime as regulated by the Budapest Convention as even in cases of state-sponsored attacks, mutual

[62] Art 23, Convention on Cybercrime, (2001) No 185.

[63] Art 25, Convention on Cybercrime.

assistance can be crucial in gathering evidence and prosecuting cross-border cyber crimes and COs in time of warfare.

Article 26 provides for the spontaneous sharing of information, that is, without any prior request when obtained by a party within its own investigations and may assist the other party.[64] This spontaneous sharing of information could apply to state-sponsored attacks as well and could facilitate faster responses and prevent further attacks. This could allow states to share intelligence or threat information before a formal investigation begins.

Article 27 provides for the 'procedures related to mutual assistance requests in the absence of applicable international agreements.' It outlines procedures where there is no treaty between two countries and guidance on how states can cooperate on matters related to cybercrime investigations including the sharing of information.[65] This as well could apply in the context of state-sponsored attacks on other states whereby cooperation between states could be achieved through mechanisms in the Budapest Convention.

2.6 International Bill of Right

The 'Universal Declaration of Human Rights', which was made in 1948, was the first agreement made with regards to inalienable human rights. Two treaties were later adopted by the United Nations General Assembly in 1966, that is, the 'International Covenant on Economic Social and Cultural Rights' (ICESCR) and the 'International Covenant on Civil and Political Rights'(ICCPR). The three instruments collectively form the International Bill of Human Rights. The UDHR and the ICCPR are applicable and guide in all instances of warfare, including cyber warfare. Article 12 of the UDHR provides for 'the right to privacy.' This right serves the purpose of 'safeguarding all individuals from arbitrary interference with their privacy, family, home or correspondence, as well as from attacks on their honor and reputation.'

[64] Art 26, Convention on Cybercrime.

[65] Art 27,Convention on Cybercrime.

It also provides everyone with 'the right to protection of the law against these interference or attacks.'[66] The same is present in article 17 of the ICCPR.[67] Although IHL is silent about most socio-economic rights, they must still be respected even in the context of warfare as there is no barrier to applying rules of International Human Rights Law to civilians and combatants.[68] It should however be applied realistically and with consideration of the extraordinary circumstances of armed conflict.[69]

Article 19 of the ICCPR also provides for 'the freedom of expression.' It states 'everyone has the right to hold opinions without information and includes the freedom to seek, receive and impart information and ideas of all kinds and in any media of his choice.' The right is however stated to be limited by law in order to, "ensure respect of the rights or reputations of others as well as for the protection of national security or public order or public health and morals."[70]

2.7 Judicial precedent

Decisions made by the ICJ form part of international law as they aid in the interpretation and development of IHL. Through ICJ jurisprudence, they clarify the principles under international law and assist in defining their scope and application. Judicial decisions strengthen the enforcement of IHL, especially in terms of contemporary challenges facing the same. Landmark decisions, for example that of the Nuclear Weapons Advisory Opinion and the Nicaragua case have contributed significantly to defining the scope and application of principles of IHL.

The case of New Zealand v France, better known as the Nuclear Tests Case, although primarily focusing on the rightness in law of atmospheric nuclear testing, offers insights into how International Law adapts to novel situations and technologies. In the case, Australia sought to

[66] Article 12, Universal Declaration of Human Rights,1948.

[67] Article 17, International Covenant on Civil and Political Rights,1966, 999 UNTS 14668.

[68] Haeck S, 'The rights to privacy and data protection in armed conflict' *International Review of the Red Cross*, 105 (923), 2023, 1160—https://international-review.icrc.org/sites/default/files/reviews-pdf/2023-06/the-rights-to-privacy-and-data-protection-923.pdf .

[69] Haeck S, 'The rights to privacy and data protection in armed conflict,' 1160.

[70] Article 19, International Covenant on Civil and Political Rights.

stop the nuclear tests which France was carrying out in the South Pacific, arguing their harmful effects to the atmosphere violated international law[71]. This demonstrates how existing legal principles, even those developed before the advent of certain technologies, can be applied to address novel challenges.

The judgement in the case emphasizes the importance of states' public statements and their potential to create legally binding obligations. France's public declarations of intent to cease atmospheric nuclear testing were deemed sufficient to resolve the dispute, despite not being formally addressed to Australia or requiring acceptance by any other state. This suggests that states' pronouncements on matters of international concern can carry significant weight and legal consequences, even in the absence of formal agreements.

Although not explicitly discussed, the approach of the court in the Nuclear Tests case suggests a possible framework for applying international law to emerging technologies like cyber warfare. The court's willingness to consider France's unilateral declarations as legally binding demonstrates a flexible approach to interpreting international obligations. This flexibility could be crucial in addressing the unique challenges of cyber warfare, which often transcends traditional legal boundaries.

The principles highlighted in the sources, particularly the application of existing legal framework to novel situations and the potential of states' public pronouncements to create legal obligations, could be relevant in the context of cyber warfare. Just as the court applied existing laws to address the novel issue of atmospheric nuclear testing, similar principles could be employed to regulate the use of cyber weapons and ensure compliance with IHL.

2.8 The Tallinn Manual

The Tallinn Manual 2.0 analyses how existing international law applies to cyber warfare. It provides some clarity on how existing frameworks apply to COs. It however is non-binding. The manual takes a consequence-based approach in defining COs. It provides ‘that the law of armed conflict applies to COs conducted during armed conflict and thus these operations must

[71] Nuclear Tests (Australia v. France), Judgment, I.C.J. Reports 1974, p. 253.

comply with the principles of International Humanitarian Law.'[72] It also states, "that the law of armed conflict applies to COs when they reach a specific threshold, such as that of causing physical injury."[73] This shows that COs can have consequences even if they do not result in physical harm.

According to Rule 5 of the manual, a state is held responsible for ensuring that, "its territory or government-controlled digital infrastructure is not used for COs that violate the rights of other states or cause significant harm."[74] The manual additionally provides that the traditional view of geographic boundaries of armed warfare is increasingly blurred, especially in terms of cyber warfare, which has effects breaching further than the physical battlefield.[75]

It further speaks on the question of combatant status and COs and states that individuals in the armed forces do not lose combatant status by engaging in COs, provided they continue to meet the requirements under international law. The manual also examines the criminal responsibility of commanders for ordering COs that would constitute war crimes.[76] It restates that it is possible for commanders to be held criminally liable for operations that 'violate international law' even if they did not personally participate in the operation. This is possible where they ordered the crime, should have known about the crime or they did not take all reasonable and available measures in prevention of the crime or to punish those responsible.[77]

2.8 Conclusion

Existing IHL framework, including 'The Geneva Conventions', 'Additional Protocols', and the 'Hague Convention', is generally considered 'applicable to cyber warfare' if COs reach the threshold of armed conflict. However, challenges arise due to the intangible nature of cyber objects, such as data, which complicates their classification under IHL protections. The

[72] Schmitt M, Tallinn Manual on the International Law Applicable to Cyber Warfare, 2 ed, Cambridge University Press, Cambridge, 2017,75.
[73] Schmitt, Tallinn Manual, 75.
[74] Schmitt, Tallinn Manual, 27.
[75] Schmitt, Tallinn Manual, 79.
[76] Schmitt, Tallinn Manual, 91.
[77] Schmitt, Tallinn Manual, 92.

Additional Protocols emphasize the need for ongoing assessment of new weapons, including cyber weapons, to ensure compliance with IHL principles. The Tallinn Manual adopts a consequence-based approach, although it is non-binding. It highlights that COs with real-world effects can trigger IHL provisions. The Budapest Convention on Cyber Crime, while focused on cyber-related criminal activities, may also apply when cyber warfare overlaps with criminal conduct. Despite broad agreement on IHL's applicability, further clarification is needed on key issues, such as defining the threshold for cyber warfare as armed conflict, protecting data under IHL, and determining direct participation in hostilities in the cyber domain.

CHAPTER 3

HOW INSTANCES OF CYBER OPERATIONS HAVE BEEN ADDRESSED UNDER CURRENT LEGAL FRAMEWORKS

The evolving landscape of cyber operations poses complex challenges to existing legal frameworks. Traditional international law was developed with conventional warfare in mind, leaving significant gaps in addressing cyberattacks. These gaps are particularly evident when considering the attribution of responsibility, the application of legal thresholds for armed attacks, and the ambiguity in defining cyber techniques as weapons. In examining key instances of COs, such as the Stuxnet worm, the NotPetya attack, the Russia-Georgia war, and the cyberattacks in Albania, exploration can be done as to how they have been addressed under current legal frameworks if at all they have been. By analysing these case studies, the legal, diplomatic, and practical reactions by affected states and the international community can also illustrate the extent to which existing mechanisms have been adequate or inadequate in addressing the unique challenges posed by COs.

3.1. Stuxnet

Discovered in June 2010, Stuxnet was a computer worm that infected over 60,000 computers, with more than half located in Iran. It also affected systems in India, Indonesia, and China. The worm spread through intermediary devices, such as USB sticks, and infiltrated in order to control targeted systems.[78] The worm was designed to target frequency converter drives, which were made in Iran and Finland, by altering the frequency of the electric current that powered the centrifuges. This therefore caused damage to the machines. Experts opined that the target was the uranium enrichment centrifuges at Natanz, although initial reports indicated that the Bushehr power reactor was the target of the attack.[79] This attack was believed to have set a precedent on the use of Cos and demonstrated the potential for cyber tools to be used in a military context. It also showed, for the first time, the destructive capabilities of the cyberspace.[80]

---

[78]Farwell J and Rohozinski R, 'Stuxnet and the future of cyber war' *Survival*, 2011, 23 —<https://www.tandfonline.com/doi/epdf/10.1080/00396338.2011.555586?needAccess=true> on 9 February 2025.

[79] Farwell J and Rohozinski R, 'Stuxnet and the future of cyber war,' 24.

[80] Crawford J and Gunn A, 'The ethics of automation in digital service work' *Journal of Business Research* 140, 2024, 75—<https://www.sciencedirect.com/science/article/abs/pii/S026736492400075X.>

After the attack, Iran refused to admit the seriousness of the same and denied any negative effects on its nuclear program as a result of the same. State officers and leaders of the Atomic Energy Department in Iran insisted that operational setbacks resulted from technical difficulties and further denied any claim of an attack. Further, the Iranian government remained quiet during the period within which the attack took place, which could lead to the reasonable conclusion that Iran did not consider Stuxnet to be an armed attack and therefore, not garnering punishment under International law. The decision by Iran not to publicly acknowledge Stuxnet as a cyberattack or formally accuse any state prevented Iran from pursuing legal recourse or retaliation under International law.

Ultimately, using Stuxnet was not seen as an armed attack due to the inability to attribute the same. This is because the designer of the weapon remained unknown and unconfirmed. The concealing of the attacker's identity rendered Article 51 ineffective with this attack and Iran's possible action. [81] Further, it would have been difficult and meaningless for Iran to make any defensive action due to the lack of a specific entity to direct the same toward.[82] Additionally, attempts to enact Security Council resolutions under Article 39 of the UNC would be at the mercy of the veto power possessed by the five permanent members of the Security Council. This poses a problem as the US for example, would not willingly permit Security Council action against its own infection.[83]

Ultimately, the UNC and Law of Armed Conflict were incapable of regulating the attack primarily due to challenges attributed to the attack and the lack of established frameworks for cyber warfare at the time.[84] Additionally, the standard of a claim being supported by convincing evidence being necessary as set out in the Nicaragua case and the Armed activities case in

[81]Masciotra C, 'Cybersecurity challenges and disconnects in policy implementation' *Political Science Graduate Student Association Journal* 3, 2020,111—<https://www.concordia.ca/content/dam/artsci/polisci/docs/psgsa/Vol%203%20ChallengesDisconnects.pdf#page=82.>

[82] Masciotra C, 'Cybersecurity challenges and disconnects in policy implementation',111.

[83] Masciotra C, 'Cybersecurity challenges and disconnects in policy implementation', 92.

[84] Masciotra C, 'Cybersecurity challenges and disconnects in policy implementation',82.

instances involving the use of force also poses a challenge for states seeking legal redress for cyberattacks to meet, given the inherent difficulties in attribution.[85]

3.2 NotPetya Attack

The NotPetya attack began on the 27th June, 2017. It was a cyberattack primarily targeted at Ukraine but spread globally causing damage worth billions of dollars. The attack was initially disguised as ransomware as it demanded 300 dollars in Bitcoin to unlock the infected machines, but it later became known that data recovery was not possible. This showed that the initial purpose may have been destruction, not financial gain. The attack is believed to have begun through a compromised software update of Ukrainian tax software. The attackers gained access and could distribute the malicious code as a legitimate update. The malware used the vulnerability previously exposed by the WannaCry ransomware to spread across networks. [86]NotPetya disrupted critical infrastructure in Ukraine and impacted multinationals such as Maersk, causing significant financial losses.[87]

Following the attack, many countries, including the US, Denmark, Lithuania and Estonia, officially accented the Russian military. This marked a significant step in holding nation-states accountable for malicious cyber activities. The attribution by these states included the issuance of a strong condemnation of Russia's actions and highlighted the disregard for Ukraine's sovereignty and the significant economic damage inflicted. The states also highlighted the need of states to be responsible when acting in the cyberspace.[88]

The US Treasury Department further imposed sanctions on five Russian entities and three individuals, blocking their assets and prohibiting transactions with them. The European Union also established a framework to impose targeted sanctions in response to cyberattacks from

[85]Aravindakshan S, 'Cyberattacks: a look at evidentiary thresholds in International Law' *Indian Journal of International Law*, 2020, 290—https://link.springer.com/article/10.1007/s40901-020-00113-0 .

[86]Krasznay C, 'Case study: The NotPetya campaign' ResearchGate, 2021, 485—https://www.researchgate.net/publication/353072644_Case_Study_The_NotPetya_Campaign .

[87] Krasznay C, 'Case study: The NotPetya campaign' ResearchGate, 2021, 486.

[88] Krasznay C, 'Case study: The NotPetya campaign' ResearchGate, 2021, 493.

outside the EU. This was aimed at deterring future attacks and providing a response mechanism within the EU.[89] The US Department of Homeland Security and FBI further created the Grizzly Steppe initiative to investigate and attribute Russian cyberattacks, including the NotPetya attack. It analysesd the tactics and procedures used by Russian, possibly state-sponsored, actors in targeting critical infrastructure and government entities.[90] Western countries were also more proactive in deterring cyberattacks through retaliation. However, many of the retaliatory acts were covert, such as the US cyberattack on the Russian power grid in 2019. Little legal action was taken about the attack. Some of the actions taken included the conviction of a Ukrainian citizen for spreading a version of the ransomware.[91]

3.3. Russia-Georgia war

The 2008 Russia-Georgia conflict was one of the first instances of COs integrated into conventional armed conflict. The targets of the attacks were the Georgian government websites and essential online services. These included the president's website, the Ministry of Foreign Affairs and the National Bank. The main tactic used was Distributed Denial of Services(DDoS). The attacks overwhelmed a target server, making the same inaccessible to legitimate users. The DDoS attacks interfered with the ability of the government to put out communication to its citizens and subsequently, the international community. Additionally, the National Bank was forced to stop electronic services as a result of the attacks which impacted the country's financial stability. Furthermore, some websites were defaced with pro-Russia messages. The DDoS coincided with the escalation of conventional conflict, which could lead to the conclusion that the two resulted from coordination. [92]

[89] Krasznay C, 'Case study: The NotPetya campaign' ResearchGate, 2021, 490.

[90] Krasznay C, 'Case study: The NotPetya campaign' ResearchGate, 2021, 491.

[91] Krasznay C, 'Case study: The NotPetya campaign' ResearchGate, 2021, 494.

[92] Deibert R, Rohozinski R, Crete-Nishihata M, 'Cyclones in cyberspace: Information shaping and denial in the 2008 Russia-Georgia war' *Security Dialogue*, 2012, 15—https://www.jstor.org/stable/pdf/26301960.pdf?refreqid=fastly-default%3A9e16260fbc4a538cda9e61e3d8b64f05&ab_segments=&initiator=&acceptTC=1.

Attribution of responsibility for the attacks was challenging as there was debate whether it was the Russian government was responsible or Russian independent patriotic hackers. Unfortunately, there was no definitive evidence to confirm either scenario.[93] Additionally, although multiple countries named Russia responsible for the cyberattacks on Georgia, there was no evidence publicly disclosed. This was taken as a lack of evidence and undermined confidence in the claims of public attribution made by the different countries. This negated any possible beneficial outcomes. It further became difficult to take legal action for malicious cyber activity as Georgia would be required to meet the standard of proof in provision of evidence,in International Law, which was difficult.[94] The lack of clear legal precedent and the difficulty in defining cyber techniques such as DDoS attacks as weapons under international law made legal redress more difficult. This created ambiguity in determining the legality of actions taken by either side.[95] The problems collectively hindered any concrete legal actions that could be taken regarding the attacks.

However, as a response, Georgian authorities implemented internet filtering and blocked access to Russian websites and online resources. Unfortunately, The filtering of information resulted in an information blackout in Georgia and increased confusion and panic. Georgia sought assistance from Estonia, Lithuania and Poland to mitigate the DDoS attacks, and Estonian officials connected them with cybersecurity professionals who provided consultations.[96]

3.4 Cyber Attacks in Albania

They were carried out by Iranian actors against Albanian organizations and government institutions with the intent to cripple essential infrastructure. These included telecommunications, transportation, law enforcement and government portals. The attacks

[93] Deibert R, Rohozinski R, Crete-Nishihata M, 'Cyclones in cyberspace: Information shaping and denial in the 2008 Russia-Georgia war' *Security Dialogue*, 2012, 17.

[94]Aravindakshan S, 'Cyberattacks: a look at evidentiary thresholds in International Law' *Indian Journal of International Law*, 2020, 290.

[95]Korns S and Kastenberg J, 'Georgia's Cyber Left Hook' *Parameters 38*, 2008, 63—https://press.armywarcollege.edu/cgi/viewcontent.cgi?article=2455&context=parameters.

[96] Deibert R, Rohozinski R, Crete-Nishihata M, 'Cyclones in cyberspace: Information shaping and denial in the 2008 Russia-Georgia war' *Security Dialogue*, 2012, 11.

began with access to the Albanian government's network and email exfiltration from the compromised network which took place between October 2021 and January 2022.[97] A separate Iranian state-sponsored actor used websites and social media platforms to leak information that had been exfiltrated months earlier. The assessment by Microsoft connected the initial access and exfiltration to 'EUROPIUM', a group associated with the Ministry of Intelligence and Security in Iran.[98] The attack also involved email harvesting, a destructive campaign that destroyed data contained in the Albanian government computer system, disruption of government services, a cyber attack on the Albanian parliament in December 2023 and the alleged destruction and leaking of 100 terabytes of Albanian geographic information system and population data.[99]

Subsequent reports revealed that multiple cyber actors were involved in the attacks, including Homeland Justice. Albanian researcher Gentian Progni suggested that Iran was not acting independently and may have been collaborating with Russia. He mentioned that the actors operated in Russian territory, the leaked information was seen to be originating from a Russian website and pro-Russia propaganda was being spread through telegram channels. Bulgaria, Kosovo Montenegro and North Macedonia were also hit by cyberattacks by Russian-speaking groups during the same period of the attacks on Albania. Progni's point was further asserted by the ongoing collaboration between Russia and Iran. This included a cyber defence cooperation diplomacy agreement beginning in June of 2015 and another cyber agreement in January 2021 stipulating broad cybersecurity cooperation.[100] This attack as was seen in the Russia- Georgia war is as well seen to be in possible contravention with the principle of necessity.

[97] Pavel T, "The Iranian Cyberattacks in Albania: Actors, Tactics, Targets" https://www.journaldot.pl/pdf-196772-117133?filename=The%20Iranian%20Cyberattacks.pdf.

[98] https://www.microsoft.com/en-us/security/blog/2022/09/08/microsoft-investigates-iranian-attacks-against-the-albanian-government/ on 9 February 2025.

[99] Pavel T, 'The Iranian Cyberattacks in Albania: Actors, Tactics, Targets'.

[100] Pavel T, 'The Iranian Cyberattacks in Albania: Actors, Tactics, Targets'.

Homeland Justice later claimed credit for the cyber attack on Albanian government infrastructure in July of 2022. [101]

In response to the cyber attacks, on September 7th, 2022, Albania severed diplomatic relations with Iran. This action demonstrated the seriousness with which Albania viewed the attacks. Further, countries such as the US condemned the attacks, which had no direct legal effect, but it put diplomatic pressure on Iran.

3.5 Principles of IHL and the cyber attacks

There are principles that should be considered with regards to the legality of these cyber attacks. However, application of these principles becomes difficult due to the inherent nature of the cyberspace to be interconnected. For instance, the principle of distinction dictates that belligerent parties in an armed conflict may only target combatants and military objectives..[102] This prohibits attacks extending to civilians and by extension, attacks which do not have a specific military target.[103] Disruption of civilian and government services was seen in the attack on Georgia and those in Albania. The case of NotPetya is however slightly different as this attack was inherently made to be indiscriminate and therefore was in direct conflict with the principle of distinction.[104] Additionally, the principle of proportionality forbids attacks that are expected to result in loss of life, injury, or damage that is excessive in comparison to the anticipated direct military advantage.[105] When it comes to the cyberspace, it is necessary but difficult to weigh the damage as against the advantage gained due to the plane of conflict being

[101] https://www.cisa.gov/news-events/cybersecurity-advisories/aa22-264a#:~:text=In%20June%202022%2C%20HomeLand%20Justice,cyber%20attack%20on%20their%20website on 9 February 2025.

[102] Art 48, Protocol Additional to the Geneva Conventions.

[103] Fraczek J, 'Is IHL Fit to Deal with the Ones and Zeroes? Analyzing the Application of the Principles of Distinction, Proportionality and Precautions to Cyber Operations' Glasgow Centre for International Law and Security, GCILS Working Paper Series 20, 2024, 13-- https://gcils.org/gcils-publications/gcils-working-paper-series/working-paper-series-2024/ on 9 February 2025.

[104] Fraczek J, 'Is IHL Fit to Deal with the Ones and Zeroes? Analysing the Application of the Principles of Distinction, Proportionality and Precautions to Cyber Operations,' 14.

[105] Fraczek J, 'Is IHL Fit to Deal with the Ones and Zeroes? Analysing the Application of the Principles of Distinction, Proportionality and Precautions to Cyber Operations,' 25.

different. The damage or injury caused when engaging in cyberwarfare is on infrastructure and online services which is difficult to assess as proportional or otherwise in terms of military advantage gained or anticipated. For example, it is difficult to analyse the NotPetya attack which caused significant financial losses to private entities in relation to the military advantage gained by Russia in the conflict.

It is also necessary to consider the principle of military necessity with regards to these attacks. This principle permits actions required to fulfill a legitimate military objective, which in armed conflict, means diminishing the military capabilities of opposing parties.[106] Application of this principle is dependent on whether cyber warfare would be considered an "armed conflict" or constituting an armed conflict and therefore any cyber attack would be legitimate if it weakened the military capacity of the other parties. In the case of the NotPetya attack and the Russia-Georgia war, there was mass economic disruptions in both Ukraine and Georgia and their respective governments which could be seen to diminish the economic capacity of their militaries as well.

3.6. Conclusion

The case studies of Stuxnet, NotPetya, the Russia-Georgia war, and the Albanian cyberattacks underscore the inaction taken concerning cyberattacks due to the significant challenges in addressing COs under current legal frameworks. Attribution of responsibility remains a persistent obstacle, as evidenced by the difficulty in identifying perpetrators or linking attacks to specific states with sufficient evidence to meet international legal standards. Furthermore, the absence of clear definitions and established norms for cyber techniques exacerbates the difficulty of applying existing laws to COs. Despite these challenges, these attacks show effort to shape responses to cyberattacks, including multilateral sanctions, public attribution, and efforts to define global standards for responsible conduct in cyberspace. However, these

[106] https://casebook.icrc.org/a_to_z/glossary/military-necessity#:~:text=The%20%E2%80%9Cprinciple%20of%20military%20necessity,prohibited%20by%20international%20humanitarian%20law on 8 February 2025.

measures often rely more on political and diplomatic pressure than enforceable legal mechanisms.

CHAPTER 4

CHALLENGES AND LIMITATIONS OF APPLYING THE EXISTING LEGAL FRAMEWORK TO CYBER-WARFARE

Several challenges and limitations come to light when applying existing frameworks to cyber warfare:

4.1. Difficulty applying the Laws of Armed Conflict

4.1.1 Ambiguities in definitions in International Humanitarian Law

The ambiguities present in International Law pose a challenge in applying the same to COs. This is seen, for example, in defining an attack in the specific context of COs. Principles under the Law of Armed Conflict, such as the principle of proportionality only apply in situations of attack, which are also understood as acts of violence. [107] Under traditional understandings in IHL, acts of violence have been seen to mostly focus on the use of force.[108] However, it is not clear whether cyber attacks would be a use of force under article 2(4) of the UNC. Additionally, COs can be seen to cause harm without necessarily any physical force being used. This can be seen, for example in the attack launched by Russia on the Georgian government systems and communication networks. This attack although not constituting physical force caused great harm to Georgia as its government was unable to communicate with its citizens and international community.[109] There has, therefore, resulted in a scholarly division where some believe that any cyber operation which causes the same damage as a physical attack should fall under an attack, while others believe that the definition should be broadened to include the disruption of the

[107] Jensen E, 'Cyber Attacks: Proportionality and Precautions in Attack' United States Naval War College, Volume 89, 89 INT'L L. STUD. 198 , 2013, 200 https://digital-commons.usnwc.edu/cgi/viewcontent.cgi?article=1029&context=ils on 6 January 2025.

[108] Mavropoulou E, 'Targeting in the Cyber Domain: Legal Challenges Arising from the Application of the Principle of Distinction to Cyber Attacks' Journal of Law and Cyber Warfare ,2015, 29 - https://www.jstor.org/stable/26441253?seq=3 on 6 January 2025.

[109] Deibert R, Rohozinski R, Crete-Nishihata M, 'Cyclones in cyberspace: Information shaping and denial in the 2008 Russia-Georgia war' *Security Dialogue*, 2012, 15— https://www.jstor.org/stable/pdf/26301960.pdf?refreqid=fastly-default%3A9e16260fbc4a538cda9e61e3d8b64f05&ab_segments=&initiator=&acceptTC=1.

functionality of critical infrastructure.[110] For example, Stuxnet is likely to be considered a 'use of force' and therefore qualify as an armed attack as it damaged the centrifuges at Natanz.[111] There is also a lack of agreement on whether temporary or reversible damage would qualify as an attack.[112] This lack of consensus is very harmful as it has caused a potential gap in legal protection where cyber attacks not considered "attacks" by some interpretations occur.[113] Further, determining whether an attack is a low-level aggression or a use of force is challenging due to factors such as duration and use of force which must be considered.[114]

In applying the prohibition on the use of force under the UNC to cyberattacks, the strict liability model can be used. Under this model, any cyber attack on critical infrastructure is considered 'a use of force.' This approach however is very broad as it characterises any attack as a use of force regardless of the intent or consequences. Further, not all cyberattacks on critical infrastructure are intended to cause physical harm or destruction. Classifying all under the use of force collapses the distinction between different dimensions of conflict. This approach has the potential to escalate conflict as it could authorise a state to respond with self-defense, which could include military force for any minor cyber offence that involves critical infrastructure.[115]

4.1.2. Challenges present under the Law of Armed Conflict: Principles of distinction, proportionality and the concept of direct participation

Cyber warfare blurs the line between combatants and civilians. This therefore makes the application of the principle of distinction difficult.[116] Due to the difficulty of cyber weapons to

[110] Mavropoulou E, 'Targeting in the Cyber Domain:Legal Challenges Arising from the Application of the Principle of Distinction to Cyber Attacks' Journal of Law and Cyber Warfare ,2015, 31 - https://www.jstor.org/stable/26441253?seq=3 on 6 January 2025.

[111] Farwell J and Rohozinski R, 'Stuxnet and the future of cyber war,' 24.

[112] Mavropoulou E, 'Targeting in the Cyber Domain:Legal Challenges Arising from the Application of the Principle of Distinction to Cyber Attacks' Journal of Law and Cyber Warfare ,2015, 32- https://www.jstor.org/stable/26441253?seq=3 on 6 January 2025.

[113] Gisel L, Rodenhauser T and Dormann K, 'Twenty years on: International humanitarian law and the protection of civilians against the effects of cyber operations during armed conflicts' International Review of the Red Cross, 2020, 325-https://international-review.icrc.org/sites/default/files/reviews-pdf/2021-03/twenty-years-ihl-effects-of-cyber-operations-during-armed-conflicts-913.pdf on 6 January 2024.

[114] Gervais M, 'Cyber Attacks and the Laws of War' 1 Journal of Law and Cyber Warfare 1, 2012, 28.

[115] Gervais M, 'Cyber Attacks and the Laws of War' 1 Journal of Law and Cyber Warfare 1, 2012, 28.

[116] Mavropoulou E, 'Targeting in the Cyber Domain: Legal Challenges Arising from the Application of the Principle of Distinction to Cyber Attacks' Journal of Law and Cyber Warfare ,2015, 23- https://www.jstor.org/stable/26441253?seq=3 on 9 February 2025.

distinguish between military and civilian targets, it subsequently becomes difficult to adhere to the principles. Cyber weapons also have a great potential for unintended consequences which contradicts proportionality which emphasises minimising collateral damage.[117] The Stuxnet attack for example could be seen to have been in contravention of the principle of distinction resulting from its indiscriminate nature and potential to harm civilians. The attack is seen to have spread beyond the intended target which raised concerns about the potential impact on civilian infrastructure. [118] Additional Protocol I mandates states to take measures to mitigate the impact of attacks, this includes separating military targets from civilian areas where possible. [119] Cyber infrastructure is dual use in nature as it can be used for both civilian and military purposes.[120] A large portion of military communication is civilian-owned and operated infrastructure and therefore it becomes difficult to make distinction between civilian and military targets in cyberspace.[121] However, this challenge could be breached by determining the object by the attacker's intent, that is, if the intent of the cyber attack was to gain military advantage, it would be lawful but if the same were to harm civilians or disrupt civilian lives, the same would be unlawful under IHL.[122] However, this interpretation hinges of the identification of the attacker which is difficult in cyberspace as could be seen in the 2007 cyber attack against Estonia where many suspected Russia's involvement but attribution was still challenging. Further, Russia denied responsibility for the same.[123] The obligation to make distinction is further complicated by the increasing integration between military and civilian infrastructure and more specifically, the adoption of cloud computing.[124]

[117] Gervais M, 'Cyber Attacks and the Laws of War' 1 Journal of Law and Cyber Warfare 1, 2012, 28.

[118] Zhuk A, 'Cyberwarfare and the Rule of Law: Exploring the Stuxnet Worm Attack from a Human Rights Perspective' Eliva Press, 2023, 40.

[119] Art 58, Protocol Additional to the Geneva Conventions.

[120] Mavropoulou E, 'Targeting in the Cyber Domain: Legal Challenges Arising from the Application of the Principle of Distinction to Cyber Attacks' Journal of Law and Cyber Warfare ,2015, 23- https://www.jstor.org/stable/26441253?seq=3 on 9 February 2025.

[121] Jensen E, 'Cyber Attacks: Proportionality and Precautions in Attack' United States Naval War College, Volume 89, 89 INT'L L. STUD. 198 , 2013, 213 https://digital-commons.usnwc.edu/cgi/viewcontent.cgi?article=1029&context=ils on 9 February 2025.

[122] Mavropoulou E, 'Targeting in the Cyber Domain: Legal Challenges Arising from the Application of the Principle of Distinction to Cyber Attacks' Journal of Law and Cyber Warfare ,2015, 23- https://www.jstor.org/stable/26441253?seq=3 on 9 February 2025.

[123] Gervais M, 'Cyber Attacks and the Laws of War' 1 Journal of Law and Cyber Warfare 1, 2012, 28.

[124] Jensen E, 'Cyber Attacks: Proportionality and Precautions in Attack' United States Naval War College, Volume 89, 89 INT'L L. STUD. 198 , 2013, 213 https://digital-commons.usnwc.edu/cgi/viewcontent.cgi?article=1029&context=ils on 9 February 2025.

Distinction becomes even more challenging when individuals involved in warfare do not belong to a state's official armed forces. A notable example is patriotic hackers operating in a state's territory. The degree of state control necessary for the groups to be considered combatants is unclear in cyberspace. Where these groups play a significant role in cyber warfare, there is a challenge posed as there are no current legal frameworks to address this situation. Likewise, levée en masse, which would have inhabitants of a territory regarded as combatants, would be impractical in cyberspace as the traditional requirements, such as openly carrying arms do not align with the covert nature of COs.[125]

Further, determining whether a response to an attack is proportional as well becomes difficult as it is difficult to measure cyber attacks along the parameters of proportionality and necessity. It is as well unclear whether economic sanctions as a response to the same would be proportional to the harm suffered as a result of COs. Additionally, the risk of escalation is high as cyber conflicts could lead to conventional warfare or the escalation of ongoing conventional warfare.

Moreover, applying the metric of 'direct participation in hostilities' to cyber warfare is extremely difficult.[126] There is a lack of clear definition of the concept under IHL and therefore it becomes more difficult to determine the legal status of civilians and combatants involved in the hostilities.[127] The ICRC Interpretive Guidance points out the elements that should have been met for an one to be "directly participating in hostilities."[128] The criteria include several key aspects. First, the act must be expected to or likely to negatively impact the military capacity of a party involved in the conflict. Second, a clear and direct causal link between the act and the resulting harm. Lastly, the act must be intentionally carried out to inflict harm in a way that

[125] Mavropoulou E, 'Targeting in the Cyber Domain: Legal Challenges Arising from the Application of the Principle of Distinction to Cyber Attacks' Journal of Law and Cyber Warfare ,2015, 23- https://www.jstor.org/stable/26441253?seq=3 on 9 February 2025.
[126] Mavropoulou E, 'Targeting in the Cyber Domain: Legal Challenges Arising from the Application of the Principle of Distinction to Cyber Attacks' Journal of Law and Cyber Warfare ,2015, 23- https://www.jstor.org/stable/26441253?seq=3 on 9 February 2025.
[127] Mavropoulou E, 'Targeting in the Cyber Domain: Legal Challenges Arising from the Application of the Principle of Distinction to Cyber Attacks' Journal of Law and Cyber Warfare ,2015, 23- https://www.jstor.org/stable/26441253?seq=3 on 9 February 2025.
[128] International Committee of the Red Cross, Interpretive Guidance on the Notion of Direct Participation in hostilities Under International Humanitarian Law, 2009, 46-64.

benefits one party while disadvantaging the other.[129] These 3 elements must be considered together and the absence of one negates the classification as "directly participating".[130] The application of these elements is difficult due to potential indirect harm or delayed effects that would not qualify as having a direct causal link.[131] Further, challenges in determining the intent of the act would make it difficult to satisfy the requirement of belligerent nexus. [132]

Protection afforded to specific groups of persons and objects under IHL, for example, medical personnel, as well poses unique challenges with regards to cyberspace. Applying such protection to cyberspace would raise complex questions. For example, medical facilities enjoy protection under IHL. However, applying such protection to the cyber space, with the digitisation of medical records adds a layer of complexity. This complexity includes instances where medical records are accessed for military purposes. This poses challenges in keeping with medical confidentiality even though there is no physical damage.[133]

4.2. Potential for indirect harm

Further, the potential for indirect harm caused by cyber-attacks poses a challenge to determine whether they constitute prohibited use of force under the UNC.[134] Cyberattacks may not necessarily result in casualties but can lead to them indirectly. For example, an attack that involves the shutting down of emergency lines may not cause death as a direct result but could lead to the same as it could cause hospitals and other basic services to be disrupted. Additionally, it becomes difficult to assess and adhere to the principle of proportionality whereby cyber

[129] International Committee of the Red Cross, Interpretive Guidance on the Notion of Direct Participation in hostilities Under International Humanitarian Law, 2009, 46-64.
[130] International Committee of the Red Cross, Interpretive Guidance on the Notion of Direct Participation in hostilities Under International Humanitarian Law, 2009, 50.
[131] Mavropoulou E, 'Targeting in the Cyber Domain: Legal Challenges Arising from the Application of the Principle of Distinction to Cyber Attacks' Journal of Law and Cyber Warfare ,2015, 23-https://www.jstor.org/stable/26441253?seq=3 on 9 February 2025.
[132] Mavropoulou E, 'Targeting in the Cyber Domain: Legal Challenges Arising from the Application of the Principle of Distinction to Cyber Attacks' Journal of Law and Cyber Warfare ,2015, 23-https://www.jstor.org/stable/26441253?seq=3 on 9 February 2025.
[133] Gisel L, Rodenhauser T and Dormann K, 'Twenty years on: International humanitarian law and the protection of civilians against the effects of cyber operations during armed conflicts' International Review of the Red Cross, 2020, 328-https://international-review.icrc.org/sites/default/files/reviews-pdf/2021-03/twenty-years-ihl-effects-of-cyber-operations-during-armed-conflicts-913.pdf on 6 January 2024.
[134] Article 2(4), Charter of the United Nations, 26 June 1945, 1 UNTS XVI.

attacks are involved as it would be difficult to predict delayed and indirect effects of cyber attacks, especially when they go beyond the intended targets.[135] The principle calls for a proportional response, however, concerning cyber warfare, this is both complex and subjective.[136] Stuxnet for example, had effects reaching far beyond Iran and affected systems in other countries as well. [137]The same is seen in the NotPetya attack which affected multinationals and had financial implications for more than just Ukraine.[138] These, when analysed with the principle of proportionality raised questions on whether these attacks really adhered to the principle.

4.3. Challenges regarding the right to self-defense

Additionally, article 51, under the UNC allows states self-defense measures if subjected to armed attack.[139] For COs, which in many cases do not cause direct physical harm, it becomes difficult to classify them as acts of violence[140] and therefore, armed attacks and consequently making it difficult to justify self-defence by affected states. Additionally, it becomes difficult to justify self-defence when cyber attacks have exploited grey areas under International law. This can be seen where actors exploit ambiguous legal rules or gaps under International Law.[141] COs, for example, which spread disinformation and manipulation are an exploitation of the grey zones. Operations which include the spread of false information or news or conspiracy theories, influence public opinion and undermine trust in public institutions. They additionally blur the lines between the truth and otherwise and therefore it becomes difficult to assess their nature and

[135] Jensen E, 'Cyber Attacks: Proportionality and Precautions in Attack' United States Naval War College, Volume 89, 89 INT'L L. STUD. 198 , 2013, 207 https://digital-commons.usnwc.edu/cgi/viewcontent.cgi?article=1029&context=ils on 6 January 2025.

[136]Farwell J and Rohozinski R, 'Stuxnet and the future of cyber war' *Survival*, 2011, 23 — <https://www.tandfonline.com/doi/epdf/10.1080/00396338.2011.555586?needAccess=true> on 9 February 2025.

[137] Farwell J and Rohozinski R, 'Stuxnet and the future of cyber war' *Survival*, 2011, 23 — <https://www.tandfonline.com/doi/epdf/10.1080/00396338.2011.555586?needAccess=true> on 9 February 2025.

[138] Krasznay C, 'Case study: The NotPetya campaign' ResearchGate, 2021, 486.

[139] Article 51, Charter of the United Nations, 26 June 1945, 1 UNTS XVI.

[140] Mavropoulou E, 'Targeting in the Cyber Domain:Legal Challenges Arising from the Application of the Principle of Distinction to Cyber Attacks' Journal of Law and Cyber Warfare ,2015, 29 - https://www.jstor.org/stable/26441253?seq=3 on 6 January 2025.

[141] Kleczkowska A, 'Explaining the Meaning of 'Grey Zones' in Public International Law Based on the Example of the Conflict in Ukraine', 1 Contemporary Central & East European Law 133, 2019, 77– https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3807147 on 1 February 2025.

purpose and seek recourse for the same. [142] Cyber espionage also forms another grey zone exploited as actors use this means to obtain strategic information to serve in the interests of a state.[143] Additionally, the use of cryptocurrencies to fund these activities and warfare takes advantage of the anonymity the method provides therefore making it difficult to trace the transactions. This allows states to support these activities while still maintaining plausible deniability.[144]

4.4. The problem of attribution

Another key challenge lies in the problem of attribution. The factors contributing to this challenge include the involvement of non state actors in conflict, when International law is the law governing states actions, the use of proxy actors and the covert nature of cyber attacks. The ICJ, in the Corfu Channel Case, while assessing the threshold for attributing responsibility for actions within a state's borders, affirmed that every state has a duty to prevent its territory from being knowingly used for acts that violate the rights of other states.[145] Therefore, states are primarily responsible for preventing cyber attacks that result in their territory as well as protecting civilians from their effects.[146] However, attribution becomes challenging, particularly in cases where attacks are carried out by non-state actors, such as patriotic hackers, who operate independently.[147] This can be seen ,for example, in the Russia-Georgia conflict which involved attacks on the Georgian government and infrastructure which coincided with military operations. Although some attributed the attacks to Russia, others stated that they were the work of patriotic hackers who acted independently.[148] It therefore becomes difficult to determine

[142] Mantea P, 'useful Tools For Measuring And Monitoring Cybersecurity' Centre for Defence and Security Strategic Studies, 5 November 2020https://cssas.unap.ro/en/pdf_books/conference_2020.pdf on 11 February 2025.
[143] Mantea P, 'useful Tools For Measuring And Monitoring Cybersecurity' Centre for Defence and Security Strategic Studies, 5 November 2020https://cssas.unap.ro/en/pdf_books/conference_2020.pdf on 11 February 2025.
[144] Constantinescu M, 'The Security implications of cryptocurrencies' Centre for Defence and Security Strategic Studies, 5 November 2020https://cssas.unap.ro/en/pdf_books/conference_2020.pdf on 11 February 2025.
[145] The Corfu Channel Case (U.K V Albania) Judgement 1949, 4.
[146] Gervais M, 'Cyber Attacks and the Laws of War' 1 Journal of Law and Cyber Warfare 1, 2012, 20.
[147] Gervais M, 'Cyber Attacks and the Laws of War' 1 Journal of Law and Cyber Warfare 1, 2012, 28.
[148] Gervais M, 'Cyber Attacks and the Laws of War' 1 Journal of Law and Cyber Warfare 1, 2012, 28.

whether the state took reasonable preventative action.[149] The covert nature of cyber-attacks further makes attribution difficult as it is difficult to determine the attackers' identity and therefore difficult to determine the responsible party.[150] In instances where states use proxy actors, for example private firms, to carry out attacks, therefore escaping responsibility, attribution is further complicated. [151] The lack of clear attribution makes it difficult to hold the attackers accountable and therefore difficult to demand the cessation of hostile acts or even take further legal responses.[152] This is especially difficult during peacetime as there is greater ambiguity which could potentially undermine international order.[153]

4.5. Technological limitations

Moreover, the workability of taking precautions in cyberattacks is constrained by technological limitations. While IHL obligates commanders to take measures to safeguard civilians, the same is limited by what is practically possible in a given circumstance.[154] Technological limitations further impact the same due to the dynamic nature of cyberspace which can hinder a complete understanding of potential consequences.[155] Further, it becomes more difficult to establish frameworks that would not quickly become obsolete with technological changes.[156] For example, quantum computing, when misused, can render current encryption based defences obsolete and allow for decryption of sensitive data, and therefore increases the risk of cyber escalation by causing an increase in the possibility of cyber threats. Especially if the decrypted information includes military data. [157] In addition, Artificial intelligence-driven warfare and

[149] Gervais M, 'Cyber Attacks and the Laws of War' 1 Journal of Law and Cyber Warfare 1, 2012, 46.
[150] Gervais M, 'Cyber Attacks and the Laws of War' 1 Journal of Law and Cyber Warfare 1, 2012, 63.
[151] https://jnslp.com/wp-content/uploads/2020/04/Projecting_Power_How_States_Use_Proxies_in_Cyberspace.pdf on 5 February 2025.
[152] Gervais M, 'Cyber Attacks and the Laws of War' 1 Journal of Law and Cyber Warfare 1, 2012, 28.
[153] Gervais M, 'Cyber Attacks and the Laws of War' 1 Journal of Law and Cyber Warfare 1, 2012, 28.
[154] Jensen E, 'Cyber Attacks: Proportionality and Precautions in Attack' United States Naval War College, Volume 89, 89 INT'L L. STUD. 198 , 2013, 213 https://digital-commons.usnwc.edu/cgi/viewcontent.cgi?article=1029&context=ils on 9 February 2025.
[155] Jensen E, 'Cyber Attacks: Proportionality and Precautions in Attack' United States Naval War College, Volume 89, 89 INT'L L. STUD. 198 , 2013, 213 https://digital-commons.usnwc.edu/cgi/viewcontent.cgi?article=1029&context=ils on 9 February 2025.
[156] Gervais M, 'Cyber Attacks and the Laws of War' 1 Journal of Law and Cyber Warfare 1, 2012, 28.
[157] Senewirathna N, 'Quantum Computing and It's Impact on Information Warfare:Threats and Cybersecurity Countermeasures' Published ,Sri Lanka Indtitute of Information Technology, Malabe, 2024,4.

autonomous cyber weapons raise ethical and legal dilemmas. These include whether AI can make judgement and reason and questions of the created accountability gap, among other dilemmas created.[158]Additionally, arms control being a potential successful means to control arms race, the lack of a treaty covering arms control in cyberspace contributes to a potential unchecked arms race.[159]

4.6. Enforcement

There is as well a challenge in enforcement. Cyber attacks originating from multiple jurisdictions make enforcement more difficult. Additionally, enforcement is made more difficult due to political tensions among states as well as alliances between states and the veto power possessed by the permanent members of the UN security council. In enforcement through Security Council resolutions, veto power by states prevents objective Security Council action as it would be unrealistic to assume that states would permit action against their and their allied states' interests. [160]This can lead to gridlock and inaction and therefore lack of enforcement. Furthermore, organisations such as the UN and the ICC lack clear mechanisms to prosecute cyber warfare violations.

Additionally, varying data sovereignty and privacy laws in different countries create further uncertainty. Furthermore, the Tallin Manual, which is a non-binding framework, provides guidelines on how to deal with cyber attacks. However, states are not obligated to follow it. This leaves a gap in states' obligations with regard to COs.

4.7. Conclusion

Ultimately, the challenges and limitations of applying existing legal framework to cyber warfare highlights the need for clearer and subject specific regulations which would result in greater international consensus. The ambiguities in definitions under IHL, difficulties applying core

[158] Caton J, 'Autonomous Weapon Systems: A Brief Survey of Developmental, Operational, Legal, and Ethical Issues ' *US Army War College Press* 2015, 17-39 – https://press.armywarcollege.edu/monographs/304/ on 1 February 2025.

[159] Reinhold T, Pleil H, Reuter C, 'Challenges for Cyber Arms Control: A Qualitative Expert Interview Study' 17 Zeitschrift für Außen- und Sicherheitspolitik 4, 2023, 290.

[160] Masciotra C, 'Cybersecurity challenges and disconnects in policy implementation',82.

principles such as the principles of distinction and proportionality and the complexities regarding attribution have all contributed to the legal uncertainty present . Further, changing technologies have continued to outpace legal development therefore further making enforcement and accountability more challenging. Without a tailored legal framework for cyber warfare, states have and will continue to exploit loopholes in law and therefore leading to escalation of conflict.

CHAPTER 5

SUMMARY OF KEY FINDINGS, RECOMMENDATIONS AND CONCLUSIONS

5.1. Summary of key findings

This dissertation establishes the existing IHL framework that is taken to be applicable to cyber warfare as is traditional armed conflict. They include the Geneva Conventions, UN Charter and Hague conventions. However, due to the intangible nature of cyber objects as well as the difficulties in properly applying the principles found, it becomes difficult to conclusively say that these principles apply to IHL. Documents such as the Tallin Manual as well offer specific guidance to address COs, however, the same is not binding and therefore does not impose legal obligation to follow on any state. Nonetheless, although existing structures are relevant, effective implementation is hindered by ambiguities, such as those in definition and the unique character of the cyberspace.

In analysing the instances of cyber warfare, the problems of attribution can clearly be seen to be brought about by a lack of clear definitions for cyber techniques and difficulty enforcing existing laws. The issues pointed out lead to inaction with regards to perpetrators of these attacks and pose questions on adherence to IHL principles such as distinction, proportionality and military necessity. In the instance of the Stuxnet attack, due to the identity of the attacker remaining unconfirmed, defensive action under article 51 of the UNCcannot be justified and thus legal recourse would also be difficult to seek. Further, the potential for damage with this attack to civilian targets further brought up questions on adherence to the principle of distinction. In the NotPetya attack, attribution by various states allowed for responses such as sanctions to be taken as the indiscriminate nature of the attack was in direct confrontation with the principle of distinction. However, this public attribution by other states is seen to rely more on political and diplomatic pressure as opposed to enforceable legal mechanisms. The question of proportionality and military necessity was also raised in the NotPetya attack due to the attack being seen to have caused damage far beyond any military advantage and if it did cause excessive incidental civilian damage, whether it was in contravention of article 51 of Additional Protocol 1. The dissertation further raised the question on whether attacks on civilian

infrastructure, for example, the attacks on the Georgian government websites, are in violation of the spirit of the Hague convention.

Further, in highlighting significant challenges in IHL to cyber warfare, the inconsistencies between the laws and situations of cyber warfare cause a legal gap in which states can exploit. Ambiguities in definitions complicate the application of core principles. Similarly, enforcement difficulties are further exacerbated by attribution challenges, stemming from the stealthiness of COs and the involvement of non-state combatants.

The evolving nature of cyber threats as well raises concerns about cyber threats and the potential for indirect harm further creates legal grey areas. In addition, enforcement mechanisms are rendered weak due to political tensions, a lack of a binding treaty with regards to cyber warfare and jurisdictional conflicts. The inconsistencies between existing laws and the realities of cyber warfare underscore the need for a specialised legal framework to address COs effectively.

5.2. Recommendations

5.2.1. Lobbying for the implementation of a legally binding dedicated framework

Cyber warfare, like any other form of warfare, cannot be fully regulated without a legally binding framework. Although the Tallinn Manual is present and can act as a guide in these conflicts, there is no legal reason states would be compelled to act in the interests of the manual. A legally binding manual would be required in order to compel states to follow it as well as allow an avenue for recourse in the instance of contravention. In lobbying for such, the pressure to implement would be higher as opposed to the current state of affairs where multiple authors and scholars iterate that current IHL is sufficient even in the instance of new and intricate methods of warfare such as cyber warfare.

5.2.2. Clarification of the scope of IHL in the cyberspace

Clarification of IHL especially the fundamental principles and their application in the cyberspace could be beneficial in allowing for consistency in terms of application of these

principles and predictability when recourse is sought out. This clarification could be done through the UN General Assembly seeking advisory opinions on the matter from the ICJ.

5.2.3. Redefinition of the terms “object” and “attack”

The redefinition of an object and attack under IHL could for a temporary solution to the challenges in applying current laws to cyber warfare, before a dedicated framework is implemented. Traditionally, IHL defines an object as something tangible however COs mostly include intangible data. In expanding this definition to include the intangible and stating the parameters of this expansion, principles such as the principle of distinction could be better applied. Further, the definition of an attack could be redefined in order to propose a clearer articulation of what constitutes a cyber attack and triggers IHL obligations.

5.3 . Conclusion

In conclusion, the existing IHL framework needs revision to effectively regulate cyber warfare and a dedicated legal framework eventually needed to address the unique challenges presented by COs in armed conflict. This dissertation aimed to come to a determination on whether a dedicated legal framework is necessary in order to achieve goals of IHL. Existing legal frameworks are inadequate when applied to COs due to ambiguities and inconsistencies in interpretation of the same. This is further exacerbated by the interconnected nature of civilian and military infrastructure which poses a challenge in the classification of military and civilian objects and applying the principle of distinction effectively. Furthermore, the potential for delayed effects from cyber attacks raises questions about accountability. Instances of COs in armed conflict have highlighted the difficulties in attributing responsibility and applying IHL effectively. The attack on Georgia raised the question of whether a cyberattack on military infrastructure could occur without directly or indirectly impacting civilians, while the NotPetya attack underscored the challenges of attribution. The challenges found in this dissertation show that current IL may not fully address the intricacies of cyber warfare. Although argument can be made that IHL can be transposed to cyber attacks as the differences are of degree and not of kind, many concepts of IHL hinge on degree, such as the principle of proportionality and therefore differences of degree are fundamental differences in the space.

Bibliography

Aravindakshan S, ‘Cyberattacks: a look at evidentiary thresholds in International Law’ *Indian Journal of International Law*, 2020.

https://casebook.icrc.org/a_to_z/glossary/cyber-warfare

https://casebook.icrc.org/a_to_z/glossary/military-necessity#:~:text=The%20%E2%80%9Cprinciple%20of%20military%20necessity,prohibited%20by%20international%20humanitarian%20law

Caton J, ‘Autonomous Weapon Systems: A Brief Survey of Developmental, Operational, Legal, and Ethical Issues ’ *US Army War College Press* 2015, 17-39 – https://press.armywarcollege.edu/monographs/304/

https://www.cisa.gov/news-events/cybersecurity-advisories/aa22-264a#:~:text=In%20June%202022%2C%20HomeLand%20Justice,cyber%20attack%20on%20their%20website

Constantinescu M, ‘The Security implications of cryptocurrencies’ Centre for Defence and Security Strategic Studies, 5 November 2020 https://cssas.unap.ro/en/pdf_books/conference_2020.pdf

Crawford J and Gunn A, ‘The ethics of automation in digital service work’ *Journal of Business Research* 140, 2024— <https://www.sciencedirect.com/science/article/abs/pii/S026736492400075X.>

Deibert R, Rohozinski R, Crete-Nishihata M, ‘Cyclones in cyberspace: Information shaping and denial in the 2008 Russia-Georgia war’ *Security Dialogue,* 2012— https://www.jstor.org/stable/pdf/26301960.pdf?refreqid=fastly-default%3A9e16260fbc4a538cda9e61e3d8b64f05&ab_segments=&initiator=&acceptTC=1.

Ethics Unwrapped, 'Deontology', McCombs School of Business, University of Texas, 2024 <https://ethicsunwrapped.utexas.edu/glossary/deontology>

Farwell J and Rohozinski R, 'Stuxnet and the future of cyber war,'

Fraczek J, 'Is IHL Fit to Deal with the Ones and Zeroes? Analyzing the Application of the Principles of Distinction, Proportionality and Precautions to Cyber Operations' Glasgow Centre for International Law and Security, GCILS Working Paper Series 20, 2024-- https://gcils.org/gcils-publications/gcils-working-paper-series/working-paper-series-2024/

Gervais M, 'Cyber Attacks and the Laws of War' 1 Journal of Law and Cyber Warfare 1, 2012

Gisel L, Rodenhauser T and Dormann K, 'Twenty years on: International humanitarian law and the protection of civilians against the effects of cyber operations during armed conflicts' International Review of the Red Cross, 2020-https://international-review.icrc.org/sites/default/files/reviews-pdf/2021-03/twenty-years-ihl-effects-of-cyber-operations-during-armed-conflicts-913.pdf

Haeck S, 'The rights to privacy and data protection in armed conflict' *International Review of the Red Cross*, 105 (923), 2023,—https://international-review.icrc.org/sites/default/files/reviews-pdf/2023-06/the-rights-to-privacy-and-data-protection-923.pdf .

Huang Z and Ying Y, 'The application of the principle of distinction in the cyber context: A Chinese perspective' International Review of the Red Cross, March 2020-- https://international-review.icrc.org/articles/principle-of-distinction-cyber-context-chinese-perspective-913#footnote149_5dif7ti

ICRC, 'Fundamentals of IHL,' https://casebook.icrc.org/law/fundamentals-ihl#footnote2_zq0q4gb.

Identity Theft Resource Centre, *ITRC Annual Data Breach Report*.

https://ihl-databases.icrc.org/en/ihl-treaties/api-1977/article-36?activeTab=

International Committee of the Red Cross, *International Humanitarian Law and the Challenges of Contemporary Armed Conflicts*, 2011, [https://casebook.icrc.org/case-study/icrc-international-humanitarian-law-and-challenges-contemporary-armed-conflicts-2011]

International Committee of the Red Cross and the Red Cresent, *How Does Law Protect in War.*

International Committee of the Red Cross and the Red Cresent, International Humanitarian Law and the challenges of contemporary armed conflicts in 2015

International Committee of the Red Cross, Interpretive Guidance on the Notion of Direct Participation in hostilities Under International Humanitarian Law, 2009.

Internet Encyclopedia of Philosophy, 'Jeremy Bentham', University of Tennessee at Martin, 2024, <https://iep.utm.edu/jeremy-bentham>

Jensen E, 'Cyber Attacks: Proportionality and Precautions in Attack' United States Naval War College, Volume 89, 89 INT'L L. STUD. 198 , 2013, https://digital-commons.usnwc.edu/cgi/viewcontent.cgi?article=1029&context=ils

Johnston A, 'Treating International Institutions as Social Environments', 45 *International studies quarterly* 4, 2001, —<https://www.jstor.org/stable/pdf/3096058>

Katzenstein P, 'Cultural Norms and National Security: Police and Military in Postwar Japan' Cornell Studies in Political Economy, 1996- https://www.jstor.org/stable/10.7591/j.ctv5rdzdm

Klabbers J, Kratochwil,'The Status of Law in World Society: Meditations on the Role and Rule of Law' *European Journal of International Law*, 2014— https://doi.org/10.1093/ejil/chu082

Kleczkowska A, 'Explaining the Meaning of 'Grey Zones' in Public International Law Based on the Example of the Conflict in Ukraine', 1 Contemporary Central & East European Law 133, 2019– https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3807147

Korns S and Kastenberg J, 'Georgia's Cyber Left Hook' *Parameters 38*, 2008— https://press.armywarcollege.edu/cgi/viewcontent.cgi?article=2455&context=parameters

Mantea P, ‘Useful Tools For Measuring And Monitoring Cybersecurity’ Centre for Defence and Security Strategic Studies, 5 November 2020https://cssas.unap.ro/en/pdf_books/conference_2020.pdf

Masciotra C, ‘Cybersecurity challenges and disconnects in policy implementation’ *Political Science Graduate Student Association Journal* 3, 2020— <https://www.concordia.ca/content/dam/artsci/polisci/docs/psgsa/Vol%203%20ChallengesDisconnects.pdf#page=82.>

Mavropoulou E, ‘Targeting in the Cyber Domain: Legal Challenges Arising from the Application of the Principle of Distinction to Cyber Attacks’ Journal of Law and Cyber Warfare ,2015, https://www.jstor.org/stable/26441253?seq=3

https://www.microsoft.com/en-us/security/blog/2022/09/08/microsoft-investigates-iranian-attacks-against-the-albanian-government/

Pavel T, “The Iranian Cyberattacks in Albania: Actors, Tactics, Targets” https://www.journaldot.pl/pdf-196772-117133?filename=The%20Iranian%20Cyberattacks.pdf

Reinhold T, Pleil H, Reuter C, ‘Challenges for Cyber Arms Control: A Qualitative Expert Interview Study’ 17 Zeitschrift für Außen- und Sicherheitspolitik 4, 2023

Schmitt M, Tallinn Manual on the International Law Applicable to Cyber Warfare, 2 ed, Cambridge University Press, Cambridge, 2017.

Senewirathna N, ‘Quantum Computing and It’s Impact on Information Warfare:Threats and Cybersecurity Countermeasures’ Published ,Sri Lanka Indtitute of Information Technology, Malabe, 2024.

Shi X, Huang M, ‘ Cyberinfrastructure and High-Performance Computing’ in Huang B, Comprehensive Geographic Information Systems, Elsevier, United States, 2018.

Theys S, ‘Introducing Constructivism in International Relations Theory’ E-International Relations, 2018, 1.

UN International Law Commission (ILC), *Report of the International Law Commission on the work of its seventy-first session (29 April–7 June and 8 July–9 August 2019)*, UN Doc A/74/10, 2019, https://legal.un.org/ilc/reports/2019/english/chp5.pdf

Viva Press, 'Deontology: Pros & Cons', Open Educational Resource, 2024, <https://viva.pressbooks.pub/phi220ethics/chapter/deontology-pros-cons>

Zhuk A, ‘Cyberwarfare and the Rule of Law: Exploring the Stuxnet Worm Attack from a Human Rights Perspective’ Eliva Press, 2023.