



UNIVERSITY OF NAIROBI

SCHOOL OF LAW

THE APPLICATION OF INTERNATIONAL LAW TO CYBER-ARMED CONFLICT

ANNE WAMBERE NDEGWA

REGISTRATION NUMBER:

G62/40701/2021

**A THESIS SUBMITTED IN PARTIAL FULFILMENT OF THE REQUIREMENTS
FOR THE AWARD OF THE DEGREE OF MASTER OF LAWS (LL.M),
UNIVERSITY OF NAIROBI**

SUPERVISOR: DR. KEN OBURA

SUBMITTED ON: 22/10/2023

DECLARATION OF ORIGINALITY

I, **ANNE WAMBERE NDEGWA**, do hereby declare that this research is my original work and that the same has not been presented for an award of a degree before by anyone else within the University of Nairobi or any other University or educational institution.

Candidate: **Anne Wambere Ndegwa**




Signature:

Date: 22/10/2023

This thesis has been submitted with my approval as the University Supervisor.

Supervisor: **Dr. Ken Obura**

Signature: ...



Date:30/10/2023.....

ACKNOWLEDGEMENTS

I am grateful to God for His boundless love, grace and providence.

I express my gratitude to my family, friends and mentors who have supported and encouraged me through this journey. I am especially grateful to my mother, Agnes Wakarindi Ndegwa, who has steadfastly encouraged and cheered me on through the course of this study.

I am indebted to my supervisor, Dr. Ken Obura for his patience and insight. Without his guidance, it would have been nearly impossible to produce this piece of work.

DEDICATION

I dedicate this work to my late father, Anthony Ndegwa Kariuki. I wish you were here.

TABLE OF CONTENTS

CHAPTER ONE	1
1.0 GENERAL INTRODUCTION.....	1
1.1 Background to the Study.....	1
1.2. Statement of the problem	2
1.3 Objectives of the Study	2
1.3.1 Main Objective	2
1.3.2 Specific Objectives	2
1.4 Research Questions.....	3
1.5 Justification of the Study.....	3
1.6 Literature Review	3
1.6.1 Application of international law to armed conflict in cyberspace.....	3
1.6.2 Establishment of a universal treaty on armed conflict in cyberspace	7
1.7 Research Methodology	9
1.8 Chapter Breakdown	10
CHAPTER TWO	11
2.0 INTERNATIONAL LAW ON ARMED CONFLICT IN CYBERSPACE.....	11
2.1. Introduction.....	11
2.2 What is Cyber Armed Conflict?	12
2.3 History of the debate on the Application of International Law to Cyberspace and Cyber-Armed Conflict.....	13
2.4 The Tallinn Manual on the International Law Applicable to Cyberwarfare	16
2.4.1 Drafting and Scope of the Manual	16
2.4.2 The Composition of the Tallinn Manual.....	17
2.4.3 Issues Emerging from the Application of International Law to Cyber-Armed Conflict.....	17

2.4.3.1 Scope of Application of International Law to Cyber Armed Conflict.....	17
2.4.3.2 The Concept of an ‘Attack’	22
2.4.3.2.1 Precautions	23
2.4.3.2.2 Conduct of Attacks	24
2.4.3.2.3 Attacks against persons	25
2.4.3.2.4 Certain Persons, Objects and Activities.....	26
2.4.3.2.5 United Nations Personnel, Installations, Materiel Units and Vehicles	26
2.4.3.2.6 Collective Punishment and Humanitarian Assistance.....	27
2.4.3.2.7 Attacks against Objects	27
2.4.3.2.8 Installations Containing Dangerous Forces.....	28
2.4.3.2.9 Objects Indispensable to the Survival of the Civilian Population.....	29
2.4.3.2.10 Cultural Property.....	29
2.4.3.2.11 The Natural Environment and Diplomatic Archives and Communications... 	29
2.4.3.3 Direct Participation in Hostilities	30
2.4.3.3.1 Participation in Armed Conflict in General.....	30
2.4.3.3.2 Members of the Armed Forces	32
2.4.3.3.3 <i>Levees en Masse</i>	33
2.4.3.3.4 Mercenaries and Civilians.....	34
2.4.3.4 The Principle of Distinction	34
2.4.4 Additional Issues Arising from the Application of International Law	35
2.4.4.1 Means and Methods of Warfare.....	35
2.4.4.2 Perfidy, Improper Use and Espionage.....	37
2.4.4.3 Blockade and Zones	38
2.4.4.4 Occupation.....	39
2.4.4.5 Neutrality	39

2.5 Critique of the Tallinn Manual on the International Law Applicable to Cyberwarfare	40
.....	
2.5.1 Value of the Tallinn Manual	40
2.5.2 Weaknesses of the Manual	41
2.5.2.1 The Proposed Application of Extant International Law To Cyberspace	41
2.5.2.2 Characterization of armed Conflict in the realm of cyberspace	42
2.5.2.3 Definitional Challenges	43
2.5.2.4 The Status of Certain Objects	44
2.5.2.5 Participation in Hostilities	45
2.5.2.6 Geographical Prejudice	46
2.5.2.7 Attribution and the Evidentiary Challenges	47
2.5.2.8 Inability to predict Implementation	47
2.6 Conclusion	48
CHAPTER THREE	49
3.0 APPLICATION OF INTERNATIONAL LAW TO ARMED CONFLICT IN CYBERSPACE: CHALLENGES AND OPPORTUNITIES	49
3.1 Introduction	49
3.2 Positions of States on the Application of International Law to Cyber Armed Conflict	49
.....	
3.3 Challenges in the Application of Existing International Law to Cyber- Armed Conflict	52
.....	
3.3.1 Attribution	52
3.3.2 Compliance with the Principle of Distinction	54
3.3.3 Insufficient State Practice	54
3.3.4 Lack of Enforcement Mechanisms	55
3.3.5 Due Diligence	56
3.3.6 Emergence of non-state actors in cyberspace	57

3.3.7 Inadequate human capacity in cybersecurity.....	57
3.4 Opportunities for States in the Application of International Law to Cyber-Armed Conflict.....	58
3.5 Establishment of a Universal Treaty Governing Cyber Armed Conflict	61
3.6 Conclusion	68
CHAPTER FOUR.....	69
4.0 CONCLUSION AND RECOMMENDATIONS.....	69
4.1 Conclusions.....	69
4.2 Recommendations	70
4.2.1 Establishment of a Universal Treaty Governing Cyber-Armed Conflict.....	70
4.2.2 Weapons Review	71
4.2.3 Capacity building in the area of cyber security	72
4.2.4 Multi-stakeholder Engagement in cyber security	72
BIBLIOGRAPHY	73

TABLE OF CASES

Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Bosnia and Herzegovina vs. Serbia and Montenegro), [2007] ICJ Reports

Corfu Channel Case (United Kingdom of Great Britain and Northern Ireland v. Albania); Merits, International Court of Justice [1949] ICJ Rep 4

Legality of the Threat or Use of Nuclear Weapons [1996] ICJ Rep 226

Prosecutor v. Kunarac, Kovac and Vukovic (Appeals) ICTY-96-23 and IT-96-23/1 (12 June 2002)

Prosecutor v. Stanislav Galic (Trial Judgment and Opinion) ICTY-98-29 T (5 December 2003)

Prosecutor vs. Dusko Tadic (Appeals Judgment) ICTY-94-1-A (26 January 2000)

Prosecutor vs. Thomas Lubanga Dyilo (Judgement), ICC-01/04-01/06

TABLE OF REGIONAL AND INTERNATIONAL INSTRUMENTS

African Union Convention on Cyber Security and Personal Data Protection (adopted 27 June 2014)

Convention on Cybercrime (adopted 8 November 2001)

Convention on the Prohibition of the Development, Production, Stockpiling and Use of Chemical Weapons and on their Destruction (adopted 13 January 1993, entered into force 29 April 1997)

International Committee of the Red Cross (ICRC), Geneva Convention Relative to the Protection of Civilian Persons in Time of War (Fourth Geneva Convention), 12 August 1949, 75 UNTS 287

International Committee of the Red Cross (ICRC), Protocol Additional to the Geneva Conventions of 12 August 1949 and Relating to The Protection of Victims of International Armed Conflicts (Protocol I), 8 June 1977, 1125 UNTS 3

International Committee of the Red Cross (ICRC), Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of Non-International Armed Conflicts (Protocol II), 8 June 1977, UNTS 609

LIST OF ABBREVIATIONS

AP	Additional Protocol
CCDCOE	Cooperative Cyber Defence Centre of Excellence
DNC	United States National Democratic Committee
ICJ	International Court of Justice
ICRC	International Committee of the Red Cross
ICT	Information Communication Technology
IHL	International Humanitarian Law
NATO	North Atlantic Treaty Organization
UN	United Nations
UN GGE	United Nations Group of Governmental Experts

CHAPTER ONE

1.0 GENERAL INTRODUCTION

1.1 Background to the Study

The emergence of the internet has increased interconnectedness between States and cyber activities are becoming increasingly crucial in international relations. In addition to the traditional forms of launching attacks against opponents during the conflict, cyberspace has emerged as a new frontier in conflict. In 2014, the North Atlantic Treaty Organization (NATO) allied leaders, made cyber defence an integral part of collective defence declaring that a cyber-attack could lead to the invoking of Article 5 (the collective defence clause) of NATO's founding treaty.¹ During the NATO Warsaw Summit held on 8th-9th July 2016, Heads of State and Government of NATO member countries reaffirmed existing commitments including the strengthening of cyber defence capabilities and the applicability of international law. The Summit recognised cyberspace as a 'domain for operations'.²

Cyber- attacks may be used to target and bring down critical and civilian infrastructure during armed conflict. In the ongoing conflict between Russia and Ukraine, military analysts and cyber security analysts fear that Russia could use devastating attacks to take down critical Ukrainian infrastructure such as government services, energy and internet services, an occurrence which is yet to occur, but one that would lead to devastating consequences if it does occur.³ NATO's Secretary General, Jens Stoltenberg when addressing the press on the ongoing Russia- Ukraine conflict, addressed the fears of a cyberattack by Russia. He warned that a cyber-attack could be enough to trigger Article 5 of the NATO treaty and compel member states into a state of war.⁴ Despite these recent events and the acknowledgement of cyberspace as a new frontier for conflict, the international legal framework is yet to develop and authoritatively address itself to the governance of armed conflict in cyberspace.

¹Laura Brent, 'NATO's Role in Cyberspace' <<https://www.nato.int/docu/review/articles/2019/02/12/natos-role-in-cyberspace/index.html>> accessed 5th March 2022.

²CCDCOE 'NATO Recognizes Cyberspace as a 'Domain of Operations' at Warsaw Summit' <<https://ccdcoe.org/about-us/>> accessed 5 March 2022.

³Kate Conger and Adam Satariano <<https://www.nytimes.com/2022/03/04/technology/ukraine-russia-hackers.html>> accessed 5th March 2022.

⁴<<https://globalnews.ca/video/8646550/russia-ukraine-conflict-nato-chief-wars-russia-that-cyber-attacks-can-trigger-nato-charter-article-5>> accessed 5th March 2022.

1.2. Statement of the problem

Cyberspace has increased the connectedness between states and it has taken a central role in relations between them. Cyberspace has however also emerged as a frontier for conflict in the recent past. In the absence of a binding universal treaty governing cyberspace and cyber-armed conflict, some states have attempted to tackle this using existing international rules and norms and regional agreements. Many states, however, are comfortable with the *status quo*, arguing that the rapid advances in technology present too many challenges to legal regulation of the cyber domain. The inadequacy of the current legal framework governing cyber space and cyber armed conflict has resulted in repeated calls for the establishment of an international treaty to govern cyberspace.

1.3 Objectives of the Study

1.3.1 Main Objective

The main objective of this study will be to examine the application of international law to cyber-armed conflict.

1.3.2 Specific Objectives

The specific objectives of the study will be to:

1. Identify and analyse the international and regional legal frameworks that apply to cyber space and cyber armed conflict;
2. Discuss and delineate the concept and scope of cyber-armed conflict;
3. Examine the challenges and opportunities of applying the existing international legal rules to cyber-armed conflict; and
4. Investigate possible solutions for the enhanced governance of cyberspace and cyber armed conflict.

1.4 Research Questions

The research will be directed by the following research questions:

1. What is the legal framework applicable to cyberspace and cyber armed conflict?
2. What is cyber-armed conflict?
3. What are the challenges and opportunities of applying extant international legal rules to cyber-armed conflict?
4. What possible solutions can be created to enhance the governance of cyberspace and cyber armed conflict?

1.5 Justification of the Study

This study focuses on the international law applicable to cyber-armed conflict. The study builds on the existing literature in the area and goes further to investigate the challenges and opportunities of applying extant international law to cyberspace, which is a new domain for cyber-armed conflict. This research will help legal practitioners, academia, militaries and international legal persons understand the intricacies of the application of international law to cyber-armed conflict. The research also seeks to contribute towards the debate about the suitability of using extant international law in this new domain.

1.6 Literature Review

1.6.1 Application of international law to armed conflict in cyberspace

According to Chris Inglis, the word ‘cyberspace’ is defined to include but not be limited to “the sum of software, hardware and interconnections that altogether are referred to as the internet”.⁵ The increasing use of cyberspace has also intensified the focus on the vulnerability of cyberspace users, as well as the need to govern cyberspace through legal mechanisms.

Catherine Lotrionte notes there are competing views by states on the application of international law to cyberspace. While the United States has expressly stated that the laws of

⁵C Inglis, ‘Cyberspace—Making Some Sense of It All’ (2016) 15 *Journal of Information Warfare* 17 <<https://www.jstor.org/stable/26487528>> accessed 30 January 2022.

war apply to cyberspace, China has expressed a contrary view that ‘existing mechanisms’ such as international humanitarian law do not apply to cyber operations.⁶ She further states that the absence of an explicit prohibition of cyber warfare by international law implies that cyber warfare is permitted.⁷ She proceeds to assert that where there is an absence of agreement in the applicability of treaty law in this area of international law and there is minimal likelihood of a new treaty being established to regulate cyberspace, state practice will inform the interpretation of the relevant treaty practice over time.⁸ Further, as state expectations change in the context of cyber warfare, international norms will advance to meet those expectations.⁹ While Lotrionte is keen to acknowledge that International Law applies to cyberspace, she does not discuss the challenges that arise in the application of existing international law to cyberspace. This study therefore aims to bridge this gap by discussing these challenges.

The United Nations in its report “The Application of International Law in Cyberspace: State of Play” noted that states have recently arrived at a consensus that international laws, agreements and norms apply to cyberspace, particularly the principles of jurisdiction, sovereignty and prohibition on the use of force and interference in the affairs of another state.¹⁰ However, the question of which international law applies in cyberspace has persisted. States are yet to reach an agreement on the applicability of International Humanitarian Law, a significant component of international law, to cyberspace.¹¹ This notwithstanding the general agreement that the Charter of the United Nations applies to cyberspace.

According to Madubuike-Ekwe,¹² International Humanitarian Law gives the basic legal structure within which the limits on the use of offensive cyber operations should be understood. According to Ekwe, International Humanitarian Law addresses the legality of the use of force by one nation against another.¹³ It also addresses the rules that regulate the behaviour of combatants who are engaged in armed conflict. He further proposes that in addition to

⁶Catherine Lotrionte, ‘Cyber Operations: Conflict Under International Law’ [2012] *Georgetown Journal of International Affairs* 15 <<https://www.jstor.org/stable/43134334>> accessed 20 October 2023.

⁷Lotrionte (n 6).

⁸ Lotrionte (n 6).

⁹ Lotrionte (n 6).

¹⁰The Application of International Law in Cyberspace: State of Play – UNODA’ <<https://www.un.org/disarmament/update/the-application-of-international-law-in-cyberspace-state-of-play/>> accessed 30 January 2022.

¹¹‘2011_CMPR_Final.Pdf’ <https://dod.defense.gov/Portals/1/Documents/pubs/2011_CMPR_Final.pdf> accessed 30 January 2022.

¹²Joseph N Madubuike-Ekwe, ‘Cyberattack and the Use of Force in International Law’ (2021) 12 *Beijing Law Review* 631 <<https://www.scirp.org/journal/paperinformation.aspx?paperid=109997>> accessed 19 October 2023.

¹³Madubuike-Ekwe (n 10).

International Humanitarian Law, the Charter of the United Nations, international treaties and domestic laws regulate cyber-attacks.

He notes that while International Humanitarian Law is inadequate, it provides some guidance for states looking to determine the scope of acceptable offensive and defensive cyber-attacks. He notes that the inadequacies in International Humanitarian Law make it imperative to establish a new legal framework to comprehensively address cyber-attacks.¹⁴ Ekwe acknowledges the challenges that emanate from the attempt to apply the extant international law to cyber-armed conflict. However, he does not examine how these challenges can be turned into opportunities for states in this area. This research will not only discuss these challenges, but it will also examine how these challenges can be turned into opportunities for states in this area.

Dipert contends in his article 'The Ethics of Cyberwarfare' that international treaties cannot regulate cyberspace and that protracted periods of mild multilateral cyberwarfare should be expected.¹⁵ He contends that existing international law and the Just War Theory principles do not apply directly to cyberwarfare. He bases his argument on the distinction between cyber warfare and 'traditional' forms of warfare, arguing that it neither kills people nor causes long-term physical damage.¹⁶ Dipert look into the challenges that cyberspace poses in the application of international law while making his argument that international law does not apply to cyberspace and to cyber-armed conflict. Just like Ekwe, Dipert does not make proposals on how these challenges can be transformed into opportunities in this context.

Sohail notes that cyber operations do not occur in a legal void as their increasing entrenchment in armed conflict demands that that existing International Humanitarian Law is interpreted in an evolutionary manner.¹⁷ He traces the historical development of the debate on history of cyber-attacks and tackles the definitional challenges that emerge with regard to terms 'attack' and 'object' in the context of cyber. He discusses the concept of attribution in the cyber context and discusses the challenges that are attendant in classifying armed conflict as international or non-international in cyberspace.¹⁸ He notes that International Humanitarian Law was

¹⁴Madubuike-Ekwe (n 10).

¹⁵Randall R Dipert, 'The Ethics of Cyberwarfare' (2010) 9 Journal of Military Ethics 384 <<http://www.tandfonline.com/doi/abs/10.1080/15027570.2010.536404>> accessed 21 October 2023.

¹⁶Dipert (n 23).

¹⁷Humna Sohail, 'Fault Lines in the Application of International Humanitarian Law to Cyberwarfare' [2022] Journal of Digital Forensics, Security and Law <<https://commons.erau.edu/jdfsl/vol17/iss1/8/>> accessed 19 October 2023.

¹⁸Sohail (n 13).

developed when cyber warfare was yet to emerge and he therefore opines that the remedies for the challenges facing the international community in respect to cyber warfare may include the establishment of a new convention specifically made for cyber-armed conflict. In the alternative, he proposes that consistent state practices out of a sense of legal obligation will create binding norms in this matter.¹⁹

He further opines that states may engage in increasingly devastating cyber conflicts, as they are involved in cyber arms race. This, he states, will possibly lead to the emergence of a new norm. He concludes that once state practice has fully developed, it would be possible to create a treaty governing cyberspace but until then, the rules of International Humanitarian Law should continue to govern cyberwarfare.²⁰ While Sohail proposes that a new treaty governing cyber-armed conflict may be the panacea of the problems that plague this domain, he does not give detailed arguments in support of his proposal to establish the conventions. Unlike Sohail's work, this research will detail the merits and demerits of conclusion of a treaty among other possible solutions

Dapo Akande argues that international law is not as a general matter specific to 'domains'. Thus, its applicability to a specific 'domain' such as sea, land, outer space and air need not be specifically proven.²¹ He argues that contrary to this assertion, any prohibition imposed on the scope of general international law whether tailored around a particular subject matter or domain cannot be assumed but must be drawn from specific evidence.²² Further, the concept of 'domain' in International Humanitarian Law and other areas was not meant to serve as a means to carve out certain types of activity from existing rules or principles of international law. This therefore means that the rules of international law, which demonstrate a general scope of application, can be interpreted to new domains. With these arguments, he concludes that all relevant existing rules of international law automatically apply to the conduct of states with respect to use of Information Communication Technologies.²³ In as much as Prof. Akande maintains that international law is not 'domain-specific' with the exception of instances where it is expressly stated to be limited to a domain such as air, land, sea and outer space, he does not explore the issues the application of international law to armed conflict in cyberspace raises.

¹⁹Sohail (n 13).

²⁰Sohail (n 13).

²¹Dapo Akande, Antonio Coco and Talita de Souza Dias, 'Drawing the Cyber Baseline: The Applicability of Existing International Law to the Governance of Information and Communication Technologies' (2022) 99.

²²Akande, Coco and Dias (n 18).

²³Akande, Coco and Dias (n 18).

1.6.2 Establishment of a universal treaty on armed conflict in cyberspace

The difficulties faced in applying international law in cyberspace have resulted in repeated debates over the establishment of an international treaty on cyberspace. Only a few international instruments focus specifically on cyberspace. Even then, these instruments are limited in scope. Additionally, most state practices in cyberspace are shrouded in secrecy as cyber operations are more often than not conducted by armed forces and intelligence organizations. Further, public statements which indicate a state's understanding of the obligations under international law that are binding on them are rare.²⁴ While this may be the case and the challenges with the applying international law to cyber space may be rife, there is general agreement that International Humanitarian Law applies to cyber-armed conflict.

According to Professor Andreas Zimmermann,²⁵ the willingness and ability of the family of nations to come up with adequate international rules applicable to cyberspace will be demonstrated with the passing of time. While the community of nations waits for such development, States and non-state actors will rely on general and ambiguous rules of international law and make an effort to apply them to human activity on cyber space.²⁶ Although Professor Zimmermann concedes that international law applies to cyberspace, he does not venture into a detailed discussion of how international law applies to cyber-armed conflict.

Judge Frank H. Easterbrook posits that technology changes so rapidly that it is not necessary for legislators to struggle to pair what he called "an imperfect legal system" to a changing world that was poorly understood. He proposes that legislators should enable members of the changing world to make their own choices. He suggests that we "let the world of cyberspace evolve as it is and enjoy the benefits of evolution."²⁷ Other than making a case against why attempts should not be made to match the law with the ever-changing cyberspace domain, he does not specifically address the application of international law to cyberspace. Additionally, he only states that the world of cyberspace should be allowed to evolve freely without giving detailed proposals why it should be allowed to evolve freely without attempts being made to govern it through legislation.

²⁴ Lt Col Torii Mayuko, 'Issues concerning Cyber Attacks in Light of the Law of Armed Conflict' 7 Air and Space Power Studies pp 255

²⁵ Andreas Zimmermann, 'International Law and "Cyber Space"' 3 ESIL Reflections.

²⁶ Zimmermann (n 26).

²⁷ Frank H Easterbrook, 'Cyberspace and The Law of The Horse' The University Of Chicago Legal Forum 217.

In a rejoinder to Judge Easterbrook's views, Professor Lessing proposes that 'Code is Law,' a term he coined to argue that "code" regulates conduct in cyberspace in the similar way that physical laws control the natural world. Conversely, unlike physics, code is pliable, raising the dilemma of when governments should modify it and when they should leave it as it is.²⁸ Professor Lessing does not engage in a comprehensive discussion on why he proposes the regulation of cyberspace by international law and norms.

Creating an internationally binding treaty on cyber armed conflict, according to Eilstrup-Sangiovanni, would enhance efforts to achieve cyber deterrence. She maintains that establishing such a treaty would solve many of the problems associated with implementing international law in cyberspace. The existing obstacles in attribution and the complexity in discriminating between a cyber-attack and a mistake would be among the concerns addressed and defined. Furthermore, the Treaty would establish a distinction between lawful and unlawful cyberspace behaviour.²⁹ Sangiovanni emerges as a strong proponent for the regulation of cyberspace through a binding treaty. She identifies the objections against the establishment of such a treaty and puts forward solutions to the challenges she has identified. She however does not engage in a discussion on the various stances that states have taken with regard to the application of international law to cyberspace and to cyber armed conflict.

Prof. Solange Ghernaouti-Hélie argues that cyberspace requires coordination, cooperation and legal measures among all states to ensure it functions smoothly in the same way as the other four domains.³⁰ To achieve this, Prof. Solange Ghernaouti-Hélie posits that the creation and utilization of a global United Nations framework is the best means. Ultimately, this would lead to the establishment of a Cyber Treaty, which would stipulate acceptable and unacceptable behaviour in cyberspace.³¹ Prof. Hélie acknowledges the necessity of the regulation of cyberspace by an international treaty. She discusses the importance of proper governance of cyberspace by an international legal framework but the discussion thereon revolves mainly around cyber-crime and cyber criminality as opposed to cyber armed conflict.

²⁸Four Challenges for International Law and Cyberspace: Sartre, Baby Carriages, Horses, and Simon & Garfunkel Part 2' (*Council on Foreign Relations*) <<https://www.cfr.org/blog/four-challenges-international-law-and-cyberspace-sartre-baby-carriages-horses-and-simon-0>> accessed 21 January 2022.

²⁹Mette Eilstrup-Sangiovanni, 'Why the World Needs an International Cyberwar Convention' (2018) 31 *Philosophy & Technology* 379 <<http://link.springer.com/10.1007/s13347-017-0271-5>> accessed 22 January 2022.

³⁰Prof. S G Hélie, 'We need a Cyberspace Treaty' [2010] IIC

³¹ *Ibid* n31

Yohannes Eneyew Ayalew also proposes the establishment of a comprehensive and well-coordinated international legal machinery through the enactment of a universal treaty governing cyber warfare to deal with the novel challenges posed by cyber warfare.³² The author is keen to identify critical issues, such as attribution, that the application of cyber-armed conflict evokes. He does not look at the opportunities for states in the application of international law to cyber-armed conflict.

While the benefits of a treaty that could potentially govern cyber weapons and cyber-attacks should be considered, Chelsey Slack³³ points out that several fundamental issues, such as the dual-purpose nature of cyberspace, the lack of common definitions of terms, and the dynamic nature of this realm, make such an undertaking ultimately impractical.³⁴ As an alternative, she advocates for further work to be done in this area using a normative approach to better develop and unify existing political and strategic frameworks in this area.³⁵ Slack engages in a discussion about the benefits and the limitations of establishing a universal treaty to govern cyber-armed conflict in proposing the adoption of a normative approach to develop political and strategic frameworks in the area. She however does not highlight the positions taken by states on the application of international law to cyberspace and the challenges with this application.

While scholars have debated on the establishment of a universal treaty governing cyber space, the existing literature on the governance of cyberspace does not examine the positions of states on the application of international law to cyber space or cyber-armed conflict or address the challenges and opportunities for states in the application of international law to cyber-armed conflict. This study shall therefore be geared towards filling these gaps.

1.7 Research Methodology

The research employs a doctrinal approach to analyse the data and uses the desktop method of research. The study reviewed primary sources of data such as case law, regional agreements, treaties and protocols. The study also employed the use of secondary sources of data such as

³²Yohannes Eneyew Ayalew, 'Cyber Warfare: A New Hullabaloo under International Humanitarian Law' (2015) 06 Beijing Law Review 209 <<http://www.scirp.org/journal/doi.aspx?DOI=10.4236/blr.2015.64021>> accessed 21 October 2023.

³³Chelsey Slack, 'Wired yet Disconnected: The Governance of International Cyber Relations' (2016) 7 Global Policy 69 <<https://onlinelibrary.wiley.com/doi/abs/10.1111/1758-5899.12268>> accessed 20 October 2023.

³⁴Slack (n 34).

³⁵Slack (n 34).

the Tallinn Manual on the International Law Applicable to Cyberwarfare, scholarly books, articles, military manuals, reports, speech transcripts, position papers and newspaper articles on the application of international law to cyber-armed conflict.

To find the relevant books, journal articles, and other publications, several libraries were visited. The internet was used to supplement the data collected from the books, journal articles and publications obtained from these libraries.

1.8 Chapter Breakdown

This study is organized into four chapters. Chapter One introduces the study and gives a background of the emergence of cyberspace as a new frontier for conflict. It gives a statement of the problem with regard to the application of international law to cyberspace and to cyber-armed conflict. It sets the main and specific objectives of the study and gives the research questions to be answered through the study and at its conclusion. It reviews the literature in the area of study and details the research methodology that will be applied in the study.

Chapter Two introduces and contextualizes the concept of cyber-armed conflict. It traces the history of the debate on the application of international law to cyberspace and cyber-armed conflict. It introduces the Tallinn Manual on the International Law Applicable to Cyberwarfare. It then proceeds to analyse the Manual.

Chapter Three highlights the various positions taken by states on the application of international law to cyberspace. It proceeds to discuss the challenges and opportunities that accompany this application. Finally, it examines whether or not there is a need to establish a universal treaty governing cyberspace.

Finally, Chapter Four concludes the study and makes recommendations on the way forward on governance of cyber space.

CHAPTER TWO

2.0 INTERNATIONAL LAW ON ARMED CONFLICT IN CYBERSPACE

2.1. Introduction

It has been said that conflict is as old as humankind. It has in the past been fashioned as a tool for foreign policy. Armed conflict has resulted in the galvanization of social and political change in society. The inevitability of armed conflict for the human race, therefore, has resulted in the formulation of various laws within the international and regional plane to govern it. Cyberspace has become a novel territory on which states and non-states engage in conflict. Additionally, the dependence on information communication technology has made it imperative that there is international agreement on proper and improper behaviour in cyberspace. The arrival at this consensus has become one of the most critical policy issues of modern times.³⁶

The first comprehensive and authoritative attempt to analyse the application of international law to cyber warfare was instituted by the North Atlantic Treaty Organization (NATO), which brought together and assembled a working group of independent legal experts in 2009 to produce a manual on the international law applicable to cyber warfare. The culmination of this exercise was the Tallinn Manual on the International Law applicable to Cyberwarfare (the Manual). The Manual reflects the personal view of the experts engaged in its drafting and identifies principles of international law applicable to cyber warfare. While the Manual is not a legally binding instrument, it gives guidance and interpretations of international law principles in the context of cyber warfare. Accordingly, in the absence of a universal international treaty, this Manual will be the focus of this research project.

This chapter will set the backdrop for this research by defining and contextualizing ‘cyber armed conflict’. It will proceed to trace the history of the debate on the application of international law to cyberspace and cyber-armed conflict and give a brief history leading up to the drafting of the Tallinn Manual on the International Law Applicable to Cyberwarfare. It will then proceed give a thematic overview of the Manual and finally examine the value and demerits of the Manual.

³⁶Anders Henriksen, ‘The End of the Road for the UN GGE Process: The Future Regulation of Cyberspace’ (2019) 5 *Journal of Cybersecurity* ty009 <<https://doi.org/10.1093/cybsec/ty009>> accessed 26 August 2022.

2.2 What is Cyber Armed Conflict?

There is no treaty definition for the term ‘armed conflict’. The *International Criminal Tribunal for the Former Yugoslavia*³⁷ stated

“... an armed conflict exists whenever there is a resort to armed force between States or protracted armed violence between governmental authorities and organized armed groups or between such groups within the State.”

The Tribunal in *Prosecutor v. Kunarac, Kovac and Vukovic, IT-96-23 and IT-96-23/1-A (Appeals Chamber)* also took this position.³⁸

The British Ministry of Defence in the Joint Service Manual of the Law of Armed Conflict takes note of the fact that neither the Geneva Treaties nor Additional Protocol I contains any definition of the term ‘armed conflict’.³⁹ It has, however, directed that any difference between states that leads to the involvement of the armed forces is an armed conflict. Additionally, an armed conflict exists any time there is a recourse to armed force between states or extended armed violence between governmental authorities and organized armed groups within a state.

The term ‘armed’ puts forward a dilemma when dealing with cyber operations because they are not kinetic and do not engage what would usually be considered ‘weapons’.⁴⁰ On the face of it, a conflict that is solely fought through cyberspace (which definition includes but is not limited to cyber-attacks)⁴¹ would therefore not appear to be ‘armed’. However, it would be difficult to draw such a conclusion in the setting of cyber operations, which can have terrible, potentially fatal outcomes.⁴²

By the definitions of armed conflict above, the term ‘armed’ implies the use of forceful acts at any level. Thus, any cyber operation that amounts to an “attack” in International Humanitarian Law terms would qualify as ‘armed’.⁴³ Additional Protocol I in Article 49(1) defines attacks as

³⁷‘Decision on the Defence Motion for Interlocutory Appeal on Jurisdiction’ (1996) 7 Criminal Law Forum 51 <<http://link.springer.com/10.1007/BF02196556>> accessed 5 September 2022.

³⁸United Nations High Commissioner for Refugees, ‘Refworld | Prosecutor v. Dragoljub Kunarac, Radomir Kovac and Zoran Vukovic (Appeal Judgment)’ pp 16 (*Refworld*) <<https://www.refworld.org/cases,ICTY,3debaafe4.html>> accessed 15 October 2023.

³⁹‘Manual of the Law of Armed Conflict (JSP 383)’ (*GOV.UK*, 21 May 2014) <<https://www.gov.uk/government/collections/jsp-383>> accessed 19 September 2023.

⁴⁰M Schmitt, ‘Classification of Cyber Conflict’ (2012) 17 Journal of Conflict and Security Law 245 <<https://academic.oup.com/jcsl/article-lookup/doi/10.1093/jcsl/krs018>> accessed 24 June 2022.

⁴¹‘2017-Tallinn-Manual-2.0 (3).Pdf’.

⁴²Schmitt (n 41).

⁴³Schmitt (n 41).

acts of violence against the adversary regardless of whether they were conducted offensively or defensively.⁴⁴

Cyber operations are not inherently violent. However, these operations can produce violent consequences. To the extent that cyber operations may end in injury, death, or destruction of property, cyber operations satisfy the ‘armed’ criteria in armed conflict.⁴⁵ Thus, an attack is not defined by the violence of the means employed but by the violence of the consequences.⁴⁶

As stated by the International Committee of the Red Cross,⁴⁷ cyber operations can also constitute attacks even though they do not result in the destruction of the object. Additional Protocol I in its definition of ‘military objective’ not only refers to destruction or capture but also refers to ‘neutralization’ as a possible consequence of an attack.⁴⁸ The term “‘neutralization’ connotes that it matters not whether an object is disabled through its destruction or any other way.’ Cyber-armed conflict would therefore be constituted when the specific acts conducted through network attacks result in effects that reach a scale similar to the effects of kinetic armed attacks and eventually include destruction or other harmful effects.⁴⁹

2.3 History of the debate on the Application of International Law to Cyberspace and Cyber-Armed Conflict

It is now widely recognized that international law applies to cyberspace. Contrary to assertions made in the past, cyberspace is not “the Wild Wild West”.⁵⁰ It has generally been agreed that the law of armed conflict applies to cyber operations in the same way it would any other

⁴⁴Protocol Additional To The Geneva Conventions of 12 August 1949, And Relating to The Protection Of Victims of International Armed Conflicts (Protocol I), of 8 June 1977’.

⁴⁵Schmitt (n 41).

⁴⁶Irrc-886-Droege.Pdf’.

⁴⁷Laurent Gisel, Tilman Rodenhäuser and Knut Dörmann, ‘Twenty Years on: International Humanitarian Law and the Protection of Civilians against the Effects of Cyber Operations during Armed Conflicts’ (2020) 102 *International Review of the Red Cross* 287 <https://www.cambridge.org/core/product/identifier/S1816383120000387/type/journal_article> accessed 21 June 2023.

⁴⁸Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflicts (Protocol I)’ (*OHCHR*) <<https://www.ohchr.org/en/instruments-mechanisms/instruments/protocol-additional-geneva-conventions-12-august-1949-and>> accessed 27 March 2023.

⁴⁹Mateusz Piątkowski, ‘The Definition of the Armed Conflict in the Conditions of Cyber Warfare’ (2017) 46 *Polish Political Science Yearbook* 271.

⁵⁰Kubo Mačák, ‘Unblurring the Lines: Military Cyber Operations and International Law’ (2021) 6 *Journal of Cyber Policy* 411 <<https://doi.org/10.1080/23738871.2021.2014919>> accessed 22 August 2022.

operations that take place during an armed conflict. Initially, the development of norms regulating conduct in cyberspace was slow. However, as engagement of various actors with cyberspace picked up the pace, the debates and norms development in the area also gained traction.

The first cyberattack happened in 1834 when two thieves used the French telegraph system to steal money. About 150 years later, Robert Tappert Morris launched the first-ever denial-of-service assault by hacking into a computer at the Massachusetts Institute of Technology and releasing a “worm” into the network. Out of the estimated 60,000 computers that were online at the time the worm was released, about 6,000 were affected within 24 hours.⁵¹ While there were advances in cyber technology in the late 1980s and early 1990s, it was not until the early 2000s, when broadband internet access became the norm, that cyberspace matured into a business medium and a battlefield. Broadband allowed for the speedy transmission of large amounts of data, resulting in technological improvements and new applications for individuals, businesses, and governments.⁵²

Russia introduced a draft resolution in the First Committee of the General Assembly in 1998 noting how new technologies could be used in a destabilizing manner, jeopardizing the national security of states. It invited the United Nations member states to convey their opinions on the resolution to the United Nations Secretary-General.⁵³ Member States were invited to comment on the “advisability” of establishing international principles to improve the security of global Information Communication Technology systems.⁵⁴ After subsequent draft resolutions were introduced by Russia, the General Assembly requested the Secretary-General to form a group of governmental experts to report on the international concepts for “strengthening the security of global information and telecommunications systems.”

The first group of experts was established in 2002. This group was made up of fifteen members chosen based on an equitable geographical distribution. However, the report from the first group was never adopted.⁵⁵ This failure did not discourage the United Nations and its member

⁵¹‘The Morris Worm’ (*Federal Bureau of Investigation*) <<https://www.fbi.gov/news/stories/morris-worm-30-years-since-first-major-attack-on-internet-110218>> accessed 28 March 2023.

⁵²International Law in Cyberspace’ <https://www.americanbar.org/groups/law_national_security/publications/aba-standing-committee-on-law-and-national-security-60-th-anniversary-an-anthology/international-law-in-cyberspace/> accessed 28 March 2023.

⁵³Henriksen (n 37).

⁵⁴Henriksen (n 37).

⁵⁵Henriksen (n 37).

states. The Secretary-General established a second group of experts in 2005. Its mandate was to continue the study of ICT threats and possible cooperation measures.⁵⁶ By the time the group met in 2009, the 2007 cyberattacks on Estonia and Russia's cyber activities in its 2008 conflict with Georgia had made states acutely aware of the possibility of conflict in cyberspace.⁵⁷ The attacks by Russia also highlighted the risk posed by the lack of international consensus on governing principles in cyberspace. This Group of Experts reached an agreement, unlike the first group. Concerning the governance of cyberspace, the Report proposed that rules could be formulated with time to add to the existing norms and that further engagement on the topic

In December 2011, the General Assembly established a third group of experts whose specific task was to deliberate on norms, rules or principles of responsible state behaviour.⁵⁸ By that point, the 2010 Stuxnet attack on the Iranian nuclear program had revealed the potential of a focused covert cyber operation. A consensus report from the third UN GGE emphasized the importance of shared “understandings on norms, standards and principles related to the use of ICTs” for advancing peace and security.⁵⁹ More importantly, the Report noticed that the conduct of ICT-related activities by states and their authority over ICT infrastructure inside their territory is governed by international law, including the Charter of the United Nations and the principles of state sovereignty.

In September 2012, Harold Koh, the Legal Adviser to the United States Department of State delivered a speech that marked the first time the United States publicly announced its view that existing international law applies in cyber space.⁶⁰ The United Nations Group of Governmental Experts concurred with this American assessment in 2012. The 2012 Group of Experts arrived at the following conclusions: “State sovereignty and the international norms and principles that flow from sovereignty apply to State conduct” in cyberspace; “States must meet their international obligations regarding internationally wrongful acts attributable to them”; and

⁵⁶Henriksen (n 37).

⁵⁷Henriksen (n 37).

⁵⁸Henriksen (n 37).

⁵⁹Richard D Heideman, ‘Legalizing Hate: The Significance of the Nuremberg Laws and the Post-War Nuremberg Trials’ (2017) 39 Loyola of Los Angeles International and Comparative Law Review 5 <<https://heinonline.org/HOL/P?h=hein.journals/loyint39&i=32>> accessed 11 August 2022.

⁶⁰International Law in Cyberspace’ <https://www.americanbar.org/groups/law_national_security/publications/aba-standing-committee-on-law-and-national-security-60-th-anniversary-an-anthology/international-law-in-cyberspace/> accessed 28 March 2023.

“States must not use proxies to commit internationally wrongful acts.”⁶¹ Following the 2012 declarations, there was broad agreement that cyberspace is subject to international law. However, there was still a question as to how it applies precisely.⁶²

In July 2013, a fourth team of experts was formed. The experts elaborated on the applicability of international law to the use of ICTs by governments in a consensus report that they presented in July 2015. These experts went on to state that the UN Charter is applicable in its totality but that more research in the area is needed. The fifth and final panel of experts was established to clarify the regulation of cyberspace. However, this panel was unable to reach an agreement on a draft report. The attempt to acknowledge that International Humanitarian Law may govern online acts was opposed by some states.

Against the backdrop of the Stuxnet attack that had occurred in 2007 and while these discussions were going on at the United Nations, the Cooperative Cyber Defence Centre of Excellence (CCDCOE) of the North Atlantic Treaty Organization (NATO) assembled a working group of independent legal experts in 2009. This group was tasked with producing a manual on the international law applicable to cyber warfare. The goal of this assignment was to elucidate how existing international law could be interpreted and applied to cyber warfare. This assignment ran from 2009 and culminated in the 2013 Tallinn Manual on International Law Applicable to Cyberwarfare.⁶³

2.4 The Tallinn Manual on the International Law Applicable to Cyberwarfare

2.4.1 Drafting and Scope of the Manual

The task assigned to the Group was to produce a manual on cyber warfare under the observership of the International Committee of the Red Cross (ICRC) in recognition of the importance of state activity in cyberspace and the lack of public positions by states about the application of international law to cyberspace.⁶⁴ Academics, practitioners, observers from

⁶¹‘International Law in Cyberspace’ (U.S. Department of State) <://2009-2017.state.gov/s/l/releases/remarks/197924.htm> accessed 22 June 2022.

⁶²‘International Law in Cyberspace’ (n 62).

⁶³Schmitt, MN (ed), *Tallinn Manual on the International Law Applicable to Cyber Warfare* (Cambridge University Press 2013) <<https://www.cambridge.org/core/books/tallinn-manual-on-the-international-law-applicable-to-cyber-warfare/50C5BFF166A7FED75B4EA643AC677DAE>> accessed 27 June 2023.

⁶⁴Sergei Yu Garkusha-Bozhko and Гаркуша-БожкоСергейЮльевич, ‘Application of the Principles of International Humanitarian Law (Principles of Distinction, Proportionality, and Precaution) to Armed Conflicts

NATO's Allied Command Transformation, the International Committee of the Red Cross, and technical specialists were among those who contributed to the preparation of the Tallinn Manual. The membership of the group was drawn from countries including Canada, Australia, United States, Belgium, Sweden, Netherlands and the United Kingdom.

The Manual addresses cyber operations that breach the prohibition against the use of force, those that entitle a state to exercise its right to self-defence or those that happen during an armed conflict.⁶⁵ Without a universal treaty governing cyberwar, the Tallinn Manual on the International Law Applicable to Cyberwarfare offers some level of clarity on the difficult issues relating to cyber operations. The intention was to premise the Manual on existing law. It was never intended to refer to an altogether new law.⁶⁶ The Rules contained in the Manual mirror existing treaties or customary international law and illustrate how those regimes apply to state actors in cyberwarfare.

2.4.2 The Composition of the Tallinn Manual.

The Tallinn Manual scrutinizes the international law governing cyber 'warfare'. It includes *jus ad bellum* and *jus in bello*. The Manual's emphasis is on cyber-to-cyber operations and it deals with international and non-international armed conflicts. It covers international and non-international armed conflict. The Manual contains ninety-five rules that expound on the experts' views on different legal issues.

2.4.3 Issues Emerging from the Application of International Law to Cyber-Armed Conflict

2.4.3.1 Scope of Application of International Law to Cyber Armed Conflict

There is no international treaty that deals with cyber armed conflict or cyberwarfare. This however does not suggest that hostile cyber operations exist in a legal vacuum. The law of armed conflict governs cyber activities performed in the setting of an armed conflict. The Tallinn Manual defines 'armed conflict' as any circumstance involving hostilities, including

in Cyberspace' (2021) 8 Russian Journal of Legal Studies (Moscow) 73 <<https://doi.org/10.17816/RJLS71332>> accessed 7 September 2022.

⁶⁵Schmitt, MN (n 64).

⁶⁶Garkusha-Bozhko and Юльевич (n 65).

those carried out through cyberspace. For example, cyber activities against Estonia in 2007 did not trigger the application of the law of armed conflict since the situation did not reach the threshold of an armed conflict. Cyber operations carried out during Georgia's armed conflict with Russia, on the other hand, prompted the application of the law of armed conflict because they were carried out in furtherance of the conflict between the two states.⁶⁷

When ongoing kinetic hostilities amount to an armed conflict, cyber actions done in relation to the conflict will be governed by the laws of armed conflict.⁶⁸ The Group of Experts at Tallinn agreed that there must be a link between the cyber activity in question and the armed conflict in order for the law of armed conflict to apply to it.⁶⁹ However, there was disagreement about the nature of the link between cyber activity and armed conflict. One faction of the Group of Experts held that the law of armed conflict governs any cyber activity done by a party to the armed conflict against its adversary. The opposing section of the Group believed that the cyber activity had to have been carried out in advancement of the war. With regard to the application of the law of armed conflict to cyber activities conducted during armed conflict by either of the parties, it should be instructive whether or not the cyber activity in question was conducted in furtherance of the hostilities or whether the cyber activity resulted in injury, damage, death, destruction or neutralization of property.

The lack of a treaty provision or custom regulating cyber-attacks or cyber weapons has invited assertions from some quarters that this absence in effect means that the law does not apply to cyber-attacks and that states have been given a free hand to operate as they please in this field. This proposition was however rejected by the in the International Court of Justice in the *Legality of the Threat or Use of Nuclear Weapons*⁷⁰. The Court invoked "the Martens Clause" which provides that:

“Until a more complete code of the laws of war has been issued, the High Contracting Parties deem it expedient to declare that, in cases not included in the Regulations adopted by them, the inhabitants and the belligerents remain under the protection and the rules of the principles of the law on nations, as they result

⁶⁷Schmitt, MN (n 64).

⁶⁸Schmitt, MN (n 64).

⁶⁹Schmitt, MN (n 64).

⁷⁰*Legality of the Threat or Use of Nuclear Weapons (Advisory Opinion)*, ICJ Reports (1996), pp 226-267

from the usages established among civilized peoples, from the laws of humanity, and the dictates of the public conscience.”⁷¹

This statement by Fyodor Fyodorovich Martens, now popularly known as ‘the Martens Clause’, is a confirmation that even in the absence of codified laws and regulations, cyber activities conducted in the course of or in furtherance of an armed conflict are not conducted in a legal void. Furthermore, the pertinent articles of international law that apply during an armed conflict place geographical restrictions on cyber operations. The geographical area in which cyber operations may be carried out is set forth by the rules of armed conflict in combination with other areas of international law. Relevant considerations include the origin of cyber actions, the location of any required instruments, and the target cyber systems.⁷² The idea is that cyber operations can be carried out from, on, or with consequences in the whole territories of the conflicting parties, in international airspace or waterways, and, with some restrictions, in outer space.⁷³

Any conflicts between two or more governments, including but not limited to cyber operations, constitute an international armed conflict. The 1949 Geneva Treaties’ Common Article 2, states that the Treaty “shall apply to all cases of declared war or of any other armed conflict, which may arise between two or more of the High Contracting parties regardless of whether or not they recognise the state of armed conflict.”⁷⁴

When the Manual was being authored, the Group of Experts adopted the position that an armed conflict qualifies as international if two or more States are participating on rival sides.⁷⁵ The experts also concurred that when non-state actors acting under the ‘overall control’ of one state engage in conflict with another state the conflict is likewise, international.⁷⁶ The International Criminal Tribunal discussed the issue of ‘overall control’ for the Former Yugoslavia in the *Tadic*⁷⁷ case. The Chamber stated that in order to attribute the actions of a military or paramilitary group to a State, it must be demonstrated unequivocally that the State exercises

⁷¹Schmitt, MN (n 64).

⁷²Schmitt, MN (n 64).

⁷³Schmitt, MN (n 64).

⁷⁴‘Geneva Convention Relative to the Protection of Civilian Persons in Time of War’.

⁷⁵Schmitt, MN (n 64).

⁷⁶Schmitt, MN (n 64).

⁷⁷*Prosecutor vs. Dusko Tadic*, IT-94-1-A, Appeals Judgement, 15 July 1999, pp. 59.

'overall control' over the group, not only by equipping and financing it but also by directing or assisting in the general planning of its military activity.⁷⁸ The Chamber further stated that

“The control required under international law may be deemed to exist when a state (or, in the context of an armed conflict a party to the conflict) has a role in organizing, coordinating or planning the military actions of the military group, in addition to financing, equipping, training or providing operational support to that group.”

The International Court of Justice responded to the *Tadic* judgement in the *Bosnia Genocide Case*⁷⁹ where the Court reiterated that while the ‘overall control’ test may be appropriate in the context of deciding whether or not an armed conflict was international, it was not suitable for determining issues of state responsibility.

The Court stated that the overall control test may be used for the classification of armed conflict. The International Criminal Court in the *Lubanga Case*⁸⁰ adopted this position. The Group of Experts agreed that the threshold for the internationalization of armed conflict is high. Illustratively, they stated that the provision of specific intelligence by a state on cyber vulnerabilities of another state to rebels to render a cyber-attack by the rebels possible would meet the threshold of internalization of that armed conflict. On the other hand, taking steps to retain rebel access to the national cyberinfrastructure would not suffice.⁸¹ Furthermore, neither individuals nor improperly organized groups are eligible for the overall control test. To find the presence of an international armed conflict, the International Criminal Tribunal for the Former Yugoslavia opined that such persons or groups needed to acquire specific orders or subsequent authorisation from a State.⁸²

Common Article 3 of the Geneva Treaties provides that non-international armed conflicts are armed conflicts which involve one or more non-State armed groups. Subject to the circumstances, hostilities may erupt between government armed forces and non-state armed groups, or exclusively between non-state armed organizations. Furthermore, two

⁷⁸ *ibid*

⁷⁹ *Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Bosnia and Herzegovina vs. Serbia and Montenegro)* Judgment, ICJ. Rep. 2007, pp. 43.

⁸⁰ Judge Adrian Fulford and Judge René Blattmann, ‘*Situation in the Democratic Republic Of The Congo In The Case Of the Prosecutor V. Thomas Lubanga Dyilo*’, ICC-PIDS-CIS-DRC-01-010/2012, pp. 247

⁸¹ Schmitt, MN (n 64).

⁸² ‘Non-International Armed Conflict | How Does Law Protect in War? - Online Casebook’ <<https://casebook.icrc.org/glossary/non-international-armed-conflict>> accessed 12 September 2022.

characteristics must be met for such incidents to be categorized as non-international armed conflicts.⁸³

1. The hostilities must intensify to a certain minimum. This might be the case, for instance, when there are multiple parties involved in the conflict or when the government is compelled to utilize military force against the insurgents rather than only the police.
2. Non-governmental groups that are actively engaged in the conflict must be regarded as “party to the conflict,” which means that they are in control of organized armed forces. This implies, for instance, that these troops must fall under a specific command structure and possess the capability of supporting military operations.⁸⁴

According to this clause, non-governmental parties must exert such territorial control “as to enable them to carry out prolonged and coordinated military actions and to implement this Protocol.”⁸⁵ Additional Protocol II specifically states that it only applies to armed conflicts involving State armed forces and armed dissidents or other organized armed groups. Unlike common Article 3, the Protocol does deal with armed situations that only include non-State armed organisations.⁸⁶

A level of organization in the armed group is mandatory for a non-international armed conflict to exist. This organization may be demonstrated by the presence of a command structure and disciplinary rules and mechanisms, the ability to obtain and distribute arms and the ability to negotiate agreements. In the absence of organization, the criteria are not met and armed conflict does not exist.⁸⁷

The application of the law of armed conflict does not depend on the means and methods of warfare involved in the conflict.⁸⁸ This, therefore, makes room for the law of armed conflict to be applied to cyber operations.⁸⁹ It can therefore be stated that absent of any kinetic means of

⁸³‘Non-International Armed Conflict | How Does Law Protect in War? - Online Casebook’ <<https://casebook.icrc.org/glossary/non-international-armed-conflict>> accessed 12 September 2022.

⁸⁴‘Non-International Armed Conflict | How Does Law Protect in War? - Online Casebook’ .

⁸⁵‘Non-International Armed Conflict | How Does Law Protect in War? - Online Casebook’ (n 85).

⁸⁶‘Non-International Armed Conflict | How Does Law Protect in War? - Online Casebook’ (n 85).

⁸⁷‘Non-International Armed Conflicts in Democratic Republic of Congo | Rulac’ <<https://www.rulac.org/browse/conflicts/non-international-armed-conflict-in-democratic-republic-of-congo>> accessed 12 September 2022.

⁸⁸Rule 23, Schmitt, MN (n 64).

⁸⁹Schmitt, MN (n 64).

warfare, an armed conflict that purely involves cyber operations could trigger application of the laws of armed conflict..

2.4.3.2 The Concept of an ‘Attack’

According to the Manual, a cyber-attack is an offensive or defensive cyber operation that is logically estimated to result in injury or death to persons or destruction to objects.⁹⁰ A cyber operation is defined as “the employment of cyber capabilities with the primary purpose of achieving objectives in or by the use of cyberspace”.⁹¹ The term ‘attack’ is defined in Article 49(1) of Additional Protocol I to mean, “Acts of violence against the adversary, whether in offence or defence”.⁹² It is apparent that the use of force against a target is what makes attacks different from other military operations. Attacks, including cyber operations that do not involve force are not considered attacks. The outcomes of an operation and not the inherent nature of the operation are what qualifies it as an attack. According to the experts, *de minimis* damage or destruction does not satisfy the standard of injury required by this rule.⁹³

The Experts at Tallinn were of the view that whenever an attack on data results in the injury or death of an individual, or damage to physical objects, those individuals or objects are ‘the object of an attack’. The Experts also opined that acts of violence, or those having violent effects aimed at civilians or civilian objects of other protected persons or objects are attacks. The experts were divided as to whether interference with functionality achieved by the use of cyber means amounted to destruction or damage. One group was of the opinion that it does not while the other group took the view that interference with functionality qualifies as damage if restoration of functionality requires replacement of physical components. The experts were unable to conclusively resolve this matter.

According to the experts, a cyber operation that is stopped and does not end in any real harm is still an attack according to International Humanitarian Law. Similarly, even where the target

⁹⁰ Rule 30, Schmitt, MN (n 64).

⁹¹Schmitt, MN (n 64).

⁹²‘Protocol Additional To The Geneva Conventions of 12 August 1949, And Relating to The Protection Of Victims of International Armed Conflicts (Protocol I), of 8 June 1977’ (n 45).

⁹³Schmitt, MN (n 64).

of a cyber-attack does not realise that there has been an attack, the cyber operation in question still qualifies as an attack notwithstanding the ignorance of the target.⁹⁴

The Tallinn Manual experts noted that Articles 51 and 52 of Additional Protocol I stipulate protections for the civilian population and civilian objects. They opined that some operations against the civilian population are not proscribed. These include psychological operations such as making propaganda. Contextualizing this to cyber warfare, conveying emails to the civilian enemy population encouraging surrender would not be a contravention of the laws of armed conflict. However, when an operation against a civilian population or civilian objects escalates to the level of an attack it is proscribed under International Humanitarian Law.⁹⁵

2.4.3.2.1 Precautions

In hostilities involving cyber operations, constant attention must be paid to the protection of civilians, civilian individuals and civilian objects.⁹⁶ Due to the intricacy of cyber operations, those planning missions should, where possible, engage technical experts to help them in deciding whether appropriate precautionary steps have been taken. The Manual provides that planners or those who decide upon a cyber-attack shall do all that they can to ensure that the objectives to be attacked are not civilian or civilian objects and that they are not subject to special protection.⁹⁷

Furthermore, if it becomes clear that the goal of a cyber-attack is not military or is subject to special protection, or that the attack is likely to result in civilian casualties, injury to civilians, damage to civilian objects, or a combination of these, those responsible for planning, approving, or carrying out the cyber-attack are expected to cancel or postpone it.⁹⁸ For cyber-attacks that may affect the civilian population, effective advance warning must be given unless circumstances do not permit.⁹⁹

⁹⁴Schmitt, MN (n 64).

⁹⁵Schmitt, MN (n 64).

⁹⁶ Rule 52, Schmitt, MN (n 64).

⁹⁷ Rule 53, Schmitt, MN (n 64).

⁹⁸ Rule 57, Schmitt, MN (n 64).

⁹⁹ Rule 58, Schmitt, MN (n 64).

2.4.3.2.2 Conduct of Attacks

The Manual prohibits cyber-attacks that are not aimed at a lawful target and consequently are of a nature to strike lawful targets and civilians or civilian objects without distinction. In the application of this Rule, a distinction must be made between an indiscriminate attack and an attack intentionally directed towards civilians and civilian objects. An indiscriminate attack is unlawful whether it is successful or not. A cyber-attack that regards multiple clearly separate cyber military objectives in cyber infrastructure primarily utilized for civilian purposes as a single target is illegal if doing so would endanger protected persons or objects.¹⁰⁰ A cyber-attack on a dual-use cyber system would be illegal if its individual military components could have been attacked separately.

The Manual states that a cyber-attack that is projected to inflict secondary loss of civilian life, injury to civilians, damage to civilian objects, or a combination of these, is banned if it is disproportionate to the tangible and direct military gain anticipated.¹⁰¹ The fact that civilians or civilian objects are harmed during a cyber-attack does not necessarily make that attack unlawful. The lawfulness of the attack depends on the connection between the harm the attacker realistically expects to cause to civilians and civilian objects incidentally and the military advantage that he or she expects predicts to achieve. Only collateral damage (direct and indirect effects) that is disproportionate to the projected tangible and direct military advantage is prohibited. The requirement of a ‘direct and concrete’ military advantage tasks decision-makers to anticipate real and quantifiable benefits.

In determining proportionality, the International Criminal Tribunal for the Former Yugoslavia in the *Galic* judgement¹⁰², the Tribunal held:

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

¹⁰⁰ Rule 50, Schmitt, MN (n 64).

¹⁰¹ Rule 51, Schmitt, MN (n 64).

¹⁰²United Nations High Commissioner for Refugees, ‘Refworld | *Prosecutor v. Stanislav Galic* (Trial Judgement and Opinion)’ (*Refworld*) <<https://www.refworld.org/cases, ICTY,4147fb1c4.html>> accessed 4 June 2023.

2.4.3.2.3 Attacks against persons

The principle of distinction codified in Article 51(2) of Additional Protocol I¹⁰³ and Article 13(2) of Additional Protocol II dictates that civilians should not be made the target of a cyber attack.¹⁰⁴ To be proscribed by this Rule, a cyber operation must satisfy the criteria of an attack as earlier set out. The ‘object’ of a cyber-attack is the person against whom that attack has been launched. Civilians however lose their protection under this rule if and when they take direct part in hostilities.¹⁰⁵ In case of uncertainty about the civilian status of a person, that person shall be deemed a civilian.¹⁰⁶

In the cyber environment, the issue of doubt is a crucial one. In many countries, computer networks and computers are prevalent and the networks used by civilians and those used by members of the armed forces may be adjoined. In these instances, computer use or the use of a certain network may not signify military status on its own. This problem is further aggravated because individuals may not always be physically visible while undertaking cyber activities.¹⁰⁷

Members of the armed forces, members of organised armed groups, civilians directly participating in hostilities and, in the case of an international armed conflict, participants in a mass deployment can all become targets of cyberattacks.¹⁰⁸ A person’s status or behaviour may make him liable to attack. The targetability of members of the armed forces and members of armed groups depends on their status, while the targetability of civilians directly participating in hostilities and of participants in a *levee en masse* depends on the conduct of the individual.¹⁰⁹

Medical or religious personnel, who are members of the armed forces or those who are *hors de combat*, may not be attacked. Persons who are wounded or sick and are not involved in hostile acts or attempting to flee, or have been captured or have yielded are *hors de combat*.¹¹⁰ A group of civilian government employees who conduct cyber operations during an armed conflict

¹⁰³Protocol Additional To The Geneva Conventions of 12 August 1949, And Relating to The Protection Of Victims of International Armed Conflicts (Protocol I), of 8 June 1977’ (n 45).

¹⁰⁴Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of Non-International Armed Conflicts (Protocol II)’ (*OHCHR*) <<https://www.ohchr.org/en/instruments-mechanisms/instruments/protocol-additional-geneva-conventions-12-august-1949-and-0>> accessed 30 June 2023.

¹⁰⁵ Schmitt, MN (n 64).

¹⁰⁶ Rule 33 Schmitt, MN (n 64).

¹⁰⁷Schmitt, MN (n 64).

¹⁰⁸ Rule 34 Schmitt, MN (n 64).

¹⁰⁹Schmitt, MN (n 64).

¹¹⁰Schmitt, MN (n 64).

qualify as an armed group and its members are subject to attack. Other civilian government employees are targetable only when they participate directly in the hostilities.

2.4.3.2.4 Certain Persons, Objects and Activities

Respect and protection must be accorded to medical and religious personnel, medical units and medical transports. They may not be made the object of cyber-attack.¹¹¹ Actions that obstruct them from carrying out their functions or otherwise adversely affect their humanitarian functions breach the duty to ‘respect and protect’ them.

Attacks may not be mounted against medical computers, computer networks and data that form an important part of the operations or administration of medical units and transports.¹¹² Computers, computer networks and data that form a key part of the operations of a medical unit should be properly identified through appropriate means, which may include electronic markings.¹¹³ The protection accorded to these units does not stop unless they are used to commit acts that are harmful to the enemy.¹¹⁴

2.4.3.2.5 United Nations Personnel, Installations, Materiel Units and Vehicles

United Nations personnel, installations, materiel, units and vehicles including computers and computer networks that support the Organisation’s work must be respected and protected as long as they are entitled to the protection accorded to civilian and civilian objects under International Humanitarian Law.¹¹⁵ This prohibition also applies to persons or locations placed under the protection of the United Nations in the discharge of its mandate. Kinetic or cyber-attacks against United Nations personnel are prohibited if the United Nations is not a party to the conflict and as long as its forces or civilian personnel do not take direct part in the hostilities.

¹¹¹ Rule 70, Schmitt, MN (n 64).

¹¹² Rule 71, Schmitt, MN (n 64).

¹¹³ Rule 72, Schmitt, MN (n 64).

¹¹⁴ Rule 73, Schmitt, MN (n 64).

¹¹⁵ Rule 74 Schmitt, MN (n 64).

2.4.3.2.6 Collective Punishment and Humanitarian Assistance

Collective punishment by cyber means is proscribed. This rule prohibits the use of cyber means to inflict revengeful punishments on persons or groups for actions they did not participate in.¹¹⁶ Seizure of all personal computers belonging to civilians in retaliation for cyber-attacks conducted by some insurgents, for example, would be a violation of this prohibition on collective punishment. The design or conduct of cyber operations to hinder impartial efforts to provide humanitarian assistance is outlawed.¹¹⁷

2.4.3.2.7 Attacks against Objects

The Manual prohibits civilian objects from being made the target of cyber-attacks. However, computers, computer networks and cyber infrastructure may be attacked if they are military objectives. Further, all objects that are not used for military purposes are considered civilian objects. Military objectives are objects that, due to their position, purpose, or function, effectively support military action and whose destruction, capture, or neutralization, depending on the current situation, delivers a clear military advantage. Computers, computer networks, and cyberinfrastructure may be used for military purposes.¹¹⁸

Objects used for civilian and military purposes are military targets.¹¹⁹ There are instances where civilians and military personnel share cyberinfrastructure and computer networks. An object becomes a military objective whenever it has been or will be used in a way that supports military action. The status given as a civilian object and a military objective cannot co-exist. Accordingly, all dual-use infrastructure and objects automatically qualify as military targets.

Cyber networks are problematic in this respect. Where a network is used for civilian and military functions, it may not be possible to distinguish which part of the network military transmissions, as separate from civilian ones, will pass. In such a case, the whole network qualifies as a military objective.¹²⁰

¹¹⁶ Rule 85, Schmitt, MN (n 64).

¹¹⁷ Rule 86, Schmitt, MN (n 64).

¹¹⁸ Rule 38, Schmitt, MN (n 64).

¹¹⁹ Rule 39, Schmitt, MN (n 64).

¹²⁰ Schmitt, MN (n 64).

Social networks have also been put to use for military purposes. Facebook and Twitter have been used for the organization of armed resistance movements and transmission of information of military value respectively. Three major issues arise when applying this Rule to such networks. First, this criterion is unaffected by the proportionality rule or the duty to take measures during an attack. Second, the legality of cyber operations against social networks is determined by whether the actions constitute an attack. If they do not, the issue of qualifying as a military target is avoided. Third, the military use of social media does not imply that they will be targeted as such. Only those used for military reasons are subject to attack.¹²¹

When there is doubt as to whether an object normally devoted to civilian purposes will be used to contribute effectively to a military action, a decision can only be taken after careful consideration.¹²² Article 52(3) of Additional Protocol I provides that if there is uncertainty whether an object which is usually used for civilian purposes is being used to make an actual contribution military action, the presumption shall be that it is not used as such.¹²³ This therefore means that doubt is legally determined in favour of civilian status.

Those who plan authorise or carry out an attack must ensure that the targets to be attacked are not civilian objects or subject to special protection. In case of uncertainty, those involved in the operation should seek more information. This rule is applicable to things that are typically used for civilian purposes. The phrase “normally dedicated” means that the item has not been regularly or meaningfully used for military objectives in any regular or considerable way. An object’s civilian status is not permanently lost due to infrequent or minor military use. The conversion of an object for military use does not require absolute certainty. What is needed is enough reliable information to convince a commander to believe the opponent is employing the possible target for military objectives, or to effectively support military action.¹²⁴

2.4.3.2.8 Installations Containing Dangerous Forces

When conducting cyber-attacks against works and installations containing dangerous forces, care must be taken to avoid their release and consequent grave losses among the civilian

¹²¹Schmitt, MN (n 64).

¹²²Rule 40 Schmitt, MN (n 64).

¹²³Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflicts (Protocol I)’ (n 45).

¹²⁴ Schmitt, MN (n 64).

population.¹²⁵ This law applies to dams, dykes, nuclear power plants, and military objectives located nearby, as well as computers and computer systems that are a significant part of and support the functioning of such works or facilities.

2.4.3.2.9 Objects Indispensable to the Survival of the Civilian Population

It is prohibited to employ cyber operations to attack, destroy, remove, or render unusable objects critical to the existence of the civilian population.¹²⁶ These objects include livestock, crops, drinking water installations and irrigation works. It includes cyber infrastructure required for the operation of electricity generators, irrigation works and installations, drinking water installations, and food producing facilities in the cyber context.

2.4.3.2.10 Cultural Property

Cultural property that may be affected by cyber operations or that is located in cyberspace must be respected and protected by parties to an armed conflict.¹²⁷ They are, in particular, banned from using digital cultural property for military purposes. Cultural property comprises movable and immovable property of the greatest importance for humanity. Digital cultural property may be made the subject of attack if it qualifies as a military objective. However, such a decision to attack cultural property must be taken at an appropriately high level.¹²⁸

2.4.3.2.11 The Natural Environment and Diplomatic Archives and Communications

The natural environment enjoys general protection accorded to civilian objects against cyber-attacks and their effects since it is a civilian object. States that are party to Additional Protocol I are barred from using cyber methods or means of warfare which are envisioned or may be anticipated to cause extensive, long-term and serious damage to the natural environment.¹²⁹ For

¹²⁵ Rule 80, Schmitt, MN (n 64).

¹²⁶ Rule 81, Schmitt, MN (n 64).

¹²⁷ Rule 82, Schmitt, MN (n 64).

¹²⁸ Rule 82, Schmitt, MN (n 64).

¹²⁹ Rule 83, Schmitt, MN (n 64).

example, it would be unlawful to use cyber means to trigger a release of oil into a waterway to cause damage to the environment.

Diplomatic archives and communications are safeguarded against cyber-attacks.¹³⁰ This includes maintaining their confidentiality, integrity, and availability. Parties to a conflict are expected to refrain from any action that might interfere with or harm their transmission or maintenance.

2.4.3.3 Direct Participation in Hostilities

2.4.3.3.1 Participation in Armed Conflict in General

The law of armed conflict does not prohibit anyone from participating in cyber operations. However, the legal repercussions vary depending on the nature of the armed conflict and the category to which a person belongs.¹³¹ The law of armed conflict does not impose limitations on who can engage in armed conflict. For the purposes of the principle of distinction, members of State armed forces may be regarded as combatants in both international and non-international armed conflicts.¹³²

This Rule's application excludes members of the armed forces, participants in a *levee en masse*, and members of armed groups since they are not 'civilians'. The application of this Rule only applies to individuals who participate in armed conflict without any association to any such group and to individuals who are members of *ad hoc* groups that fail to meet the criteria of an 'organized armed group'.

Direct participation in armed hostilities leaves civilians vulnerable to attack, whether through cyberattacks or other lawful means. Moreover, when considering harm to civilians or the safeguards that must be taken to avoid harm to them during operations by the military, harm to direct participants is not considered. There is no definition of 'direct participation' in International Humanitarian Law. The International Committee of the Red Cross issued Interpretive Guidance, which provides recommendations on the interpretation of International Humanitarian Law with respect to the idea of 'direct participation.'¹³³ Direct participation in

¹³⁰ Rule 84, Schmitt, MN (n 64).

¹³¹ Rule 25, Schmitt, MN (n 64).

¹³² Rule 25, Schmitt, MN (n 64).

¹³³ 'Direct Participation in Hostilities | How Does Law Protect in War? - Online Casebook' (n 114).

hostilities refers to particular acts performed by individuals as part of the conduct of hostilities between armed conflict parties.¹³⁴

A particular act must satisfy all of the following requirements to be considered direct participation in hostilities:¹³⁵

- a) the conduct must have the potential to negatively impact a party's military operations or military capacity, or to cause death, damage, or destruction to people or property that is shielded from direct attack (threshold of harm);
- b) a direct contributory relationship must exist between the conduct and the harm anticipated to stem from that act or from a planned military operation in which that act plays a key role; and
- c) The act must be explicitly intended to create the necessary amount of injury in favour of one party to the conflict and against another, and it must do so directly (belligerent nexus).

In the absence of a requirement of physical damage to objects or harm to individuals, actions that do not qualify as a cyber-attack will meet this requirement as long as they adversely affect the rival military.¹³⁶ For the duration of a civilian's direct involvement in hostilities, a civilian may be attacked directly as if he were a combatant.¹³⁷ The duration of a person's direct participation in hostilities starts from the beginning of his involvement in operational planning to the end of his active role in the operation.

Performing cyber-attacks related to an armed conflict is direct participation in the armed conflict. The requirement of belligerent connection disqualifies acts of a criminal or private nature that take place during hostilities.

Cyber-attacks or the threats thereof, which are aimed primarily at spreading terror among the civilian population, are prohibited.¹³⁸ For a cyber operation to be deemed to be in breach of this rule, it must amount to a cyber-attack. A cyber-attack against a public transport system that

¹³⁴'Direct Participation in Hostilities | How Does Law Protect in War? - Online Casebook' (n 114).

¹³⁵'Direct Participation in Hostilities | How Does Law Protect in War? - Online Casebook' (n 114).

¹³⁶ Schmitt, MN (n 64).

¹³⁷'Direct Participation in Hostilities | How Does Law Protect in War? - Online Casebook' (n 114).

¹³⁸ Rule 36 Schmitt, MN (n 64).

leads to death or injury violates this Rule if the main aim of the attack was to terrorize the civilians.

In the absence of a definition of the term “civilian” in non-international armed conflicts, the drafters of the Tallinn Manual defined the term in relation to non-international armed conflicts as persons who are not members of the armed forces of the state, dissident armed forces or other organised armed groups.¹³⁹ Since the law of armed conflict does not proscribe participation in non-international armed conflict, special prohibitions apply to all those who actively participate in hostilities, such as attacking persons who are not actively participating in the armed conflict. In addition, civilians are subject to prosecution under the national law of the state that apprehends them.¹⁴⁰

2.4.3.3.2 Members of the Armed Forces

International Humanitarian Law recognizes two classes of combatants. The first class is members of the armed forces of a party to the hostilities and members of militias or volunteer corps that make up part of the armed forces. The second is other militias and members of other volunteer corps including members of armed resistance movements belonging to a party to the armed conflict.¹⁴¹

Members of a party's armed forces, with the exception of chaplains and medical staff, are combatants in international armed conflict, meaning they have the right to participate directly in armed conflict.¹⁴² Participants in a *levee en masse* are also recognised as combatants and have the right to participate directly in hostilities.¹⁴³ Although there is no limitation as to who can take part in armed conflict, there are consequences that result from direct participation in armed conflict. The entitlement of an individual to Prisoner of War status and combatant immunity depends on whether that person is a lawful combatant in an international armed conflict. Combatants enjoy immunity against prosecution for acts that would otherwise, during peacetime, be criminal offences. This exception however does not apply to war crimes.¹⁴⁴

¹³⁹Schmitt, MN (n 64).

¹⁴⁰Schmitt, MN (n 64).

¹⁴¹Rule 25, Schmitt, MN (n 64).

¹⁴² Rule 25, Schmitt, MN (n 64).

¹⁴³ Rule 27, Schmitt, MN (n 64).

¹⁴⁴‘Combatants | How Does Law Protect in War? - Online Casebook’ <<https://casebook.icrc.org/glossary/combatants>> accessed 17 October 2022.

This immunity allows combatants to conduct lawful acts of war such as killing or wounding enemy combatants and destroying enemy property as long as they are part of lawful military engagement.¹⁴⁵ Upon capture, combatants are given Prisoner of War status, which accords them various protections such as protection from physical violence and the right to receive and send correspondence to their family under the Third Geneva Treaty.¹⁴⁶

Whereas computer network attacks enable the use of “cyber militia” and provide a State with the appeal of “plausible deniability”, the participants will not be considered legitimate soldiers unless a relationship between the organization and the State can be proven.¹⁴⁷ It would not be necessary for the State’s regular armed forces to demonstrate such a connection, but it is unclear how much control is necessary over organized internet groupings.

If a person involved in an armed conflict is a member of an organised armed group that is not a party to the conflict, it is irrelevant whether the group and its members meet the four conditions of combatancy.¹⁴⁸ The individual in question does not have combatant status and therefore does not qualify for combatant immunity or treatment as a Prisoner of War.

2.4.3.3.3 *Levees en Masse*

According to the Manual, occupants of an unoccupied territory who engage in cyber operations as part of a *levee en masse* enjoy combatant protection and Prisoner-of-War status in an international armed conflict.¹⁴⁹ A *levee en masse* occurs where “inhabitants of a non-occupied territory on the approach of the enemy spontaneously take up arms to resist the invading forces.” When a *levee en masse* occurs, individuals who were otherwise deemed civilians are transformed into combatants and are granted the rights and obligations of combatant status.

When Russia recently invaded Ukraine, the Ukrainian President called on people to support Ukraine noting that his government would give weapons to anyone willing to defend the country. In response to this call, Ukrainians rose in defence of their country alongside the

¹⁴⁵ Rule 26, Schmitt, MN (n 64).

¹⁴⁶ Rule 26, Schmitt, MN (n 64).

¹⁴⁷ ‘The Application of the Principle of Distinction in the Cyber Context: A Chinese Perspective’ (*International Review of the Red Cross*) <<http://international-review.icrc.org/articles/principle-of-distinction-cyber-context-chinese-perspective-913>> accessed 18 October 2022.

¹⁴⁸ Rule 26, Schmitt, MN (n 64).

¹⁴⁹ Rule 27, Schmitt, MN (n 64).

country's formal armed forces.¹⁵⁰ In addition to those who took up arms as a response to the call, there were reports of Ukrainian citizens, on their accord buying guns and booking times at shooting ranges in preparation for the invasion.¹⁵¹ Although most Ukrainians responded by taking up arms, some Ukrainians responded by launching cyber-attacks through which electronic attacks against Russian forces and the Russian state were mounted.¹⁵²

2.4.3.3.4 Mercenaries and Civilians

Mercenaries who take part in cyber operations do not enjoy combatant immunity or Prisoner-of-War status.¹⁵³ Civilians are not forbidden from directly participating in cyber operations that amount to hostilities; however, they lose their immunity from attack while doing so.¹⁵⁴ In addition, citizens who actively participate in hostilities may be prosecuted and punished to the degree that their actions, affiliation with a group, or injury they caused are illegal under domestic law.¹⁵⁵

2.4.3.4 The Principle of Distinction

According to the Manual, the principle of distinction applies to cyber a distinction applies to cyber-attacks.¹⁵⁶ This principle draws its origin from the 1868 St. Petersburg Declaration, which stipulates “the only legitimate object which states should endeavour to accomplish during war is to weaken the military forces of the enemy.” This principle is one of the most crucial International Humanitarian Law principles and it was recognised by the International Court of

¹⁵⁰‘Cyber Warfare and *Levées En Masse* in International Humanitarian Law: New Wine into Old Wineskins’ <<https://www.jurist.org/features/2022/07/22/cyber-warfare-and-levees-en-masse-in-international-humanitarian-law-new-wine-into-old-wineskins/>> accessed 19 October 2022.

¹⁵¹Emily Crawford, ‘Armed Ukrainian Citizens: Direct Participation in Hostilities, *Levée En Masse*, or Something Else?’ (*EJIL: Talk!*, 1 March 2022) <<https://www.ejiltalk.org/armed-ukrainian-citizens-direct-participation-in-hostilities-levee-en-masse-or-something-else/>> accessed 20 October 2022.

¹⁵²‘Cyber Warfare and *Levées En Masse* in International Humanitarian Law: New Wine into Old Wineskins’ (n 107).

¹⁵³ Rule 28, Schmitt, MN (n 64).

¹⁵⁴ Rule 29, Schmitt, MN (n 64).

¹⁵⁵‘Direct Participation in Hostilities | How Does Law Protect in War? - Online Casebook’ <<https://casebook.icrc.org/glossary/direct-participation-hostilities>> accessed 23 October 2022.

¹⁵⁶ Rule 31, Schmitt, MN (n 64).

Justice in its Advisory Opinion on *The Legality of the Threat or Use of Nuclear Weapons* ¹⁵⁷ case. According to the court, in addition to the prohibition of unnecessary suffering, this principle of international law is inviolable. Article 48 of the AP I codifies this protection by stating that a distinction between civilian objects and military purposes must be made. Only military targets may be deliberately targeted during an armed conflict.¹⁵⁸ The deliberate targeting of civilian objects constitutes a war crime under International Humanitarian Law.¹⁵⁹ Additionally, this rule obligates parties to an armed conflict to distinguish between civilians on one hand and combatants on the other. This principle applies to international and non-international armed conflict.

Articles 51 and 52 of Additional Protocol I stipulate protections for the civilian population and civilian objects. Some operations against the civilian population are not proscribed. These include psychological operations such as making propaganda. Contextualizing this to cyber warfare, conveying emails to the civilian enemy population encouraging surrender would not be a contravention of the laws of armed conflict. However, when an operation against a civilian population or civilian objects escalates to the level of an attack it is proscribed under International Humanitarian Law.¹⁶⁰

2.4.4 Additional Issues Arising from the Application of International Law

2.4.4.1 Means and Methods of Warfare

Cyber weapons are not expressly mentioned in the law of armed conflict. In the *Nuclear Weapons Case*,¹⁶¹ the International Court of Justice confirmed that the **“established principles and rules of International Humanitarian Law apply to all forms of warfare and to all kinds of weapons including those of the future.”**

¹⁵⁷ ‘Legality of the Threat or Use of Nuclear Weapons’ <<https://www.icj-cij.org/case/95>> accessed 18 March 2023.

¹⁵⁸Khawaja (n 123).

¹⁵⁹Khawaja (n 123).

¹⁶⁰Schmitt, MN (n 64).

¹⁶¹‘Legality of the Threat or Use of Nuclear Weapons’ <<https://www.icj-cij.org/case/95>> accessed 18 March 2023 para 86.

'Methods of warfare' refers to the cyber tactics, techniques, and procedures by which hostilities are conducted, while 'Means of cyber warfare' refers to cyber weapons and the systems that go along with them.¹⁶² The Manual forbids the use of cyber warfare means or methods that have the potential to inflict needless harm or suffering. This Rule only applies to suffering or harm to fighters, members of organized armed groups, and civilians directly taking part in conflicts.¹⁶³ A cyber means or method of warfare violates this Rule regardless of whether it was intended to cause such pain or harm or not. Means and methods of warfare can breach this Rule if they are intended to increase injuries or suffering unnecessarily.

It is unlawful to use indiscriminate cyber warfare means or methods. Any means or method of warfare that cannot be aimed at a specific target or whose effects cannot be circumscribed as required by international law and thus spread irrepressibly into civilian and other protected computers and computer networks is illegal. The use of cyber booby traps related with certain objects specified in the law of armed conflict is prohibited.¹⁶⁴ To succeed as a cyber booby-trap, a cyber-weapon must look safe to a reasonable observer or the observer must be performing a seemingly safe act. The cyber weapon must in one way or another be associated with certain specified objects such as those that are associated with medical functions, education and religious functions among others.

The starvation of civilians as a method of warfare is forbidden.¹⁶⁵ The Tallinn Manual defines starvation as the deliberate deprivation of nourishment (including water) from a civilian population with the aim of weakening or killing it. To violate this rule, starvation should be a strategy intentionally used by one of the parties to the conflict against the civilian population. In exceptional instances, cyber operations break this Rule. A breach could occur, however, during an armed conflict in which one party intends to starve the enemy civilian population. This can occur when a party to an armed conflict launches cyber operations against civilians as part of its starvation campaign, with the primary goal of disrupting food transportation to civilians, or when it attacks food manufacturing and storage units. Where not proscribed by international law, belligerent reprisals are subject to strict conditions.¹⁶⁶ This Rule is based on the Geneva Treaties' restrictions against belligerent reprisals. Belligerent reprisals are defined

¹⁶² Rule 41, Schmitt, MN (n 64).

¹⁶³ 'Legality of the Threat or Use of Nuclear Weapons' (n 160).

¹⁶⁴ Rule 44, Schmitt, MN (n 64).

¹⁶⁵ Rule 45, Schmitt, MN (n 64).

¹⁶⁶ Rule 46, Schmitt, MN (n 64).

as *prima facie* criminal acts committed against a party to an armed conflict who is breaking the law in order to coerce that party to stop.¹⁶⁷

Cyber operations may be employed to carry out belligerent reprisals in reaction to kinetic violations of International Humanitarian Law. Kinetic operations may also be used to respond to cyber violations of the law of armed conflict. It is forbidden for states to use cyberattacks as retaliation against the civilian population, specific citizens, civilian items, cultural artefacts, places of worship, objects essential for the survival of the civilian population, the environment, dams, dykes, and nuclear power plants. They must make sure that any cyber weapons they acquire or employ adhere to the laws of armed conflict that apply to that state.¹⁶⁸

2.4.4.2 Perfidy, Improper Use and Espionage

The Manual prohibits the killing or injuring of an adversary in the conduct of hostilities by resorting to perfidy. To violate this Rule, the perfidious act must be proximate to the cause of death or injury.¹⁶⁹ Take for instance a deceptive email inviting an adversary to a meeting with a United Nations official that is actually intended to lead the enemy into an ambush. The enemy is misled, and while traveling to the meeting location, the car strikes a landmine (which the adversary did not expect), resulting in death. These deaths are not proximately caused by the email since they were not predictable thus, this rule was not breached.

The Rule, however, does not cover perfidious acts that end in damage or destruction of property. Cyber-attacks that qualify as ruses of war are allowed.¹⁷⁰ These are acts designed to deceive the enemy or to persuade enemy forces to act carelessly but do not breach the law of armed conflict. In the cyber context, these may include the creation of dummy computer systems mimicking non-existent forces, use of enemy codes, signals and passwords or even use of false computer identifiers or computer transmissions.

¹⁶⁷Shane Darcy, 'What Future for the Doctrine of Belligerent Reprisals?' (2002) 5 Yearbook of International Humanitarian Law 107 <<https://www.cambridge.org/core/journals/yearbook-of-international-humanitarian-law/article/abs/what-future-for-the-doctrine-of-belligerent-reprisals/1D101514B4C86F85BF9A617DAF147BFA7>> accessed 29 June 2023.

¹⁶⁸ Rule 47, Schmitt, MN (n 64).

¹⁶⁹Schmitt, MN (n 64).

¹⁷⁰ Rule 61, Schmitt, MN (n 64).

Inappropriate use of the protective emblems, signs or signals such as the Red Cross and the Red Crescent is prohibited. Also included in this Rule are the sign for civil defence, the distinctive emblem for cultural property and the flag of truce.¹⁷¹ Improper use of the emblem of the United Nations is also forbidden in cyber operations, except as authorised by the United Nations.¹⁷² Where the United Nations becomes a party to an armed conflict or intervenes militarily, the emblem loses its protective function.

It is illegal to utilize enemy flags, military emblems, insignia, or uniforms while they are visible to the enemy during a cyber-attack.¹⁷³ Using enemy flags, military emblems, insignia, or uniforms while they are visible to the enemy during a cyber-attack is illegal. However, since the cyber operators would not be in visual contact with the adversary during a remote access cyber-attack, it is not likely that inappropriate usage of enemy uniforms would occur. The improper use of enemy uniforms is banned during a close-access cyber-attack. It is also illegal to utilize flags, military symbols, insignia, or uniforms of neutral or other non-conflict governments during cyber operations.¹⁷⁴

Furthermore, cyber espionage and other forms of information collection directed at an adversary during an armed conflict do not violate international humanitarian law.¹⁷⁵ Cyber espionage is any act undertaken covertly or under false pretences that uses cyber capabilities to attempt to collect or gather information to communicate it with the opposing party. Cyber information collection is done under false pretext when it is carried out in a manner that creates the impression that the concerned individual is entitled to the information in question.

2.4.4.3 Blockade and Zones

According to the Manual, if, alone or in conjunction with other techniques, cyber methods and means of warfare do not result in acts that violate the law of armed conflict, they may be employed to maintain and enforce a naval or aerial blockade.¹⁷⁶ When the harm to the civilian population is or is expected to be too much as compared to the real and direct military

¹⁷¹ Rule 62, Schmitt, MN (n 64).

¹⁷² Rule 63, Schmitt, MN (n 64).

¹⁷³ Rule 64, Schmitt, MN (n 64).

¹⁷⁴ Rule 65, Schmitt, MN (n 64).

¹⁷⁵ Rule 66, Schmitt, MN (n 64).

¹⁷⁶ Rule 67, Schmitt, MN (n 64).

advantage, the blockade is unlawful. Further, the use of cyber means to enforce a naval or aerial blockade must not result in blocking or otherwise seriously affecting access to neutral territory.

2.4.4.4 Occupation

The idea of occupation does not exist in cyberspace. Cyber activities may be insufficient to create or sustain the level of authority over territory required to constitute an occupation. They, on the other hand, can be used to help build or sustain the necessary authority. Similarly, cyber operations can be employed to disrupt or damage computer systems utilized by an Occupying Power to maintain control.

Protected persons in occupied territory protected from harmful cyber operations.¹⁷⁷ Occupying powers are required to treat all protected individuals with the same respect, without discrimination based on religion, race, or political ideology. The Occupying Power may limit freedoms of expression and the press in cyberspace as necessary for its security. It may also abolish or suspend existing laws that impede its cyber operations in cases where they pose a security risk.

2.4.4.5 Neutrality

The law of neutrality governs the interaction between governments that are not parties to an international armed conflict and those that are. Parties to a dispute are not permitted to engage in hostilities on neutral territory.¹⁷⁸ Due to the sovereignty of the state of nationality, neutral cyber infrastructure that is physically located in international airspace, outer space, or the high seas is protected. Similarly, exercising belligerent rights in neutral territory by cyber operations is prohibited.¹⁷⁹ As a result, armed forces from a conflicting party are barred from conducting cyber operations from neutral territory.¹⁸⁰

¹⁷⁷ Rule 87, Schmitt, MN (n 64).

¹⁷⁸ Rule 91, Schmitt, MN (n 64).

¹⁷⁹ Schmitt, MN (n 64).

¹⁸⁰ Schmitt, MN (n 64).

Additionally, digital technologies have been used for misinformation and disinformation campaigns. The neutrality of these digital technologies has been questioned due to these campaigns during armed conflicts and other situations of violence.¹⁸¹ A neutral state should not knowingly allow parties to a conflict to exercise belligerent rights from cyber infrastructure located on its territory or under its absolute control, with the exception of public, internationally and openly accessible networks such as the Internet, which may be used for military communications.

If a neutral state fails to put an end to the exercise of belligerent rights on its territory, the affected party to the conflict may take whatever actions are required to oppose such behaviour. Cyber activities may be included in these measures.¹⁸² This rule aims to make good the damage suffered by a party because of its opponent's violation of the right of neutrality.

2.5 Critique of the Tallinn Manual on the International Law Applicable to Cyberwarfare

2.5.1 Value of the Tallinn Manual

The Tallinn Manual on International Law Applicable to Cyberwarfare has received considerable reactions from various quarters. Reactions by states are seen to be varied with some adopting a “wait and see approach”, maintaining a stance of silence and opacity.¹⁸³ Some states have publicly articulated national security principles that apply to cyberspace including certain customary international law principles that have been incorporated in the Tallinn Manual.¹⁸⁴

While it is not binding law, it was the first real effort to deliberate on the application of international law to cyberspace.¹⁸⁵ It advanced the debate and conversation on the governance of what was previously thought to be a lawless void. Indeed, it led to the drafting of the Tallinn

¹⁸¹Saman Rejali and Yannick Heiniger, ‘The Role of Digital Technologies in Humanitarian Law, Policy and Action: Charting a Path Forward’ (2020) 102 *International Review of the Red Cross* 1 <https://www.cambridge.org/core/product/identifier/S1816383121000114/type/journal_article> accessed 23 June 2023.

¹⁸² Rule 94, Schmitt, MN (n 64).

¹⁸³Dan Efrony and Yuval Shany, ‘A Rule Book on the Shelf? Tallinn Manual 2.0 on Cyberoperations and Subsequent State Practice’ (2018) 112 *The American Journal of International Law* 583 <<https://www.jstor.org/stable/26568993>> accessed 21 January 2022.

¹⁸⁴Efrony and Shany (n 204).

¹⁸⁵Mark Pomerleau, ‘The Need for International Law in Cyberspace’ (*C4ISRNet*, 9 February 2017) <<https://www.c4isrnet.com/2017/02/09/the-need-for-international-law-in-cyberspace/>> accessed 13 July 2023.

Manual 2.0¹⁸⁶ and paved the way for a new Tallinn 3.0 edition which is currently being worked on.¹⁸⁷ While the rules elucidated in the Manual are yet to be accepted by states they give indicative guidelines on the trajectory the norms formulation process can take.¹⁸⁸ According to Dieter Fleck, the International Group of Experts excelled in demonstrating the ability to apply *lex lata* rules to new means and methods of warfare that were not even envisaged when the rules were developed.¹⁸⁹

By applying existing legal norms to cyberspace, the Tallinn Manual demonstrates that international law is not mum on new technological developments. Contrarily, *jus ad bellum* protects the sovereignty of states against cyber-attacks, *jus in bello* applies in armed conflict to the effect that means, and methods of cyber warfare are not limitless.¹⁹⁰ Therefore, any assertion that cyber operations are subject to international legal control only based on a new treaty has been proven by the International Group of Experts to be unfounded.¹⁹¹

Despite the commendable effort of the Tallinn Experts to demonstrate the applicability of international law to cyber armed conflict, the Manual has come under sharp criticism for numerous reasons.

2.5.2 Weaknesses of the Manual

2.5.2.1 The Proposed Application of Extant International Law To Cyberspace

As pointed out earlier, the Experts at Tallinn affirmed that International Law, in particular International Humanitarian Law applies to the conduct of parties engaged in armed hostilities. It is clear that the lack of treaty provisions regulating cyber-attacks and cyber weapons does not automatically mean that international law does not apply to the cyber realm. It is accepted that the law of armed conflict applies to cyber operations conducted during kinetic hostilities.

¹⁸⁶Michael N Schmitt, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (Cambridge University Press 2017).

¹⁸⁷'CCDCOE' <<https://ccdcoe.org/news/2021/the-ccdcoe-invites-experts-to-contribute-to-the-tallinn-manual-3-0/>> accessed 22 August 2023.

¹⁸⁸Arindrajit Basu and others, 'The Potential for the Normative Regulation of Cyberspace: Implications for India'.

¹⁸⁹D Fleck, 'Searching for International Rules Applicable to Cyber Warfare--A Critical First Assessment of the New Tallinn Manual' (2013) 18 *Journal of Conflict and Security Law* 331 <<https://academic.oup.com/jcsl/article-lookup/doi/10.1093/jcsl/krt011>> accessed 25 July 2023.

¹⁹⁰Fleck (n 209).

¹⁹¹Fleck (n 209).

The nature of the necessary connection between the cyber operation and the armed conflict was a cause of disagreement between the Experts.¹⁹² One faction of the group of experts was of the view that a connection can only be established if a cyber operation is conducted by a party to an armed conflict or on its behalf while the second faction was of the opinion that the cyber operation must have been used to contribute to the instigator's military effort.¹⁹³

Further, a condition that must be met for the laws of armed conflict to apply is the presence of an armed conflict. There was however a debate about the threshold of the prerequisite violence. The International Committee of the Red Cross in its 1949 Commentary on the Geneva Conventions, it does not matter how long the conflict between the two states lasts or the degree of slaughter that takes place. An opposing view was that a greater degree, duration or intensity of violence is required for the law of armed conflict to come into play. Analogously, one cyber incident that causes only minimal damage, injury or destruction would not necessarily initiate international armed conflict according to the latter view. Such fundamental disagreements may limit the development of legal regulation of cyber activity.¹⁹⁴

The covert nature of cyber operations poses a challenge to their regulation since it can be difficult for a State to ascertain that a cyber operation is taking place, much less in a heightened situation such as combat. Additionally, it may be difficult to identify an instigator of the attack due to the interconnected nature of cyberspace. The effects of the operation may also be difficult to identify with precision. The divergence of views on the existence of an armed conflict and the scope of application of the laws of armed conflict demonstrates how complex the regulation of fluid and hard to define conflicts may be.¹⁹⁵

2.5.2.2 Characterization of armed Conflict in the realm of cyberspace

The law of armed conflict applies to non-international armed conflict. One of the fundamental criterion that must be met for an armed conflict to be categorized as non-international is that the non-governmental groups engaged in the conflict must be regarded as a 'party to the conflict'. This means that the group is in control of organized armed forces. A degree of organization in the armed group must therefore be present. Such organization may be illustrated

¹⁹² Michael Sang, 'Legal Regulation Of Cyber Warfare: Reviewing The Contribution Of The Tallinn Manual To The Advancement Of International Law' (2015).

¹⁹³ Rule 20, Schmitt, MN (n 64).

¹⁹⁴ Sang (n 275).

¹⁹⁵ Sang (n 275).

by the presence of a command structure of disciplinary rules. The lack of such organization negates the existence of an armed conflict.

In this case, it may prove difficult to meet this requirement in the case of virtual armed groups. Cyber-attacks can be conducted from different locations. Hackers and other persons who conduct cyber operations may do so autonomously and on an individual basis. Further, the mere fact that several hackers conduct a cyber-operation against the same target does not necessarily mean that the hackers are operating in an orchestrated manner. It may prove difficult to apply the law of armed conflict to persons with whom there has been no physical contact.

2.5.2.3 Definitional Challenges

The Tallinn Manual gives direction on the legal regulation of cyber operations that amount to an ‘attack’ as per Article 48 of Additional Protocol I. The Manual focuses on cyber operations that take place within the context of armed conflict. It does not deal with the application of international law to cyberspace during peacetime or general interactions between states.¹⁹⁶ Additionally, the Manual gives minimal guidance on the application of international law in situations where cyber operations do not meet the threshold of an attack. The assertion in Rule 30 of the Manual that *de minimis* damage or destruction further muddles the debate on the application of the laws of armed conflict to cyber operations.

From the definition and the discussions of the Experts on the concept and definition of attack, it is evident that the qualifying factor, according to the Group of Experts at Tallinn, as to whether an action is an attack or not is the outcome of its consequences with a particular focus on death or injury of individuals or destruction of property.

However, there is disagreement about whether a cyber-operation that causes a loss of function without inflicting physical harm may be termed an attack. According to the International Committee of the Red Cross (ICRC), an action designed to disable a computer network during an armed conflict is considered an attack under International Humanitarian Law, regardless of whether the object is disabled using kinetic or cyber methods.¹⁹⁷ A narrow interpretation of ‘attack’ as only denoting an operation that results in death or physical destruction would

¹⁹⁶ Pomerleau (n 268).

¹⁹⁷ ‘Icrc_ihl-and-Cyber-Operations-during-Armed-Conflicts (1).Pdf’.

exclude cyber operations geared at making a civilian network dysfunctional or that are anticipated to cause such effects and may not be dealt with by key International Humanitarian Law rules protecting civilians and civilian objects.¹⁹⁸

2.5.2.4 The Status of Certain Objects

The Experts at Tallinn argued that due to the intangible nature of data, it is ineligible to be an object for the purposes of the rules of targeting under the laws of armed conflict. Some scholars however opine that data can be defined as an object since it is susceptible to being attacked and destroyed. Consequently, when states or non-state actors hack into essential civilian data such as medical records during armed conflict, such an attack could be considered a violation of the principle of distinction.¹⁹⁹ Some scholars have taken the view that data is an ‘object’ within the meaning assigned to the term under International Humanitarian Law.

According to Kubo Mačák,²⁰⁰ data qualifies as an object due to its vulnerability to alteration and destruction it therefore may qualify as a military objective. Accordingly, data that does not fulfil the standards for qualification as a military objective must be considered as a civilian object.²⁰¹ This lack of common understanding on critical issues such as the status of data further complicates the governance of cyber-armed conflict. The discussion on data as an object is still ongoing. The Tallinn Group of Experts was tasked with the mandate of clarifying the application of international law to cyber warfare. The group however did not consider the nuances of data as an object of attack.

Such a restricted interpretation of the term ‘attack’ would conflict with the purpose of the rules of International Humanitarian Law on the conduct of hostilities.²⁰² An opposite view is that in cyber operations the rights of others may be violated without causing any physical damage and this would not necessarily be termed an ‘attack’ in the true sense of the word.²⁰³ Those in favour

¹⁹⁸‘Icrc_ihl-and-Cyber-Operations-during-Armed-Conflicts (1).Pdf’ (n 121).

¹⁹⁹Khawaja (n 218).

²⁰⁰Kubo Mačák, ‘Military Objectives 2.0: The Case for Interpreting Computer Data as Objects under International Humanitarian Law’ (2015) 48 *Israel Law Review* 55 <<https://www.cambridge.org/core/journals/israel-law-review/article/abs/military-objectives-20-the-case-for-interpreting-computer-data-as-objects-under-international-humanitarian-law/9DD4F5EBF48CF8C665F7B5E27049E3F7>> accessed 14 March 2023.

²⁰¹Mačák (n 152).

²⁰²‘ICRC_IHL-and-Cyber-Operations-during-Armed-Conflicts (1).Pdf’ (n 121).

²⁰³Khawaja (n 123).

of this proposition argue that there must be an extinguished or diminished functionality due to such an operation for the operation to constitute an attack.²⁰⁴

Operations against data which result in the death or destruction of physical objects, those objects or individuals are ‘objects’ of attack and the operation in question constitutes an ‘attack’. According to the International Committee of the Red Cross, using cyber operations, belligerents can modify, encrypt or destroy data, or control processes by a controlled computer system. Several targets in the ‘physical world’ including infrastructure, industries or transport can be altered, destroyed or disrupted as a result of this control.²⁰⁵

Further, the Committee, in its 2019 position paper on International Humanitarian Law and Cyber Operations during Armed Conflicts²⁰⁶ proposed that the main principles of International Humanitarian Law (distinction, proportionality, prohibition, military necessity, humanity and precautions) protect civilians and civilian objects. Based on this, the Committee called on states to come to a consensus that civilian data is protected by these rules. Some experts are however of the view that the definition of an ‘object’ is limited to physical properties only, that is, something that is visible and tangible. In view of this, they propose that the rules of International Humanitarian Law would not apply to cyber operations unless they involve some degree of physical effect and/or loss of functionality.

2.5.2.5 Participation in Hostilities

The law of armed conflict recognizes two classes of persons who can participate in armed hostilities. These are combatants and participants in a *levee en masse*. One of the requirements for proof of combatant status is organization. Due to the unique nature of virtual organizations, proving organization as a criterion for combatant status is difficult. Furthermore, proving that a virtual group was acting on the orders of a responsible commander may be difficult.

Additionally demonstrating that a virtual group is subject to internal disciplinary procedures capable of ensuring adherence to the law of armed conflict may be more difficult in the cyber realm.²⁰⁷ It is also possible that those involved in cyber-attacks do not know each other at all.

²⁰⁴Khawaja (n 123).

²⁰⁵‘ICRC_IHL-and-Cyber-Operations-during-Armed-Conflicts (1).Pdf’ (n 121).

²⁰⁶‘ICRC_IHL-and-Cyber-Operations-during-Armed-Conflicts (1).Pdf’ (n 121).

²⁰⁷‘The Application of the Principle of Distinction in the Cyber Context: A Chinese Perspective’ (n 100).

The environment of cyberspace does not allow combatants to carry their weapons openly.²⁰⁸ Cumulatively, these challenges make it extremely difficult for an organization that is purely virtual to meet the requirements for an armed group for determination of combatant status.

Moreover, adapting the requirement of wearing a fixed distinctive sign by combatants from the kinetic realm of armed conflict to the cyber realm may prove to be a puzzling endeavour.²⁰⁹ While the rules of armed conflict were prepared at a time when a certain level of physical closeness between the combatants was expected, the same does not hold in cyber armed conflict at whose core lies anonymity and an attack can be conducted in the absence of physical proximity between the parties.²¹⁰

Applying the *levee en masse* criteria to cyber-attacks is problematic. Regarding the inhabitation criterion, for instance, those who were abroad before the invasion started or who can escape the nation once it has begun are more likely to be able to initiate strikes from abroad.²¹¹ This is worrying because, despite being in a different country, these people could still be targets. As a result, the invading State might be inclined to go against Article 2(4) of the Charter of the United Nations, which forbids using force against other States, to exact revenge on these people.²¹² The law of armed conflict places particular importance on the essential requirement for those participating in a *levee en masse* to carry their arms openly. In a cyber *levee en masse*, the weapon used is a computer. Whereas it may be feasible for a computer to be considered a weapon, possession only cannot be construed to be suggestive of combatant activity. It is also extremely difficult to distinguish participants in a cyber *levee en masse*. It, therefore, follows that conformity with the principle of distinction becomes difficult.

2.5.2.6 Geographical Prejudice

Most of the twenty-three experts involved in drafting the Manual were Anglo-American and present or past members of the International Committee of the Red Cross. There was a notable absence of African, Chinese, Latin American, Middle Eastern, Asian and Russian participation

²⁰⁸‘The Application of the Principle of Distinction in the Cyber Context: A Chinese Perspective’ (n 100).

²⁰⁹‘The Application of the Principle of Distinction in the Cyber Context: A Chinese Perspective’ (n 100).

²¹⁰‘The Application of the Principle of Distinction in the Cyber Context: A Chinese Perspective’ (n 100).

²¹¹‘Cyber Warfare and *Levéés En Masse* in International Humanitarian Law: New Wine into Old Wineskins’ (n 107).

²¹²‘Cyber Warfare and *Levéés En Masse* in International Humanitarian Law: New Wine into Old Wineskins’ (n 107).

in the process of drafting the Manual. This limitation in the diversity of the experts as well as the over-reliance on Western Legal sources drew strong criticism of the Manual.²¹³ The legitimacy of the Tallinn question has been questioned by states that are considered superior militarily such as China, Russia and North Korea.²¹⁴

2.5.2.7 Attribution and the Evidentiary Challenges

The application of existing norms to cyber-armed conflict may prove to be problematic. One of the biggest challenges in this respect is the attribution of cyberattacks. Cyber attackers are capable of blurring their identities using various cyber techniques. “Stepping stones” is one of the methods used by cyber attackers to hide their identity.²¹⁵ This method involves routing a cyber-attack through third-party computers, which usually belong to another state. This, therefore, poses the risk of drawing third-party states who unknowingly host an attack into a conflict.²¹⁶

Further, while kinetic attacks tend to leave physical evidence of the attack such as the weapons used, the identity of the attackers and the geographical location of the attack, the same does not apply to cyberspace.²¹⁷ This compounds the attribution challenge.²¹⁸ Moreover, the rapidity of cyber-attacks leaves little or no time for an attacked state to determine the source of the attack. Even though a cyber-attack is conducted in a short time, the duration required for discovering an attack may be significantly longer, usually taking weeks or months.²¹⁹

2.5.2.8 Inability to predict Implementation

According to Terence Check, the Manual, in the commentaries accompanying each rule refers to ‘some’, ‘many’ or ‘all’ when referring to the Experts. A record of the vote or the identities

²¹³Pauline Charlotte Janssens and Jan Wouters, ‘Informal International Law-Making: A Way around the Deadlock of International Humanitarian Law?’ (2022) 104 *International Review of the Red Cross* 2111 <https://www.cambridge.org/core/product/identifier/S1816383122000467/type/journal_article> accessed 9 July 2023.

²¹⁴ Sang (n 275).

²¹⁵Ido Kilovaty, ‘Cyber Warfare and the Jus Ad Bellum Challenges’: 5.

²¹⁶Basu and others (n 214).

²¹⁷Kilovaty (n 214).

²¹⁸Kilovaty (n 214).

²¹⁹Yuan Fang, ‘Is The Current International Law A Good Fit For Cybersecurity? A U.N. Charter-Based Analysis’.

of the dissenting experts would have substantially boosted the Manual's utility.²²⁰ In his opinion, if the Manual had specified which experts reached which conclusions, it would have permitted analysis to determine which governments and organizations backed the experts' views, improving the predictability of the Manual's implementation. He further opines that this information would have helped in tracking how extensively governments and other entities are adopting the Manual.²²¹

2.6 Conclusion

Although there is no internationally binding treaty on cyber-armed conflict, the Tallinn Manual on the International Law applicable to Cyberwarfare, clarifies the murky issues, related to the application of current international law to cyberspace. While the Manual is not comprehensive or binding, it demonstrates that states are obligated to comply with applicable international law even where conflict takes place in relatively new domains such as cyberspace. It was a critical first move in the process of developing the international legal framework on governance of cyber operations. This chapter identified and examined the aspects of existing international law, in particular, the law of armed conflict and exposed the challenges that arise in the attempt to apply extant international law to cyberspace. The next Chapter delves into the various positions taken by states on the application of international law to armed conflict in cyberspace and identifies the challenges and opportunities posed by the application of existing international rules to cyber-armed conflict.

²²⁰Terence Andrew Check, 'Book Review: Analyzing the Effectiveness of the Tallinn Manual's Jus Ad Bellum Doctrine on Cyber Conflict, a NATO-Centric Approach' [2013] SSRN Electronic Journal <<http://www.ssrn.com/abstract=2347736>> accessed 19 July 2023.

²²¹Check (n 222).

CHAPTER THREE

3.0 APPLICATION OF INTERNATIONAL LAW TO ARMED CONFLICT IN CYBERSPACE: CHALLENGES AND OPPORTUNITIES

3.1 Introduction

This chapter seeks to examine the positions taken by states with regard to the application of international law to cyberspace and to armed conflict in cyberspace. It will also illuminate the challenges and opportunities emerging from the application of international law to cyber-armed conflict. Further, this Chapter will examine various arguments made with regard to the establishment of a universal treaty governing cyberspace and cyber-armed conflict.

3.2 Positions of States on the Application of International Law to Cyber Armed Conflict

States have achieved consensus that International Law applies to cyberspace. The United Nations Group of Experts stated in its 2013 report that the Group's conclusion was that international law is applicable and is key to maintaining peace and stability and stimulating an open, secure and peaceful ICT environment.²²² However, despite this and subsequent agreements in the application of international law to cyberspace, progress in resolving the question of *how* international law applies has proven difficult to achieve.²²³ Away from international fora and negotiations, states have elected to remain non-committal on how international law applies to cyberspace. In many cases, States do not refer to international law when they are attributing cyber operations.²²⁴ According to Efrony and Shany, states have a tendency to maintaining a policy of silence and ambiguity when it comes to international law governing cyber operations.²²⁵

There has however been increased activity on issues of cyber norms and the applicability of international law in the recent past.²²⁶ Several states have released statements on how they perceive the applicability of international law to cyberspace. The official compendium of state

²²²Dennis Broeders and others, 'Revisiting Past Cyber Operations in Light of New Cyber Norms and Interpretations of International Law: Inching towards Lines in the Sand?' (2022) 7 Journal of Cyber Policy 97 <<https://doi.org/10.1080/23738871.2022.2041061>> accessed 24 August 2023.

²²³Broeders and others (n 224).

²²⁴Efrony and Shany (n 204).

²²⁵Efrony and Shany (n 204).

²²⁶Broeders and others (n 224).

visions on international law²²⁷ in cyberspace adds some more detail to the positions adopted by states on the application of international law to cyberspace. Strikingly, major world powers such as China have not given their vision yet. These statements however differ substantially from each other in form, legal depth and precision.²²⁸

Germany released its position paper on the applicability of international law in cyberspace in which it expressed its conviction that International law, the Charter of the United Nations and International Humanitarian Law apply in the context of cyberspace. Germany reiterated that International Humanitarian Law applies to cyber activities in the context of armed conflict. It further stated that the mere fact that cyberspace had not emerged, as a domain for warfare at the time when core treaties of IHL were drafted does not exempt the conduct of hostilities in cyberspace from the application of IHL.²²⁹ With regard to other military operations, Germany took the view that IHL applies to cyber operations in the context of armed conflict independent of its qualification as lawful or unlawful armed conflict according to *jus ad bellum*.²³⁰

New Zealand affirmed that International Law applies online as it does offline. She identified applicable international law such as the Charter of the United Nations, the law on state responsibility and international humanitarian law and human rights law as applicable to cyberspace.²³¹ The Republic of Poland reaffirmed that the requirements of international humanitarian law also apply to actions conducted in cyberspace during hostilities.²³² Australia took the view that general principles of international law are applicable to cyber activities taking place outside of armed conflict.²³³

²²⁷ ‘UN_ -Official-Compendium-of-National-Contributions-on-How-International-Law-Applies-to-Use-of-ICT-by-States_A-76-136-EN.Pdf’.

²²⁸ Broeders and others (n 224).

²²⁹ ‘On-the-Application-of-International-Law-in-Cyberspace-Data.Pdf’.

²³⁰ ‘On-the-Application-of-International-Law-in-Cyberspace-Data.Pdf’ <<https://www.auswaertiges-amt.de/blob/2446304/32e7b2498e10b74fb17204c54665bdf0/on-the-application-of-international-law-in-cyberspace-data.pdf>> accessed 18 October 2023.

²³¹ New Zealand Ministry of Foreign Affairs and Trade, ‘The Application of International Law to State Activity in Cyberspace’ (*New Zealand Ministry of Foreign Affairs and Trade*, 1 December 2020) <<https://www.mfat.govt.nz/en/media-and-resources/the-application-of-international-law-to-state-activity-in-cyberspace/>> accessed 8 July 2023.

²³² ‘The Republic of Poland’s Position on the Application of International Law in Cyberspace - Ministry of Foreign Affairs Republic of Poland - Gov.Pl Website’ (*Ministry of Foreign Affairs Republic of Poland*, 2022) <<https://www.gov.pl/web/diplomacy/the-republic-of-polands-position-on-the-application-of-international-law-in-cyberspace>>.

²³³ ‘Australia’s Position on The Application of International Law to State Conduct in Cyberspace.Pdf’.

Germany emphasized that the principles governing the conduct of armed hostilities including distinction apply to cyber-attacks in international and non-international armed conflict.²³⁴ Further Germany took the view that the yardstick for the application of the principle of distinction is the “effect caused by a cyber-attack”, irrespective of whether it was used defensively or offensively. New Zealand also noted that all cyber-attacks must comply with the cardinal principles of international humanitarian law such as the principle of distinction.²³⁵ This assertion was supported by the Republic of Poland.²³⁶

New Zealand noted that civilians operating in cyberspace can be considered as taking direct part in the armed conflict with the outcome of losing their protection from attacks and the effects of hostilities. Germany identified some conditions that need to be met for this to happen. These are: their acts are likely to negatively affect the military operations of a party, there is a direct causal link between their acts and the adverse effects and the acts are specifically aimed at inflicting harm in support of a party to the conflict and to the detriment of the other. Additionally, Germany posited that a cyber-attack in the context of IHL is “an action initiated through cyberspace to cause harmful outcomes on communication, information or other electronic systems on the information that is stored, processed or transmitted on these systems or on physical objects or persons.” She was of the view that the occurrence of physical damage, injury, death or destruction comparable to effects of conventional weapons is not a requirement for an action to constitute an attack under Article 49 (1) of Additional Protocol I.²³⁷

New Zealand noted that cyber activity that constitutes use of force would also constitute an armed attack for purposes of Article 51 of the charter of the United Nations if its results in outcomes of a magnitude similar to those occasioned by a kinetic armed attack.²³⁸ Australia²³⁹ and The Republic of Poland adopted a similar position on the concept of ‘armed attack’.²⁴⁰ This scale and effect proposition was also adopted by Denmark in its definition of a cyber-attack. Denmark contended that a state might in certain circumstances be permitted to exercise

²³⁴ ‘Germany Releases Position Paper on Applicability of International Law in Cyberspace | Digital Watch Observatory’ (5 March 2021) <<https://dig.watch/updates/germany-releases-position-paper-applicability-international-law-cyberspace>> accessed 8 July 2023.

²³⁵ Trade (n 327).

²³⁶ ‘The Republic of Poland’s Position on the Application of International Law in Cyberspace - Ministry of Foreign Affairs Republic of Poland - Gov.Pl Website’ (n 328).

²³⁷ ‘Protocol Additional To The Geneva Conventions of 12 August 1949, And Relating to The Protection Of Victims of International Armed Conflicts (Protocol I), of 8 June 1977’ (n 44).

²³⁸ Trade (n 327).

²³⁹ ‘Australia’s Position on The Application of International Law to State Conduct in Cyberspace.Pdf’ (n 329).

²⁴⁰ ‘The Republic of Poland’s Position on the Application of International Law in Cyberspace - Ministry of Foreign Affairs Republic of Poland - Gov.Pl Website’ (n 328).

self-defence against a non-state actor contrary to assertions by other states that an armed attack can only be undertaken by state actors or actors acting under the direction of States.²⁴¹

3.3 Challenges in the Application of Existing International Law to Cyber- Armed Conflict

3.3.1 Attribution

One of the most confounding issues around the application of international law to cyber-armed conflict is the issue of attribution, which combines technical and legal aspects that are not always easily separated. Legally, to hold a state accountable for a malicious cyber incident, the operation that caused it must be attributed to it. In line with the Articles on State Responsibility, which, although not a multilateral treaty, are generally accepted as reflective of customary international law, a state is principally responsible for the conduct of its organs. Activities that are conducted by non-state actors on the other hand can only be attributed to a state if they are “in fact acting on the instructions of, or under the direction of the state.”²⁴²

To trigger the rules of the Articles on State Responsibility for Internationally Wrongful Acts²⁴³, the system in which the antagonistic cyber operation had been launched and the individual executing the operation need to be identified. The former is imperative to determine the location of origin while the latter is needed to assess the actor’s status in relation to a state.²⁴⁴

Although states have made significant progress in their technical abilities to track the origin of malicious cyber operations, taking into consideration the fundamental principles of computer code and how the global network infrastructure is set up, conducting secret activities in cyberspace while retaining some degree of anonymity is possible for reasonably sophisticated actors.²⁴⁵ Even if the computer from which a malicious attack was conducted can be detected,

²⁴¹ Jeppe Mejer Kjelgaard and Ulf Melgaard, ‘Denmark’s Position Paper on the Application of International Law in Cyberspace: Introduction’ (2023) 1 *Nordic Journal of International Law* 1 <<https://brill.com/view/journals/nord/aop/article-10.1163-15718107-20230001/article-10.1163-15718107-20230001.xml>> accessed 8 July 2023.

²⁴² Article 8 ‘Responsibility of States for Internationally Wrongful Acts (2001)’.

²⁴³ ‘Responsibility of States for Internationally Wrongful Acts (2001)’ (n 262).

²⁴⁴ Henning Lahmann, ‘State Behaviour in Cyberspace: Normative Development and Points of Contention’ (2023) 16 *Zeitschrift für Außen- und Sicherheitspolitik* 31 <<https://link.springer.com/10.1007/s12399-023-00939-7>> accessed 17 August 2023.

²⁴⁵ Lahmann (n 264).

that fact does not always who is responsible for the aggression since states may not be able to determine the individual who operates the computer or his associations.²⁴⁶

From a legal standpoint, when a state seeks to attribute a cyber-security incident to an opponent, the attribution problem mainly concerns the question of the degree of evidence necessary for a state to discharge its burden of proof in this respect.²⁴⁷ There is a need for concrete standards for producing sufficient evidence for states to accuse each other of wrongdoing. It is only when international law's attribution conditions for self-defence are fulfilled that a victim state can initiate self-defence actions against an aggressor state.²⁴⁸ Australia identified attribution as one of the problems posed by cyber space in its public statement acknowledging the application of international law to this realm.²⁴⁹

There are opposing views among states on the issue of attribution and the disclosure of evidence on attribution. For example, Russia is of the view that that states should refrain from publicly attributing cyber incidents in cyberspace to a particular state without availing the necessary technical evidence. Sweden on the other hand opines that there is no legal requirement to disclose any evidence in relation to the attribution of conduct to a state and that public attribution is a decision of states and is not a requirement under international law.²⁵⁰ Estonia is of the view that attribution is not something that is unachievable and difficult and that an attributing state is not required to be absolutely certain but to be reasonable when attributing an operation.²⁵¹ Germany has declared that there is no general obligation under international law in its current form to make public a decision on attribution and to provide for scrutiny by the public evidence on which attribution is premised.²⁵² The divergent opinions of states in their interpretation of the law leads to the fragmentation of the process of establishment of norms governing this domain.²⁵³

²⁴⁶Han Li and Junhao Zhang, 'Application of Existing Rules of International Law in Cyberspace': (2022) <<https://www.atlantis-press.com/article/125973741>> accessed 18 August 2023.

²⁴⁷Lahmann (n 264).

²⁴⁸Li and Zhang (n 266).

²⁴⁹ 'Australia's Position on The Application of International Law to State Conduct in Cyberspace.Pdf' (n 329).

²⁵⁰'Attribution' (*International cyber law: interactive toolkit*, 28 July 2023).<<https://cyberlaw.ccdcoe.org/wiki/Attribution>> accessed 25 August 2023.

²⁵¹'Attribution' (n 260).

²⁵²'On-the-Application-of-International-Law-in-Cyberspace-Data.Pdf' (n 324).

²⁵³Broeders and others (n 224).

3.3.2 Compliance with the Principle of Distinction

The dual-purpose nature of cyber infrastructure poses a real obstacle to the application of the laws of armed conflict in cyber-armed conflict. The infrastructure used to conduct legal and critical civilian business may be the same infrastructure used to carry out cyber aggression. Unfortunately, this may affect the notion of protecting civilian infrastructure because there is no purely civilian infrastructure.²⁵⁴ For example, an attack may be carried out on military cyber infrastructure using malicious code which subsequently spreads to connected civilian cyber infrastructure. This therefore makes complying with the principle of distinction very difficult.²⁵⁵

3.3.3 Insufficient State Practice

While there is agreement that international law applies to cyberspace, the argument over how it does so continues. Customary international law is created by nations through state practice and *opinio juris*, as acknowledged by the Tallinn Manual's authors. Due to the scarcity of state cyber practice and publicly available pronouncements of *opinio juris*, the experts observed, "it is sometimes difficult to definitively conclude that any cyber-specific customary international law norm exists."²⁵⁶

While some states have publicly expressed their opinions on the application of international law to cyberspace, many states are still unwilling to do so. States' silence may lead to uncertainty in the cyber sphere, as states may be left assuming each other's perspectives on the appropriate legal framework.²⁵⁷ Such ambiguity may lead to misunderstandings among states, potentially leading to conflict escalation.²⁵⁸

While states generally believe that the extant international legal framework is enough to regulate state behaviours, there are divergent views on various issues. For example, the issue of collective countermeasures has also come into sharp focus. It is doubtless that a state has the right to respond to malicious cyber activity by imposing countermeasures, that is acts which would otherwise be unlawful under international law, provided attribution of the activity to the

²⁵⁴Gary D Brown, 'International Law Applies To Cyber Warfare! Now What?' 46.

²⁵⁵Brown (n 385).

²⁵⁶ Schmitt, MN (n 63) pp 5.

²⁵⁷ Brian J Egan, 'International Law and Stability in Cyberspace' (2017) 35.

²⁵⁸ Egan (n 388).

state against which countermeasures are successful and the aggrieved state can prove that the latter bears responsibility.²⁵⁹ The question that has arisen is whether a third-party state can engage in countermeasures of its own to assist the injured state. The President of Estonia came out in favour of the engagement in countermeasures by a third-party state. This position was cautiously endorsed by New Zealand and the United Kingdom.²⁶⁰

The lack of state practice has also been acknowledged by some states. Illustratively, when issuing its position paper on the application of international law in the cyber domain, New Zealand acknowledged that the rule of territorial sovereignty applies. However, she acknowledged that further state practice is required for the precise boundaries of its application to crystallise. In its 2022 statement, Canada disagreed with the position taken by Estonia in 2019 and stated that there is not sufficient State practice or *opinio juris* to determine that international law permits collective countermeasures.²⁶¹

Despite the rising attributions of state and state-sponsored cyber activities being on the rise, accountability for these actions has proven to be challenging. States that accuse other states of malicious activity in cyberspace seldom invoke international law in so doing.²⁶² The lack of international rhetoric implies that such behaviour by states may be lawful even if it is unwanted. The outright naming and shaming of states involved in such undesirable behaviour has done little to change it.²⁶³ Additionally, the lack of binding norms regulating conduct in cyberspace leaves states with few options for responding to and preventing cyber-enabled malicious behaviour, which results in more contradictions and conflicts.²⁶⁴

3.3.4 Lack of Enforcement Mechanisms

Under international law, States may bear the responsibility for cyber operations carried out by their agents or those for which the State can be held accountable based on the law of state

²⁵⁹Lahmann (n 264).

²⁶⁰Lahmann (n 264).

²⁶¹‘International Law in Cyberspace’ (n 62).

²⁶²Duncan Hollis, ‘A Brief Primer on International Law and Cyberspace’ (*Carnegie Endowment for International Peace*) <<https://carnegieendowment.org/2021/06/14/brief-primer-on-international-law-and-cyberspace-pub-84763>> accessed 25 May 2023.

²⁶³Duncan Hollis, ‘A Brief Primer on International Law and Cyberspace’ (*Carnegie Endowment for International Peace*) <<https://carnegieendowment.org/2021/06/14/brief-primer-on-international-law-and-cyberspace-pub-84763>> accessed 21 January 2022.

²⁶⁴Li and Zhang (n 266).

responsibility.²⁶⁵ In some situations, the actions of non-state actors may be attributed to states. A challenge, however, arises concerning the judicial mechanism that would be used in cases where a state is behind a cyber-attack. There is no international body authorised to oversee non-state cyber activity and enforce the will of states to punish perpetrators. This task is left to individual states, which reinforces state-centrism to the detriment of international cooperation.²⁶⁶ If a country is elected to run the body, it may be swayed to abuse the power that comes with this responsibility to hide its activities.²⁶⁷ In addition to this, verification of violation may be difficult because victim states would be hesitant to disclose an attack to avoid embarrassment and loss of credibility. They do not gain much for disclosing a malicious attack when there is no neutral body to penalize a perpetrator.²⁶⁸

The lack of a judicial mechanism essentially means that a cyber-attack actor bears no consequences for his actions.²⁶⁹ Most of the laws of armed conflict were developed when states had monopoly over the means of warfare such as bombs, tankers and ships. However, unlike these means of warfare cyber techniques are widely available to the public.²⁷⁰

3.3.5 Due Diligence

Due diligence requires that a state has a duty not to allow its territory to be used for activities that are harmful to other states. The International Court of Justice in the *Corfu Channel* decision stated, “Every state is under an obligation not to allow knowingly its territory to be used for acts contrary to the rights of other States.”²⁷¹ The discussion on due diligence has recently re-emerged in the ongoing Russia- Ukraine conflict. Ukraine’s ‘IT army’ comprises many volunteer hackers who engage in offensive cyber activities against Russia from the territories of third countries. The question then arises, do the third countries have any positive obligations

²⁶⁵Kosmas Pipyros and others, ‘Cyber operations and International Humanitarian Law: A Review of Obstacles in Applying International Law Rules in Cyber Warfare’ (2016) 24 *Information & Computer Security* 38 <<https://doi.org/10.1108/ICS-12-2014-0081>> accessed 18 August 2023.

²⁶⁶Nori Katagiri, ‘Why International Law and Norms Do Little in Preventing Non-State Cyber Attacks’ (2021) 7 *Journal of Cybersecurity* tyab009 <<https://doi.org/10.1093/cybsec/tyab009>> accessed 24 August 2023.

²⁶⁷Nori Katagiri, ‘Why International Law and Norms Do Little in Preventing Non-State Cyber Attacks’ (2021) 7 *Journal of Cybersecurity* tyab009 <<https://doi.org/10.1093/cybsec/tyab009>> accessed 21 January 2022.

²⁶⁸Katagiri (n 276).

²⁶⁹Pipyros and others (n 275).

²⁷⁰Gary D Brown, ‘International Law Applies To Cyber Warfare! Now What?’ 46.

²⁷¹‘The Corfu Channel Case, United Kingdom of Great Britain and Northern Ireland v. the People’s Republic of Albania | InforMEA’ <<https://www.informea.org/en/court-decision/corfu-channel-case-united-kingdom-great-britain-and-northern-ireland-v-people%E2%80%99s>> accessed 30 January 2023.

to try to prevent the hackers from hacking or can the inactivity of the third states be justified in light of the adversarial context in which they occur?²⁷²

This territoriality criterion is however not fool proof. The use of ICTs allows an attacker to take advantage of the many internet service providers of the existing cloud-based services to hide his physical and territorial identity. In addition to this, an ICT device or system can become an instrument of a cyber-attack without its user or owner's knowledge.²⁷³ Consequently, while leading actors are usually nation-state actors, the activities of non-state actors, including terrorist groups, create confusion and misperception as to the real cyberwarfare 'players'. In effect, conflicts in cyberspace allow for the combination of crime, military action and espionage in ways that make it challenging to distinguish them.²⁷⁴

3.3.6 Emergence of non-state actors in cyberspace

The majority of cyberspace is operated and controlled by the private sector.²⁷⁵ Furthermore, the private sector is taking on duties that were formerly only associated with states. Cyber threat intelligence and attribution are examples of this.²⁷⁶ This presents challenges to governments in terms of ensuring the safety and security of the state's key infrastructure when the infrastructure is really managed by the private sector.

3.3.7 Inadequate human capacity in cybersecurity

Concerns about the execution of stated norms have led to the necessity for cyberspace capacity building.²⁷⁷ For example, one of the norms recommended by the UN GGE report in 2015 is that "states should not knowingly allow their territory to be used for internationally wrongful acts using ICTs." The phrasing of this standard suggests that a state could be held liable for violating this norm, also known as the due diligence obligation, if it is aware of the conditions

²⁷²Lahmann (n 375).

²⁷³Pipyros and others (n 275).

²⁷⁴Pipyros and others (n 275).

²⁷⁵ Ronald Deibert and others (eds), *Access Controlled: The Shaping of Power, Rights, and Rule in Cyberspace* (MIT Press 2010).

²⁷⁶ Eo Goldman and Ed Monarez, 'Persistent Engagement and the Private Sector' (2021) 20 *Journal of Information Warfare* 107 <<https://www.jstor.org/stable/27036533>> accessed 25 November 2023.

²⁷⁷ Zine Homburger, 'The Necessity and Pitfall of Cybersecurity Capacity Building for Norm Development in Cyberspace' (2019) 33 *Global Society* 224 <<https://doi.org/10.1080/13600826.2019.1569502>> accessed 26 November 2023.

and can take reasonable steps to eradicate them.²⁷⁸ A state must have a specific level of capacity in order to be subject to the positive obligation imposed by this standard.²⁷⁹ In the context of ICTs, such capability could include software-related abilities, skills linked to the preservation of digital evidence, and the ability to act on obtained intelligence.²⁸⁰

3.4 Opportunities for States in the Application of International Law to Cyber-Armed Conflict

The debate on the application of international law and the challenges related to the same provides an opportunity for states to continue publicly declaring their official positions on this issue. These public statements would not only demonstrate the position of states on this issue but would also provide a chance to shape the discourse in this area. Further, states have the opportunity to deepen the dialogue among themselves about how international law applies to this realm. This will enhance the understanding of the rules and how they apply resulting in more transparency and communication with each other.²⁸¹

States that have traditionally not been deeply engaged in this discourse also have an opportunity to delve into this debate and give their views on this area of the law. Aside from the Tallinn Manual on International Law Applicable to Cyberwarfare and the Tallinn Manual on International Law Applicable to Cyber Operations, there have been several initiatives, including the London Process, the NetMudial process led by Brazil, and China's World Internet Conference.

This indicates how many stakeholders are involved in the global cyber rule-making process.²⁸² So far, no single party or organization has been able to play a comprehensive and integrative role in the process, casting doubt on the future direction of international cyber policy. These

²⁷⁸ Homburger (n 416).

²⁷⁹ Homburger (n 416).

²⁸⁰ Homburger (n 416).

²⁸¹ Harriet Moynihan, 'The Vital Role of International Law in the Framework for Responsible State Behaviour in Cyberspace' (2021) 6 Journal of Cyber Policy 394 <<https://www.tandfonline.com/doi/full/10.1080/23738871.2020.1832550>> accessed 30 January 2022.

²⁸² Ma Xinmin, 'Key Issues and Future Development of International Cyberspace Law' (2016) 02 China Quarterly of International Strategic Studies 119 <<https://www.worldscientific.com/doi/abs/10.1142/S2377740016500068>> accessed 21 October 2023.

disparate attempts present a good opportunity for states or international organizations such as the United Nations to step in and lead the way in unifying the rule-making process.²⁸³

The emergence of cyberspace as a new frontier for armed conflict means that states require a vibrant cybersecurity sector. The opportunity to build legal and technical capacity in this area is apparent. This will ensure that states are adequately equipped to deal with the dynamic and novel challenges posed by this new domain.

The development of cyber-armed conflict also presents an opportunity for states to collaborate with and harness the technical and academic expertise of non-state actors as reflected in the Tallinn Manuals. While international law is largely a preserve of states, the importance of non-state actors in the ICT sector and cyberspace cannot be ignored. Engagement with these actors will undoubtedly offer states an opportunity to tap into the wealth of expertise available to enable them to address the emergent issues concerning cyberspace. In the long term, this will lead to a steady development of international law in this area.

Additionally, there is an opportunity for the Tallinn Manual on the International Law Applicable to Cyberwarfare to contribute and possibly be adopted under the auspices of non-governmental fora and to be incorporated into the military manuals of States. While international law is made by states, non-binding instruments produced by international groups of experts have been adopted and some are included in military manuals.²⁸⁴ Examples of these non-binding instruments include the San Remo Manual on the International Law Applicable to Armed Conflicts at Sea²⁸⁵ (Naval Warfare Manual), the San Remo Manual on the Law of Non-International Armed Conflict²⁸⁶ (Non- Non-International Armed Conflict Manual), both adopted by the International Institute of Humanitarian Law and the Manual on International

²⁸³Xinmin (n 289).

²⁸⁴Michael Sang, 'Legal Regulation Of Cyber Warfare: Reviewing The Contribution Of The Tallinn Manual To The Advancement Of International Law'.

²⁸⁵'San Remo Manual on International Law Applicable to Armed Conflicts at Sea - ICRC' (*International Review of the Red Cross*, 00:00:00.0) <<https://www.icrc.org/en/doc/resources/documents/article/other/57jmsu.htm>> accessed 31 August 2023.

²⁸⁶Michael N Schmitt, Charles HB Garraway and Yoram Dinstein, *The Manual on the Law of Non-International Armed Conflict* (International Institute of Humanitarian Law 2006) <<https://centaur.reading.ac.uk/90435/>> accessed 31 August 2023.

Law Applicable to Air and Missile Warfare²⁸⁷ (Air and Missile Warfare Manual) adopted by the Harvard Program on Humanitarian Policy and Conflict Research.²⁸⁸

States have an opportunity to agree on rules of engagement, policy norms and international cooperation mechanisms to ensure a peaceful ICT environment and to promote ICTs as a tool for peace and success.²⁸⁹ The divergent opinions in the debate about how international law applies to cyberspace can fortify and diversify the debate, help to comprehend and reach wider audiences and engage and accommodate best practices of international law.²⁹⁰

The prospect of creative thinking to increase the granularity of the legal and normative analysis of international law's application to cyber-armed conflict is apparent.²⁹¹ The current debate by states on the application of international law to cyberspace is key to developing their understanding of this area and the reinforcement of their capabilities to achieve it. The continued issuance of position papers and statements by states on how international law applies to cyber activities presents an opportunity for development of state practice and *opinio juris* regarding this area.²⁹²

Additionally, matters requiring further clarification such as the status of data as a protected object in International Humanitarian Law, answers to the question of sovereignty as a rule of international law and the lawfulness of collective countermeasures can also be clarified while the debate on international law's application to cyberspace is live.²⁹³ In the recent past, progress has been made in developing global cybersecurity norms. In July 2015, government experts from 20 nations recommended cyber security norms for states geared at promoting an open, stable, secure and accessible ICT environment.²⁹⁴

²⁸⁷Bo Hurkmans, 'Manual on International Law Applicable to Air and Missile Warfare' (*Humanitarian Library*, 1 January 1970) <<https://www.humanitarianlibrary.org/resource/manual-international-law-applicable-air-and-missile-warfare>> accessed 31 August 2023.

²⁸⁸Sang (n 291).

²⁸⁹'International Law in Cyberspace: Mind the Gap :: EU Cyber Direct' (*Horizon*, 4 March 2020) <<https://eucyberdirect.eu/research/international-law-in-cyberspace-mind-the-gap>> accessed 25 August 2023.

²⁹⁰'International Law in Cyberspace: Mind the Gap :: EU Cyber Direct' (n 296).

²⁹¹Broeders and others (n 224).

²⁹²'International Law in Cyberspace' (n 62).

²⁹³'International Law in Cyberspace' (n 62).

²⁹⁴Brad Smith, 'The Need for a Digital Geneva Convention' (*Microsoft on the Issues*, 14 February 2017) <<https://blogs.microsoft.com/on-the-issues/2017/02/14/need-digital-geneva-convention/>> accessed 29 August 2023.

Powerful states have also demonstrated that they can address these issues through direct and honest bilateral talks. In September 2015, China and the United States agreed to commitments pledging that none of their governments would conduct or give support to cyber-enabled theft of intellectual property.²⁹⁵ This led to the Group of 20 affirming the same principle shortly thereafter.²⁹⁶ Similarly, if powerful states took the lead in addressing issues related to the application of international law to cyber-armed conflict by way of talks, this would undoubtedly give impetus to other states to follow suit and address these issues.²⁹⁷

3.5 Establishment of a Universal Treaty Governing Cyber Armed Conflict

The Tallinn Manual was an excellent starting point for an international dialogue on the parameters of acceptable conduct with regard to international cyber warfare.²⁹⁸ Several nations including China and Russia proposed an ‘International Code of Conduct for Information Security’, which has been interpreted as advancing totalitarian principles prevalent in these nations to the detriment of human rights.²⁹⁹ While the Code may not be as palatable as the Tallinn Manual, it demonstrates a willingness of many nations to move towards a streamlined international cyberwarfare treaty regime.³⁰⁰

According to Benjamin Mueller, cyber operations will proliferate until the day an injured state makes a decision that the law of armed conflict has been breached and retaliates accordingly. Thus, if constraints on cyber operations are put in place, such a disaster can easily be averted.³⁰¹ He rebuts the opposition to creation of a cyber-treaty due to the challenges that would be encountered when attributing attacks.³⁰² While acknowledging the legitimacy of the difficulties in the attribution of cyber operations, he states that contrary to common belief, attribution is

²⁹⁵Smith (n 301).

²⁹⁶Smith (n 301).

²⁹⁷Brad Smith, ‘The Need for a Digital Geneva Convention’ (*Microsoft On the Issues*, 14 February 2017) <<https://blogs.microsoft.com/on-the-issues/2017/02/14/need-digital-geneva-convention/>> accessed 29 August 2023.

²⁹⁸Alexi Franklin, ‘An International Cyber Warfare Treaty: Historical Analogies and Future Prospects Comments’ (2018) 7 *Journal of Law & Cyber Warfare* 149 <<https://heinonline.org/HOL/P?h=hein.journals/jlacybrwa7&i=165>> accessed 4 September 2023.

²⁹⁹Franklin (n 305).

³⁰⁰Franklin (n 305).

³⁰¹Benjamin Mueller, ‘On the Need for a Treaty Concerning Cyber Conflict’.

³⁰²Mueller (n 308).

not so much a technical issue but one of lack of international cooperation.³⁰³ Through a mixture of technical forensic and traditional intelligence network, security experts are able to come up with comprehensive investigative case after an attack.³⁰⁴ To cure this attribution challenge, he proposes the creation of an organization by treaty to facilitate cross-border law enforcement on cyberspace akin to Interpol.³⁰⁵ Signatories to the treaty would accept a positive duty to assist each other's law enforcement enquiries for specified crimes thus reducing the incentive for states to conduct offensive cyber operations through proxy actors.³⁰⁶

Further, scholars argue that a universal treaty is needed to clarify the definitions on the law of armed conflict in cyberspace, aiding in bringing clarity into this domain of warfare.³⁰⁷ With a level of certainty concerning permissible state behaviour in cyberspace, governments can move away from the strategy of maximizing cyber operations without breaching the threshold of armed attack and focus on pertinent issues such as cybercrime, which has reduced confidence in the internet.³⁰⁸ He argues that the internet is a force that can be channelled for good. If insecurity and aggression however become its characteristic features, it will lose its potential as a force for good. On the other hand, if cyberspace no longer poses as an arena of conflict with blurred rules, and militaries can approach this realm with a degree of regulatory clarity, then states can channel their energies on pursuing other issues.³⁰⁹

Suggestions have also been made that as a tool for regulation of state conduct, 'soft law' of non-binding agreements and gradual norm building is better since it is easier to convince states to join a non-binding agreement and because a soft regime is more flexible and can therefore be easily customized to suit changing circumstances.³¹⁰ Julija Kalpokiene and Ignas Kalpokas argue that contrary to this assertion, only a binding agreement especially one that contains a robust enforcement mechanism could be seen as ensuring state compliance.³¹¹

³⁰³Mueller (n 308).

³⁰⁴Mueller (n 308).

³⁰⁵Mueller (n 308).

³⁰⁶Mueller (n 308).

³⁰⁷Mueller (n 308).

³⁰⁸Mueller (n 308).

³⁰⁹Mueller (n 308).

³¹⁰Daniel Joyner, 'Jus Ad Bellum in the Age of WMD Proliferation' <<https://papers.ssrn.com/abstract=2776771>> accessed 5 September 2023.

³¹¹Julija Kalpokiene and Ignas Kalpokas, 'Contemplating a Cyber Weapons Convention: An Exploration of Good Practice and Necessary Preconditions' (2020) 13 *Baltic Journal of Law and Politics* 51 <<https://heinonline.org/HOL/P?h=hein.journals/bjlp13&i=51>> accessed 4 September 2023.

In supporting the establishment of a universal treaty governing cyberspace, Sangiovanni proposes that the large number of stakeholders in the cyber domain and for the avoidance of vast havens for cyber criminality, it is imperative that a majority of states creates an international agreement to ensure compliance in the system.³¹² Sangiovanni³¹³ argues that history has demonstrated that while international norm creation and acceptance is generally a slow process, the process is often sped up by formal treaty negotiations that add political weight and visibility to an issue.³¹⁴ She adds that while the journey to a binding international treaty may be a long and winding one, embarking on negotiations may have a positive impact.³¹⁵ While rebutting the assertion that a universal treaty on cyberspace would be unable to keep up with developments in cyberspace, she puts forward that technically all spheres of international arms control must grapple with technological advances.³¹⁶

In response to this assertion, Sangiovanni posits that most international arms control agreements make provision for periodic review conferences that make room for governments to update the terms of the agreements. Illustratively, the state parties to the Biological Weapons Treaty have held several review conferences since the Treaty came into force in 1975.³¹⁷ These conferences have focused on fortifying verification and the operation of the Treaty to cater for new scientific and technological developments.³¹⁸

In addition to this, Sangiovanni states that there is need to come up with robust norms of prohibition against cyber-attacks. The ready availability and the ease with which cyber weapons can be concealed make a case for the establishment of a universal binding treaty-governing cyberspace. Due to the uncertainty about the strength of adversaries, states must be able to trust that cyber-attacks would be met with strong international condemnation and set off severe sanctions.³¹⁹ This necessitates a formal treaty, which would stipulate the rules of prohibition and set out clear responsibility for responding to norm violations. She further notes that whereas no international agreement would be perfect and that any agreement reached on

³¹²Mette Eilstrup-Sangiovanni, 'Why the World Needs an International Cyberwar Convention' (2018) 31 *Philosophy & Technology* 379 <<https://doi.org/10.1007/s13347-017-0271-5>> accessed 18 August 2023.

³¹³Eilstrup-Sangiovanni (n 319).

³¹⁴Eilstrup-Sangiovanni (n 319).

³¹⁵Eilstrup-Sangiovanni (n 319).

³¹⁶Eilstrup-Sangiovanni (n 319).

³¹⁷Eilstrup-Sangiovanni (n 319).

³¹⁸Eilstrup-Sangiovanni (n 319).

³¹⁹Kenneth W Abbott and Duncan Snidal, 'Hard and Soft Law in International Governance' (2000) 54 *International Organization* 421 <<https://www.jstor.org/stable/2601340>> accessed 6 September 2023.

cyber governance will likely require revision in response to changes in technology it is imperative to establish a universal treaty regulating cyber space.³²⁰

The expanding scope and scale of cyber security also make the establishment of an international agreement necessary.³²¹ The threat landscape in cyber security is expanding. States are not immune from enemies who include highly sophisticated organizations that leverage integrated tools and capabilities with artificial intelligence and machine learning. Even the current highly advanced cyber controls, regardless of how effective they are will soon be obsolete.³²² International agreement in the form of a universal treaty would establish norms of international state behaviour. Hughes argues that in the absence of some rules governing cyberwarfare, states will not feel constrained to develop and deploy cyber weaponry if military and civilian planners do not comprehend the consequences.³²³

On the other hand, some scholars argue that the regulation of cyberwarfare and cyber weapons is a herculean task due to the fluid nature of cyberspace. As things currently stand, states are already grappling with the definitional challenges.³²⁴ The community of nations cannot easily reach a consensus on an issue that is constantly changing and whose specific components present challenges with respect to definitions.³²⁵

The attribution challenge has been one of the major issues that many scholars have highlighted is a barrier to any form of international agreement governing cyber conflict.³²⁶ Furthermore, whereas it may be possible to attribute cyber-attacks with some degree of precision, he argues that it is currently impossible to prove their origin beyond reasonable doubt.³²⁷

³²⁰Eilstrup-Sangiovanni (n 319).

³²¹Stephen Moore, 'Cyber Attacks and the Beginnings of an International Cyber Treaty' (2013) 39 *North Carolina Journal of International Law and Commercial Regulation* 223 <<https://search.ebscohost.com/login.aspx?direct=true&db=edshol&AN=edshol.hein.journals.ncjint39.10&site=eds-live>> accessed 7 September 2023.

³²²'Cybersecurity Trends: Looking over the Horizon | McKinsey' <<https://www.mckinsey.com/capabilities/risk-and-resilience/our-insights/cybersecurity/cybersecurity-trends-looking-over-the-horizon>> accessed 8 September 2023.

³²³Dr Rex Hughes, 'Towards a Global Regime for Cyber Warfare'.

³²⁴Christopher Rosana Nyabuto, 'A Game of Code: Challenges of Cyberspace as a Domain of Warfare' (2018) 3 *Strathmore Law Review* 49 <<https://heinonline.org/HOL/P?h=hein.journals/strathlwr3&i=53>> accessed 4 September 2023.

³²⁵Nyabuto (n 331).

³²⁶Michael N Schmitt and Liis Vihul, 'The Emergence of International Legal Norms for Cyber conflict' in Fritz Allhoff, Adam Henschke and Bradley Jay Strawser (eds) (Oxford University Press 2016) <<https://centaur.reading.ac.uk/89809/>> accessed 6 September 2023.

³²⁷Krol (n 333).

Additionally, according to Lukasz,³²⁸ the jurisdictional challenges that accompany the cross-border nature of many digital attacks and the unwillingness of states to investigate attacks that emanate from their territory makes it extremely difficult to create a global regulatory systems. Consequently, international tribunals and other organs that uphold treaties would need a very high threshold of legal certainty to come to a definite decision on this issue.³²⁹ Further, the uncertainties surrounding attribution of attacks suggest that a cyber treaty is neither likely to increase the predictability in engagements between hostile states nor would it foster a more civil atmosphere.³³⁰

History shows that treaties dealing with new technology are created only after the technology in question has been in use for some time. Treaties dealing with outer space activities were created and adopted shortly after such activities had begun.³³¹ Gil Baram and Harel Menashri argue that after new technologies emerge, it is doubtful that states would want to limit themselves before the significance and potential implications of such limitations are known – especially for military cyber operations.³³² Accordingly, a binding legal framework in the form of a cyberwar treaty can therefore be intentionally pursued only after states have familiarised themselves with emerging technologies and practices.³³³ Moreover, even if states were to limit the practical and strategic facets of cyber operations, there would still be apprehension that other states would use the same to commit hostile acts.³³⁴

They also draw attention to the complexities that exist in effectively enforcing laws and such laws and verifying that states are abiding by their stipulations. This in effect means that there is a very real possibility of every treaty dealing with cyberspace having reservations about a nation's 'privacy'.³³⁵ This challenge is compounded by the fact that the dual use nature of cyber

³²⁸Krol (n 477).

³²⁹Krol (n 333).

³³⁰ Louise Arimatsu, 'A Treaty for Governing Cyber-Weapons: Potential Benefits and Practical Limitations'.

³³¹Gil Baram and Harel Menashri, 'Why Can't We Be Friends? Challenges to International Cyberwarfare Cooperation Efforts and the Way Ahead' (2019) 38 Comparative Strategy 89 <<https://doi.org/10.1080/01495933.2019.1573069>> accessed 5 September 2023.

³³²Baram and Menashri (n 337).

³³³Michael N Schmitt and Liis Vihul, 'The Nature of International Law Cyber Norms'.

³³⁴Baram and Menashri (n 337).

³³⁵Baram and Menashri (n 337).

weapons and the ease with which cyber operations can be concealed.³³⁶ This makes the inspection and verification of such tools close to impossible.

States can therefore move from a state of compliance to gross violation in a matter of seconds and without warning.³³⁷ Critics have also argued that states would not wish to comply with an international treaty regulating cyber-armed conflict unless they are certain that other states are also complying. Additionally, there is minimal possibility of integrating a verification system into a cyber space treaty regime.³³⁸ It is improbable that a state would consent to external verification measures which may mean scanning devices such as computers owned and used by the state including all classified systems.³³⁹ This is a huge obstacle taking into account the success of arms control treaties has been mainly hinged on the existence of vibrant compliance and verification regimes.³⁴⁰ This means that any cyber treaty would fall apart very fast and very easily.³⁴¹

States do not have control, monopoly or ownership of cyber weapons, States are often users of malicious programmes while private sector usually has ownership of malicious code. Thus, states would be unwilling to make a commitment to control cyber weapons yet they are beyond their control.³⁴²

Another basis for the opposition against the creation of a cyber-treaty is that cyberwarfare is still in its formative stages and it is premature to start work on a global regime to govern it.³⁴³ Finnemore³⁴⁴ argues that negotiation of treaties is a long and cumbersome process that is not well suited to fast and ever-changing issues such as cyber security and internet governance. In support of this argument, she notes that negotiation of the United Nations Treaty on the Laws of the Sea took more than ten years. Further, the cyber domain is characterized by conflicts of interest and highly disjointed power, which makes formal agreement unachievable. These

³³⁶Chris Bronk, PW Singer and Allan Friedman, 'Review of Cybersecurity and Cyberwar: What Everyone Needs to Know, Singer P. W., Friedman Allan' (2015) 9 Strategic Studies Quarterly 141 <<https://www.jstor.org/stable/26270839>> accessed 6 September 2023.

³³⁷Richard A Clarke and Robert K Knake, *Cyber War: The next Threat to National Security and What to Do about It* (1st ed, Ecco 2010).

³³⁸ Arimatsu (n 480).

³³⁹ Arimatsu (n 480).

³⁴⁰ Arimatsu (n 480).

³⁴¹Eilstrup-Sangiovanni (n 319).

³⁴² Nyabuto (n 473).

³⁴³Hughes (n 320).

³⁴⁴Martha Finnemore, 'Cultivating International Cyber Norms'.

conditions favour devolved cooperation premised on flexible, non-binding commitment as opposed to a formal, centralized approach.³⁴⁵

The different imbalance among states' cyber capabilities and vulnerabilities may also prove to be a real challenge to conclusion of a cyber treaty. Less militarily developed states may not willingly give up an opportunity to achieve a level of equality with wealthy, more developed states through development of their cyber capabilities.³⁴⁶ The affordability and ease of acquisition of cyber weapons allows state and non-state actors alike to potentially cause serious harm to stronger, more superior states. This strategic advantage is one that few states may be willing to give up.³⁴⁷

According to Sang, the enforcement of international treaty restrictions on the use of specific weapons is a key impediment to the conclusion of a cyber treaty. One of the key issues with cyberspace is the effective enforcement of treaty prohibitions.³⁴⁸ To begin with, the unique nature of cyber-armed conflict necessitates a distinct approach and specialized knowledge in order to fully appreciate the scope of rights, obligations, and remedies involved.³⁴⁹ Second, when cyber activities are used, it may be difficult to confirm that an international unlawful act has been committed. In any case, even if it were possible to assign and discover a breach, the issue of attribution would remain unresolved.³⁵⁰

Another significant impediment to enforcement will be the issue of jurisdiction.³⁵¹ The growing number of non-state actors with strong cyber capabilities, along with these actors' failure to comply with international law constraints, makes it even more difficult to enforce traditional prohibitions.³⁵² States will undoubtedly reject any treaty clause that limits their cyber action against non-state entities that violate cyber treaty prohibitions.³⁵³

³⁴⁵ Finnemore (n 346).

³⁴⁶ Sang (n 275).

³⁴⁷ Sang (n 275).

³⁴⁸ Sang (n 275).

³⁴⁹ Sang (n 275).

³⁵⁰ Sang (n 275).

³⁵¹ Sang (n 275).

³⁵² Sang (n 275).

³⁵³ Sang (n 275).

3.6 Conclusion

Efforts have been made to customize the extant international law to the fifth domain of armed conflict with the most prominent of these efforts being the Tallinn Manual on the Application of International Law to Cyberwarfare. While the Manual may not be perfect, it has served to illustrate how international law as we currently know it may be applied to armed conflict in cyberspace. This Manual is a seminal work that has drawn recognition even from states in their statements on the application of international law to cyberspace. While there is no international consensus on *how* international law applies to cyberspace, there is agreement that indeed, it does apply.

This application is however not devoid of challenges. As clearly pointed out the use of old wineskins for new wine has drawn criticism from many quarters with some scholars arguing that cyberspace needs to be governed by a universal treaty specifically established for that purpose while other scholars argue that the law as we have it suffices. There are also scholars, who, while acknowledging that indeed a universal treaty needs to be established, argue that the time for such discussions is not nigh.

CHAPTER FOUR

4.0 CONCLUSION AND RECOMMENDATIONS

4.1 Conclusions

The main objective of this study was to identify and analyse the international and regional legal frameworks governing cyber-armed conflict. The specific objectives of the study were; to discuss and delineate the concept and scope of cyber armed conflict, to examine the challenges and opportunities of applying the existing international legal rules to cyber armed conflict and to as if there is a need to establish a universal international treaty governing cyber armed conflict. This study has met its main and specific objectives.

Chapter One gave a broad overview and layout of the study and gave a background of the emergence of cyberspace as a new frontier for battle. Chapter Two delineated and contextualized the concept of cyber-armed conflict. It traced the evolution of the debate on the application of international law to cyber space and to cyber armed conflict. The research in this chapter established that there are no regional or international legal frameworks specifically governing cyber armed conflict. In the absence of these, the Chapter analysed the Tallinn Manual on the International Law Applicable to Cyber Warfare, which is a seminal scholarly work that illustrates how existing international law is applicable to Cyber warfare. Further, the Chapter analysed the Tallinn Manual on the International Law Applicable to Cyberwarfare.

Chapter Three highlighted the positions taken by various states on the application of international law to cyberspace. It examined the challenges in the application of existing international law to cyber-armed conflict and the opportunities that accompany this application. Finally, the chapter delved into the arguments raised for and against the establishment of a universal binding treaty governing cyber-armed conflict.

Ultimately, Chapter Four concludes that the extant international law does not adequately cater for the peculiarities of cyberspace. Despite arguments against the establishment of a universal treaty governing cyber-armed conflict, this study recommends the establishment of a universal treaty as one of the possible ways of dealing with the challenge of governing cyberspace.

4.2 Recommendations

This study makes the following recommendations based on the research findings

4.2.1 Establishment of a Universal Treaty Governing Cyber-Armed Conflict

The existing international law is not adequate to govern cyber-armed conflict. In the absence of clear limits as to what conduct actors can engage in cyberspace, state and non-state actors will continue to push the limits. While this may occur unabated on some occasions, it may only be a matter of time before a state feels violated by cyber-attacks and reacts in response to this violation, which may result in disaster. A cyber treaty would help prevent the escalation of cyber-attacks to full-blown cyber armed conflict.

Additionally, the establishment of a universal treaty will not only limit the possibility of such retaliatory attacks happening but it will also help establish norms of acceptable behaviours in cyberspace and promote greater transparency and accountability among the community of nations. Further, a cyber-treaty would serve to protect states from each other. In particular, states with less advanced cyber capabilities would be protected from ‘mightier’ states who have advanced and sophisticated cyber capabilities.

A well-drafted cyber treaty would help protect the critical infrastructure of states such as power grids and transportation systems from cyber-attacks in addition to encouraging the ethical use of technology. A cyber treaty would without a doubt promote international cooperation, reduce the risk of conflict between nations and promote increased stability in the international system. Cyber-attacks directed against states could result in significant economic damage. Creation of a treaty for cyberspace could help prevent the likelihood of such attacks happening and ensure that the global economy remains stable.

Additionally, a cyber-treaty would limit cyber-attacks and make the way for international peace. Borrowing from The Convention on the Prohibition of the Development, Production, Stockpiling and Use of Chemical Weapons and on their Destruction (Chemical Weapons Convention), a cyber treaty could establish an independent organ to monitor cyber activities that happen across boundaries and assist with attribution of cyber activities to a particular actor. To avert the possibility of any one state monopolizing the organization, a representative structure could be adopted. The power of the organization would be limited and serious

infractions would be submitted to the United Nations' organs such as the General Assembly or the Security Council.

Upon ratification of the cyber treaty states can domesticate the treaty by passing municipal legislation that would make provisions such as the prohibition of individuals or private organizations from developing or using malicious code. A cyber treaty would make provision for frameworks to address violations of the treaty and support states in responding to cyber-attacks. While a cyber treaty does not guarantee that cyber armed conflict will not occur, the complete lack of an instrument regulating cyber space leaves it open for use and abuse by all.

While the benefits of concluding a treaty are considerable, the process of making a treaty is long and convoluted, punctuated by multiple impediments. A new convention would be best developed once existing objections to the implementation of existing international law have been resolved. It may also be counterproductive to add more legal instruments to the already massive pile of current international accords that are straining to adapt to socio-political developments.

Political processes are used to create treaties. As a result, they require political backing to be effective. It is certainly conceivable to sign a pact while having minimal governance influence. Based on the current dispersion of view among states and the lack of pronouncements on how international law should be applied in cyberspace, it is difficult to conclude that a cyber convention, even if finished, would gain strong support from states to ensure its efficacy. The problems with the compliance and verification mechanisms identified in this study also constitute a severe threat to the success of a cyber treaty.

4.2.2 Weapons Review

In the face of the many challenges that conclusion of a universal treaty may encounter, one possibility for the international community to handle cyberspace concerns is international collaboration in weapons review which will provide states with insight into potential future challenges, as well as ways for enforcing armed conflict rules.

Since the internet provides people with anonymity, malicious actors can use it to commit crimes without being identified. Due to the fact that the equipment and expertise used in cyberwarfare are widely available to civilians, cyberspace provides an unsafe setting in which total war may erupt. The laws of armed conflict do not protect civilians who directly participate

in hostilities. The goal of international humanitarian law is to alleviate the suffering caused by armed conflict, not to justify the use of cyber warfare as a deterrence to violations of international humanitarian law.

To that aim, Article 36 of the Additional Protocol I requires state parties to decide whether the use of new weapons, tools, or tactics of combat is prohibited by the protocol or any other rule of international law. This evaluation aids the execution of International Humanitarian Law, addresses future weaponry and may provide a solution to the issues caused by cyber-attacks.

4.2.3 Capacity building in the area of cyber security

There is need to build capacity in the area of cyber security. While cyber security is a sensitive issue in modern national intelligence, the need to build capacity in the area of cyberspace is evident. States must embrace national cyber security education strategies that support multiple initiatives, as well as the creation of a multi-stakeholder space in which government, industry, and academia can collaborate to address national cyber security educational requirements. Additional activities should include improving educator training and cyber security programmes, as well as pushing for research and development skills and cyber security awareness. The treaty-based organization proposed may also be used to provide training to officials of state parties that may lack the resources or knowledge to train in cyber security.

4.2.4 Multi-stakeholder Engagement in cyber security

The use of cyberspace is not a preserve of states. While international law is mainly moulded by states, it is important to engage various stakeholders including academia, the private sector and civil society in the discussions and decision-making process. It is imperative to ensure that all relevant actors in this domain have their voices heard. Addressing threats from cyberspace requires a concerted, collective and multi-stakeholder response. This approach will tap into the capacity and the knowledge that these stakeholders have to support the designing of rules and principles governing this sphere. Additionally, a multi-stakeholder approach will ensure that the contributions of academia, civil society, industry and states are taken into consideration across the pillars of any framework that would be agreed upon and incorporated into its implementation.

BIBLIOGRAPHY

BOOKS

Hurkmans B, *Manual on International Law Applicable to Air and Missile Warfare* (Humanitarian Library1 January 1970)
<<https://www.humanitarianlibrary.org/resource/manual-international-law-applicable-air-and-missile-warfare>> accessed 18 October 2023

Ministry of Defence, *Manual of the Law of Armed Conflict (JSP 383)* (GOV.UK2013)
<<https://www.gov.uk/government/collections/jsp-383>> accessed 12 December 2021

Sassòli M, *International Humanitarian Law: Rules, Controversies, and Solutions to Problems Arising in Warfare* (www.elgaronline.com29 March 2019)
<<https://www.elgaronline.com/view/9781786438546/9781786438546.xml>> accessed 18 October 2023

Schmitt M, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (Cambridge University Press 2017)

Schmitt M, *Tallinn Manual on the International Law Applicable to Cyber Warfare : Prepared by the International Group of Experts at the Invitation of the NATO Cooperative Cyber Defence Centre of Excellence* (Cambridge University Press 2013)

Schmitt MN, Garraway CHB and Dinstein Y, *The Manual on the Law of Non-International Armed Conflict* (International Institute of Humanitarian Law 2006)
<<https://centaur.reading.ac.uk/90435/>> accessed 18 October 2023

BOOK CHAPTERS

Clarke RA, *Cyber War: The next Threat to National Security and What and What to Do About It* (Ecco 2010)

Hughes R, *Towards a Global Regime Cyberspace* in Christian Czosseck and Kenneth Geers (eds), *The Virtual Battlefield: Perspectives in Cyber Warfare* (IOS Press 2009)

CONFERENCE PAPERS

Mačák K, “Is the International Law of Cyber Security in Crisis?” 2016 8th International Conference in Cyber Conflict (CyCon) (IEEE 2016) <<https://ieeexplore.ieee.org/abstract/document/7529431/>>

INTERNET SOURCES

Association for Progressive Communications, ‘Open Letter to UN General Assembly: Proposed International Convention on Cybercrime Poses a Threat to Human Rights Online | Association for Progressive Communications’ (www.apc.org2019)<<https://www.apc.org/en/pubs/open-letter-un-general-assembly-proposed-international-convention-cybercrime-poses-threat-human>> accessed 18 October 2023

Cherry L and Pascucci P, ‘International Law in Cyberspace’ (2023) <https://www.americanbar.org/groups/law_national_security/publications/aba-standing-committee-on-law-and-national-security-60-th-anniversary-an-anthology/international-law-in-cyberspace/>

Crawford E, ‘Armed Ukrainian Citizens: Direct Participation in Hostilities, Levée En Masse, or Something Else?’ (EJIL: Talk!1 March 2022) <<https://www.ejiltalk.org/armed-ukrainian-citizens-direct-participation-in-hostilities-levee-en-masse-or-something-else/>> accessed 2 June 2022

FBI, ‘The Morris Worm | Federal Bureau of Investigation’ (Federal Bureau of Investigation2 November 2018) <<https://www.fbi.gov/news/stories/morris-worm-30-years-since-first-major-attack-on-internet-110218>>

Geneva Academy, ‘Non-International Armed Conflicts in Democratic Republic of Congo | Rulac’ (www.rulac.org) <<https://www.rulac.org/browse/conflicts/non-international-armed-conflict-in-democratic-republic-of-congo>> accessed 1 December 2022

Li H and Zhang J, ‘Application of Existing Rules of International Law in Cyberspace’ (www.atlantis-press.com29 April 2022) 169 <<https://www.atlantis-press.com/article/125973741>> accessed 18 October 2023

McKinsey, ‘Cybersecurity Trends: Looking over the Horizon | McKinsey’

<<https://www.mckinsey.com/capabilities/risk-and-resilience/our-insights/cybersecurity/cybersecurity-trends-looking-over-the-horizon>> accessed 8 September 2023

Taddeo M, 'Why We Need Philosophy and Ethics of Cyber Warfare | University of Oxford' (www.ox.ac.uk 16 June 2022) <<https://www.ox.ac.uk/news/2022-06-16-why-we-need-philosophy-and-ethics-cyber-warfare>>

JOURNAL ARTICLES

——, 'Direct Participation in Hostilities | How Does Law Protect in War? - Online Casebook' (*casebook.icrc.org*) <<https://casebook.icrc.org/glossary/direct-participation-hostilities>> accessed 22 December 2020

——, 'The Application of the Principle of Distinction in the Cyber Context: A Chinese Perspective' (*International Review of the Red Cross* 1 March 2021) <<http://international-review.icrc.org/articles/principle-of-distinction-cyber-context-chinese-perspective-913>> accessed 18 October 2023

——, 'Unblurring the Lines: Military Cyber Operations and International Law' (2021) 6 *Journal of Cyber Policy* 411 <<https://doi.org/10.1080/23738871.2021.2014919>>

——, *Combatants | How Does Law Protect in War? - Online Casebook* <<https://casebook.icrc.org/glossary/combatants>> accessed 5 January 2022

——, *International Humanitarian Law and Cyber Operations during Armed Conflicts - ICRC Short Papers* <<https://www.icrc.org/en/document/short-papers-on-international-humanitarian-law-and-cyber-operations-during-armed-conflicts>> accessed 18 October 2023

Abbott KW and Snidal D, 'Hard and Soft Law in International Governance' (2000) 54 *International Organization* 421 <<https://www.jstor.org/stable/2601340>>

Akande D, Coco A and Dias T de S, 'Drawing the Cyber Baseline: The Applicability of Existing International Law to the Governance of Information and Communication Technologies' (2022) 99 *International Law Studies*

Baram G and Menashri H, 'Why Can't We Be Friends? Challenges to International Cyberwarfare Cooperation Efforts and the Way Ahead' (2019) 38 *Comparative Strategy* 89

Basu A, 'The Potential for the Normative Regulation of Cyberspace: Implications for India' (Elonnai Hickok, Sunil Abraham and Udbhav Tiwari (eds)

Broeders D and others, 'Revisiting Past Cyber Operations in Light of New Cyber Norms and Interpretations of International Law: Inching towards Lines in the Sand?' [2022] *Journal of Cyber Policy* 1

Bronk C, Singer PW and Friedman A, 'Review of Cybersecurity and Cyberwar: What Everyone Needs to Know, Singer P. W., Friedman Allan' (2015) 9 *Strategic Studies Quarterly* 141 <<https://www.jstor.org/stable/26270839>> accessed 17 December 2021

Brown G, 'International Law Applies to Cyber Warfare! Now What?' (2017) 46 *Southwestern Law Review* 355

Check T, 'Book Review: Analyzing the Effectiveness of the Tallinn Manual's Jus Ad Bellum Doctrine on Cyber Conflict, a NATO-Centric Approach' [2013] *SSRN Electronic Journal* <<http://www.ssrn.com/abstract=2347736>> accessed 19 July 2023

Darcy S, 'What Future for the Doctrine of Belligerent Reprisals?' (2002) 5 *Yearbook of International Humanitarian Law* 107

Dipert RR, 'The Ethics of Cyberwarfare' (2010) 9 *Journal of Military Ethics* 384 <<http://www.tandfonline.com/doi/abs/10.1080/15027570.2010.536404>>

Droege C, 'Get off My Cloud: Cyber Warfare, International Humanitarian Law, and the Protection of Civilians' (2012) 94 *International Review of the Red Cross* 533 <<https://www.cambridge.org/core/journals/international-review-of-the-red-cross/article/get-off-my-cloud-cyber-warfare-international-humanitarian-law-and-the-protection-of-civilians/72114EF6E71757FAB2B37E7DE918B2BB>>

Easterbrook F, 'Cyberspace and the Law of the Horse' *The University Of Chicago Legal Forum*

Efrony D and Shany Y, 'A Rule Book on the Shelf? Tallinn Manual 2.0 on Cyber operations and Subsequent State Practice' (2018) 112 *The American Journal of International Law* 583 <<https://www.jstor.org/stable/26568993>> accessed 18 October 2023

Eilstrup-Sangiovanni M, 'Why the World Needs an International Cyberwar Convention' (2017) 31 *Philosophy & Technology* 379 <<https://link.springer.com/article/10.1007/s13347-017-0271-5>> accessed 11 November 2019

Fang Y, 'Is the Current International Law a Good Fit for Cybersecurity? A U.N. Charter-Based Analysis' (2021) 20 Washington University Global Studies Law Review 549

Finnemore M, 'Cultivating International Cyber Norms'

Fleck D, 'Searching for International Rules Applicable to Cyber Warfare--A Critical First Assessment of the New Tallinn Manual' (2013) 18 Journal of Conflict and Security Law 331 <<https://academic.oup.com/jcsl/article-lookup/doi/10.1093/jcsl/krt011>> accessed 25 July 2023

Franklin A, 'An International Cyber Warfare Treaty: Historical Analogies and Future Prospects Comments' (2018) 7 Journal of Law & Cyber Warfare 149 <<https://heinonline.org/HOL/P?h=hein.journals/jlacybrwa7&i=165>> accessed 9 April 2023

Garkusha-BozhkoSYu, 'Application of the Principles of International Humanitarian Law (Principles of Distinction, Proportionality, and Precaution) to Armed Conflicts in Cyberspace' (2021) 8 Russian Journal of Legal Studies (Moscow) 73

Gisel L, Rodenhäuser T and Dörmann K, 'Twenty Years On: International Humanitarian Law and the Protection of Civilians against the Effects of Cyber Operations during Armed Conflicts' (2020) 102 International Review of the Red Cross 287 <https://www.cambridge.org/core/product/identifier/S1816383120000387/type/journal_article> accessed 21 June 2023

Heideman R, 'Legalizing Hate: The Significance of the Nuremberg Laws and the Post-War Nuremberg Trials' (2017) 39 Loyola of Los Angeles International and Comparative Law Review (ILR) <<https://digitalcommons.lmu.edu/ilr/vol39/iss1/2>>

Henriksen A, 'The End of the Road for the UN GGE Process: The Future Regulation of Cyberspace' (2019) 5 Journal of Cybersecurity

Hollis D, 'A Brief Primer on International Law and Cyberspace' (Carnegie Endowment for International Peace 14 June 2021) <<https://carnegieendowment.org/2021/06/14/brief-primer-on-international-law-and-cyberspace-pub-84763>>

Inglis C, 'Cyberspace—Making Some Sense of It All' (2016) 15 Journal of Information Warfare 17 <<https://www.jstor.org/stable/26487528>> accessed 23 February 2023

International Committee of the Red Cross, 'Non-International Armed Conflict | How Does Law Protect in War? - Online Casebook' (*Icrc.org*2011) <<https://casebook.icrc.org/glossary/non-international-armed-conflict>> accessed 15 May 2019

Janssens PC and Wouters J, 'Informal International Law-Making: A Way around the Deadlock of International Humanitarian Law?' (2022) 104 *International Review of the Red Cross* 2111

Jordan WJ, 'Controlling Cyberwarfare '

Joyner D, 'Jus Ad Bellum in the Age of WMD Proliferation' <<https://papers.ssrn.com/abstract=2776771>>

Kalpokiene J and Kalpokas I, 'Contemplating a Cyber Weapons Convention: An Exploration of Good Practice and Necessary Preconditions' (2020) 13 *Baltic Journal of Law and Politics* 51 <<https://heinonline.org/HOL/P?h=hein.journals/bjlp13&i=51>>

Katagiri N, 'Why International Law and Norms Do Little in Preventing Non-State Cyber Attacks' (2021) 7 *Journal of Cybersecurity*

Khawaja AA, 'Cyber Warfare and International Humanitarian Law' (*DLP Forum* 17 August 2022) <<https://www.dlpforum.org/2022/08/17/cyber-warfare-and-international-humanitarian-law/>>

Kilovaty I, 'Cyber Warfare and the Jus Ad Bellum Challenges: Evaluation in the Light of the Tallinn Manual on the International Law Applicable to Cyber Warfare' (2014) 5 *American University American University National Security Law Brief*

Krol LA, 'Look toward Norms, Not Treaties, to Regulate Digital Weapons' (2019) 14 *Yale Journal of International Affairs* 31 <<https://heinonline.org/HOL/P?h=hein.journals/yaljoia14&i=38>>

Lahmann H, 'State Behaviour in Cyberspace: Normative Development and Points of Contention' (2023) 16 *Zeitschrift für Außen- und Sicherheitspolitik* 31

Lotrionte C, 'Cyber Operations: Conflict under International Law' [2012] *Georgetown Journal of International Affairs* 15 <<https://www.jstor.org/stable/43134334>>

Mačák K, 'Military Objectives 2.0: The Case for Interpreting Computer Data as Objects under International Humanitarian Law' (2015) 48 *Israel Law Review* 55

Madubuike-Ekwe JN, 'Cyberattack and the Use of Force in International Law' (2021) 12 *Beijing Law Review* 631

<<https://www.scirp.org/journal/paperinformation.aspx?paperid=109997#ref39>>

Mayuko LCT, 'Issues Concerning Cyber Attacks in Light of the Law of Armed Conflict' 7
Air and Space Power Studies

Moore S, 'Cyber Attacks and the Beginnings of an International Cyber Treaty' (2013) 39 North
Carolina Journal of International Law 223

Moynihan H, 'The Vital Role of International Law in the Framework for Responsible State
Behaviour in Cyberspace' (2020) 6 Journal of Cyber Policy
<<https://www.tandfonline.com/doi/full/10.1080/23738871.2020.1832550>>

Mueller B, 'The Laws of War and Cyberspace: On the Need for a Treaty Concerning Cyber
Conflict' <<https://core.ac.uk/download/pdf/35432773.pdf>>

NATO Cooperative Cyber Defence Centre of Excellence, 'Attribution' (International Cyber
law: Interactive Toolkit 28 July 2023) <<https://cyberlaw.ccdcoe.org/wiki/Attribution>> accessed
18 October 2023

Nyabuto CR, 'A Game of Code: Challenges of Cyberspace as a Domain of Warfare' (2018) 3
Strathmore Law Review 49
<<https://heinonline.org/HOL/P?h=hein.journals/strathlwrv3&i=53>>

Piątkowski M, 'The Definition of the Armed Conflict in the Conditions of Cyber Warfare'
(2017) 46 Polish Political Science Yearbook 271' (2017) 1 Polish Political Science Yearbook
271 <<https://czasopisma.marszalek.com.pl/10-15804/ppsy/142-vol-46/issue-1/155-ppsy20171117>>

Pipyros K and others, 'Cyber operations and International Humanitarian Law' (2016) 24
Information and Computer Security 38 <<https://doi.org/10.1108/ICS-12-2014-0081>> accessed
1 October 2020

Pomerleau M, 'The Need for International Law in Cyberspace' (C4ISRNet9 February 2017)
<<https://www.c4isrnet.com/2017/02/09/the-need-for-international-law-in-cyberspace/>>
accessed 18 October 2023

Rejali S and Heiniger Y, 'The Role of Digital Technologies in Humanitarian Law, Policy and
Action: Charting a Path Forward' (2020) 102 International Review of the Red Cross 1
<<https://international-review.icrc.org/sites/default/files/reviews-pdf/2021-03/digital-technologies-humanitarian-law-policy-action-913.pdf>> accessed 27 April 2021

Schmitt M and Vihul L, 'The Nature of International Law Cyber Norms' (2014)

Schmitt M, 'Classification of Cyber Conflict' (2012) 17 *Journal of Conflict and Security Law* 245 <<https://academic.oup.com/jcsl/article-lookup/doi/10.1093/jcsl/krs018>> accessed 25 May 2020

Schmitt MN and Vihul L, 'The Emergence of International Legal Norms for Cyber conflict' (Fritz Allhoff, Adam Henschke and Bradley Jay Strawsereds, *centaur.reading.ac.uk* 18 February 2016) 34 <<https://centaur.reading.ac.uk/89809/>> accessed 18 October 2023

Schmitt MN, 'Grey Zones in the International Law of Cyberspace' (papers.ssrn.com 18 October 2017) <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3180687> accessed 27 April 2022

Slack C, 'Wired yet Disconnected: The Governance of International Cyber Relations' (2016) 7 *Global Policy* 69

Sohail H, 'Fault Lines in the Application of International Humanitarian Law to Cyberwarfare' [2022] *Journal of Digital Forensics, Security and Law* <<https://commons.erau.edu/jdfsl/vol17/iss1/8/>>

Tikk E, 'International Law in Cyberspace: Mind the Gap EU Cyber Direct' (Horizon4 March 2020) <<https://eucyberdirect.eu/research/international-law-in-cyberspace-mind-the-gap>> accessed 18 October 2023

Winter E, 'Cyber Warfare and Levées En Masse in International Humanitarian Law: New Wine into Old Wineskins' (*www.jurist.org* 22 July 2022) <<https://www.jurist.org/features/2022/07/22/cyber-warfare-and-levees-en-masse-in-international-humanitarian-law-new-wine-into-old-wineskins/>> accessed 18 October 2023

POSITION PAPERS

Australian Government, 'Australia's Position on the Application of International Law to State Conduct in Cyberspace' (2017)

Department of Foreign Affairs, 'Ireland Position Paper on the Application of International Law in Cyberspace' (2023)

Engdahl O, 'Sweden's Position Paper on the Application of International Law in Cyberspace' [2023] *Nordic Journal of International Law* 1

Government Offices of Sweden, 'Position Paper on the Application of International Law in Cyberspace' (2022)

Kjelgaard JM and Melgaard U, 'Denmark's Position Paper on the Application of International Law in Cyberspace: Introduction' (2023) -1 Nordic Journal of International Law 1 <<https://brill.com/view/journals/nord/aop/article-10.1163-15718107-20230001/article-10.1163-15718107-20230001.xml>> accessed 18 October 2023

Ministero degli Affari Esteri della Cooperazione Internazionale, 'Italian Position Paper on International Law and Cyberspace.' (2021)

Ministry of Foreign Affairs, Republic of Poland, 'The Republic of Poland's Position on the Application of International Law in Cyberspace - Ministry of Foreign Affairs Republic of Poland - Gov.pl Website' (Ministry of Foreign Affairs Republic of Poland 2022) <<https://www.gov.pl/web/diplomacy/the-republic-of-polands-position-on-the-application-of-international-law-in-cyberspace>>

Republic of Finland, 'Cyber and International Law; Finland's Views'

The Federal Government of Germany, 'On the Application of International Law in Cyberspace' (2021)

Trade NZM of FA and, 'The Application of International Law to State Activity in Cyberspace' (New Zealand Ministry of Foreign Affairs and Trade 1 December 2020) <<https://www.mfat.govt.nz/en/media-and-resources/the-application-of-international-law-to-state-activity-in-cyberspace/>> accessed 10 June 2023

REPORTS

—, 'UN Official Compendium of National Contributions on How International Law Applies to Use of ICT by States A-76-136-EN' (2021)

United Nations, 'The Application of International Law in Cyberspace: State of Play – UNODA' (www.un.org 2018) <<https://www.un.org/disarmament/update/the-application-of-international-law-in-cyberspace-state-of-play/>> accessed 26 March 2020

THESES

Sang M, 'Legal Regulation of Cyber Warfare: Reviewing the Contribution of the Tallinn Manual to the Advancement of International Law' (Thesis 2015)