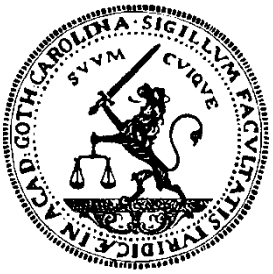

FACULTY OF LAW

LUND UNIVERSITY

Demi Bylon

Cyber Warfare in Ukraine and Beyond

Jus in Bello and Its Application to Wartime Cyber Operations

JURM02 Graduate Thesis

Graduate Thesis, Master of Laws Program

30 Higher Education Credits

Supervisor: Markus Gunneflo

Semester: Fall Semester 2022

Contents

Summary

International Humanitarian Law (IHL), also referred to as *jus in bello,* constitutes the laws regulating the conduct of parties engaged in an armed conflict. Over the past few decades, the emergence of cyberspace as a domain of war has given rise to discussions on the application of IHL to wartime cyber operations. Despite the consistent reiteration of the application of international law to cyberspace, the jus in bello framework remains a subject of debate.

The Russo-Ukrainian war illustrates the latest example of the deployment of different means of warfare, including conventional, kinetic warfare as well as acts of cyber warfare. The impact of these wartime cyber operations on societal functions vital to civilians has been significant.

This thesis sets out to examine the use of cyber operations in international armed conflicts and the application of the jus in bello regime. By analysing the current legal landscape of IHL through the lens of the cyber elements in the Russo-Ukrainian war, this thesis provides a critical analysis of lex lata, i.e. the law as it is, and suggest possible ways forward. The research takes into consideration that the application of international law in cyberspace, and the application of IHL in particular, is heavily affected by States' political objectives in the current geopolitical context.

The findings show that the current application of IHL, as outlined in guiding instruments such as the Tallinn Manual 2.0, does not encompass the complexities of cyber warfare. The author calls for further efforts to enforce the objective of the jus in bello regime in the cyber domain. Moving forward, it is suggested that the core principles and provisions of IHL should be discussed amongst Sates in multilateral fora and that national positions should be shared in order to form a general approach.

Sammanfattning

Internationell humanitär rätt, även kallad *jus in bello*, utgör de lagar som reglerar parters uppförande under en väpnad konflikt. Under de senaste decennierna har framväxten av cyberrymden som en domän för krigföring gett upphov till diskussioner om tillämpningen av internationell humanitär rätt vid krigstida cyberoperationer. Folkrättens tillämplighet i cyberrymden har konsekvent blivit bekräftad – jus in bello är däremot fortsatt föremål för debatt.

Det rysk-ukrainska kriget illustrerar det senaste exemplet på användningen av ett brett spektrum av metoder av krigföring, inkluderat såväl konventionell, kinetisk krigföring som cyberkrigföring. Effekterna av dessa krigstida cyberoperationer på samhällsfunktioner av vikt för den civila befolkningen har varit betydande.

Denna studie syftar till att undersöka användningen av cyberoperationer i internationella väpnade konflikter och tillämpningen av jus in bello. Genom att analysera det nuvarande rättsliga landskapet av internationell humanitär rätt i ljuset av cyberelementen i det rysk-ukrainska kriget, förser uppsatsen en kritisk analys av rättsläget och föreslår möjliga vägar framåt. Utredningen tar i beaktning att tillämpningen av internationell rätt i cyberrymden, och tillämpningen av internationell humanitär rätt i synnerhet, i hög grad påverkas av staters politiska agendor.

Resultaten visar att den nuvarande tillämpningen av internationell humanitär rätt, som beskrivs i vägledande instrument som Tallinn Manual 2.0, inte omfattar cyberkrigföringens komplexitet. Författaren efterlyser ytterligare ansträngningar för att genomdriva syftet med jus in bello i cyberdomänen på ett mer ändamålsenligt sätt. Det föreslås att de centrala principerna och bestämmelserna i den internationella humanitära rätten bör diskuteras stater emellan i multilaterala forum och att nationella positioner bör offentliggöras för att möjliggöra utformningen av en allmän inriktning.

Abbreviations

CCDCOE	NATO Cooperative Cyber Defence Centre of Excellence
CNI	Critical National Infrastructure
DDoS	Distributed Denial-of-Service
ENISA	European Union Agency for Cybersecurity
GGE	United Nations Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security
ICJ	International Criminal Court of Justice
ICRC	International Committee of the Red Cross
ICT	Information and Communications Technologies
IHL	International Humanitarian Law
OEWG	Open-ended Working Group on security of and in the use of information and communications technologies
PoA	Programme of Action

1 Introduction

1.1 Background

The advancement of information and communications technologies (ICT), including the use of computer networks, has brought numerous benefits and opportunities for mankind. According to some scholars, the COVID-19 pandemic has further accelerated our reliance on digital means, both as a society and as individuals.[1] As of July 2022, 69% of the global population had access to the Internet, which represents an increase of 1,416% since 2000.[2] By 2021, 92% of the households in the European Union had Internet access, which corresponds to an increase of 20 percentage points from just ten years prior.[3] Cyberspace can be used to facilitate problem-solving and streamline many crucial functions for society, yet the increased interconnectivity is a double-edged sword, expanding the attack surface for hostile cyber operations. The consequences of the developing cyber threat landscape are of major concern worldwide, and the concept of an open, free, secure and peaceful cyberspace seems to be a utopia out of reach.[4]

The increased dependence has also been acknowledged as something to observe in the context of war. In 2012, the then American Defence Secretary Leon E. Panetta warned that due to the intensified hostile behaviour of nation adversaries the United States was more susceptible to attacks from foreign computer hackers with the aim to disrupt the power grid, transportation systems, financial institutions and overarching governmental operations.

[1] Schmitt, 'Introduction to the Research Handbook on International Law and Cyberspace', in Tsagourias, Nikolaos K. and Buchan, Russell (2021), p. 1.
[2] Internet World Stats: Usage and Population Statistics, <https://www.internetworldstats.com/stats.htm>, accessed 28 December 2022.
[3] Statista Research Department, 'Share of households with internet access in the European Union (EU) from 2008 to 2021', 11 August 2022 <https://www.statista.com/statistics/377585/household-internet-access-in-eu28/> accessed 2 January 2023.
[4] Gisel, Rodenhäuser and Dörmann (2020), 'Twenty Years on: International Humanitarian Law and the Protection of Civilians against the Effects of Cyber Operations during Armed Conflicts', 102 International Review of the Red Cross 287 [Twenty years on]; The European Union Institute for Security Studies (EUISS), 'A Language of Power: Cyber defence in the European Union', 2022 [EUISS]; ICRC, 'The potential human cost of cyber operations', <https://www.icrc.org/en/document/potential-human-cost-cyber-operations>, accessed 28 December 2022 [The potential human cost of cyber operations].

According to Mr. Panetta, the country was facing the possibility of multiple cyber attacks targeting national critical infrastructure (CNI) accompanied by kinetic use of force, a so-called 'cyber-Pearl Harbor'.[5]

Initiatives from both States and non-governmental entities display that the cyber domain as a military arena is crystalizing. In 2016, NATO recognized cyberspace as a domain of operations[6] and an increasing number of States are fortifying their military cyber capabilities. Deployment of such capabilities in the context of armed conflict is likely to escalate in the future.[7] This was most recently demonstrated as the President of the United States, Joe Biden, signed a $858 billion defence policy bill on the 23rd of December 2022. The bill stipulates an additional $44 million to the U.S. Cyber Command's 'hunt forward' missions. Since 2018, the digital warfighting unit has deployed such missions 38 times to 21 foreign countries to identify malware and other vulnerabilities on 60 networks.[8] In the European Union's Strategic Compass for Security and Defence from 2022 the word 'cyber' is mentioned 82 times[9] and the newly presented 'Policy on Cyber Defence' represents the first comprehensive effort by the union to outline its strategic, policy and operational objectives in cyber defence.[10] Against this backdrop, the International Committee of the Red Cross (ICRC) has initiated an inquiry on implementing the internationally recognized red cross, red crescent and red crystal emblems in cyberspace as a 'digital emblem' to protect vital functioning against harm online.[11] Reports also state that insurance

[5] Bumillier, Shanker, 'Panetta Warns of Dire Threat of Cyberattack on U.S', The New York Times, 11 October 2012 <https://www.nytimes.com/2012/10/12/world/panetta-warns-of-dire-threat-of-cyberattack.html>, accessed 28 December 2022.
[6] NATO, 'Cyber defence', <https://www.nato.int/cps/en/natohq/topics_78170.htm>, accessed 2 January 2023.
[7] EUISS, p. 60.
[8] Matishak, 'Biden signs $858 billion defense policy bill into law, expanding gov't cyber operations', The Record by Recorded Future, 23 December 2022 <https://therecord.media/biden-signs-858-billion-defense-policy-bill-into-law> accessed 28 December 2022.
[9] Council of the European Union, A Strategic Compass for Security and Defence - For a European Union that protects its citizens, values and interests and contributes to international peace and security, 7371/22, 21 March 2022 [Strategic Compass].
[10] European Commission, Joint Communication to the European Parliament and the Council: EU Policy on Cyber Defence, JOIN(2022) 49 final, 10 November 2022.
[11] ICRC, 'Digitalizing the Red Cross, Red Crescent and Red Crystal Emblem – Benefits, risks and possible solution', 3 November 2022.

companies have started reassessing the cyber sphere, enforcing exclusions for State-backed cyber attacks and underscoring that cyber is the risk to watch as it is set to become 'uninsurable'.[12]

To date, the world has not witnessed a declaration of war over an offensive cyber attack, nor have any states publicly qualified a cyber attack as an armed attack.[13] Nonetheless, it is now a fact that cyber operations are being deployed as a means of warfare. There are only a few countries that previously admitted to conducting such operations; the United States, the United Kingdom, and Australia have stated that they used cyber operations in their battle against the Islamic State group.[14] The Russian aggression against Ukraine demonstrates the use of kinetic force at the highest level combined with hybrid means such as cyber attacks, economic and energy coercion and foreign information manipulation and interference.[15] Nation-State actors are launching increasingly sophisticated cyber operations to gain strategic advantages[16] and there are those who purport that the use of cyber offensives in Ukraine marks the beginning of a new era of conflict.[17] The unprecedented volume of cyber attacks in the Russo-Ukrainian war has historical significance. It is comparable to the first recorded conflict at sea in 1210 BC and the use of aerial combat techniques during World War I. These early developments may have seemed small at the time, but they laid the foundation for modern military capabilities that allow for simultaneous action on multiple battlefield fronts.[18]

---

[12] Smith, 'Lloyd's of London defends cyber insurance exclusion for state-backed attacks', Financial Times, 5 September 2022, <https://www.ft.com/content/e865a3d1-5652-41aa-990a-bb5ad57288c6>, accessed 25 December 2022; Smith, 'Cyber attacks set to become 'uninsurable', says Zurich chief', Financial Times, 26 December 2022, <https://www.ft.com/content/63ea94fa-c6fc-449f-b2b8-ea29cc83637d>, accessed 25 December 2022.

[13] Tiirmaa-Klaar, 'Cyber Symposium – Diplomatic considerations for armed attack', Lieber Institute, 27 July 2022, <https://lieber.westpoint.edu/diplomatic-considerations-armed-attack/>, accessed 23 December 2022.

[14] Twenty years on, p. 289.

[15] Strategic Compass, p. 7.

[16] Microsoft, 'Microsoft Digital Defense Report 2022', 4 November 2022, p. 30 [Microsoft Digital Defense Report].

[17] Ibid.

[18] CyberPeace Institute, 'A moment of historical significance' – Russia's invasion of Ukraine underlines the need for cyber peace', 23 June 2022,

The unique nature of cyberspace presents difficulties in terms of legal regulation. While it has been affirmed on several occasions that international law applies to cyberspace, the practical application of these rules is often uncertain and subject to competing views. As a result, there is ongoing debate about the effectiveness of international law in regulating cyber operations.[19] In recent years, the use of cyber operations in armed conflicts and the question of how jus in bello, i.e. international humanitarian law (IHL), applies to these operations have become more prominent.[20] The application of IHL to the use of information and communications technologies has also proven to be one of the more challenging topics for States to agree upon in the United Nations.[21] The ICRC consider it necessary to advance multilateral discussions to provide further clarity on whether common understandings of IHL provide sufficient protection for humans and societies when facing acts of cyber warfare.[22]

The Russo-Ukrainian war has shed light on a range of considerations linked to IHL and its application to wartime cyber operations. The jus in bello regime is in place to protect civilians and civilian objects from the effects of hostilities[23] and it is therefore important to gain clarity on the application of the framework in cyberspace to expose potential gaps that can leave humans and societies vulnerable during an armed conflict.

<https://cyberpeaceinstitute.org/news/a-moment-of-historical-significance-russias-invasion-of-ukraine-underlines-the-need-for-cyber-peace/>, accessed 25 December 2022 [CyberPeace Institute, A moment of historical significance].

[19] Schmitt, 'Introduction to the Research Handbook on International Law and Cyberspace', in Tsagourias, Nikolaos K. and Buchan, Russell (2021), p. 1.

[20] Twenty years on p. 292; EUISS p. 60.

[21] Delerue (2020), p. 5.

[22] ICRC, 'Cyberspace is not a legal vacuum, including during armed conflict', 8 December 2022, <https://www.icrc.org/en/document/cyberspace-not-legal-vacuum-including-during-armed-conflict>, accessed 28 December 2022.

[23] Twenty years on, p. 301.

1.2 Purpose and Research Questions

The purpose of this thesis will be to examine wartime cyber operations in international armed conflicts and the application of jus in bello, i.e. the laws of war. By examining the current legal landscape of IHL through the lens of the cyber elements in the Russo-Ukrainian war, the thesis will provide a critical analysis of lex lata and suggest possible ways forward. The research will take into consideration that the application of international law in cyberspace, and the application of IHL in particular, is heavily dependent on States' political will in the current geopolitical context carrying historical significance.

In order to achieve the purpose of this study, the following questions will be answered:

1) In the light of the developments in the Russo-Ukrainian war, what is the current status of the jus in bello regime and its application to wartime cyber operations?

2) What developments with regards to the application of the jus in bello framework would be advisable going forward?

1.3 Method and Material

The legal dogmatic method will be employed to outline the current legal framework within international law and hence provide answers to the posed research questions.[24] The choice to use the method of legal dogmatics is motivated by the aim of the research to elucidate lex lata, i.e. the law as it is. The method further enables a normative discussion corresponding to lex ferenda, i.e. the law as it should be.[25]

The research material will be evaluated in conformity with Article 38(1) of the Statute of the International Court of Justice (ICJ) – the article is considered

[24] Kleineman, 'Rättsdogmatisk metod', in Nääv and Zamboni (ed.) (2018), p. 21.
[25] Ibid. p. 36.

to have a general applicability and stipulates the sources of international law. Article 38(1) outlines the five main sources of international law: international conventions, international custom, general principles, judicial decisions, and judicial doctrine.[26] The primary international law that regulate the way in which warfare is conducted is the four Geneva Conventions and the Additional Protocols I-II to the Geneva Conventions. There are also general principles and a considerable body of customary law specific to this branch of law.[27]

While international law does apply to cyberspace, as affirmed in the consensus reports presented by the United Nations Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (GGE) in 2013[28] and 2015[29], there are limited case law and international conventions that explicitly regulate the cyber domain. Secondary sources will therefore be essential as an instrument to interpret the jus in bello regime and its application to wartime cyber operations.

The Tallinn Manual 2.0 is the product of the International Groups of Experts at the invitation of the NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE). The Manual addresses IHL in the context of cyber warfare and is to be recognized as a secondary source as described in Article 38(1)(d).[30]

Soft law instruments are also of importance within the field, and can be described as principles, rules, and standards that govern international relations, which do not fall under any of the sources of international law listed

[26] Art. 38(1), Statute of the International Court of Justice.
[27] Saul, Ben and Akande (2020), pp. 17, 21.
[28] UNGA, Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (24 June 2013) UN Doc A/68/98, para. 19 [2013 UNGGE Report].
[29] UNGA, Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (22 July 2015) UN Doc A/70/174, para. 24 [2015 UNGGE Report].
[30] Henriksen (2019), p. 32; Saul, Ben and Akande (2020), p. 26; Art. 38(1)(d), Statute of the International Court of Justice.

in Article 38(1) of the ICJ Statute.[31] The ICRC is recognized as an authority on the interpretation of IHL, and is tasked with promoting the application of the law of armed conflict, addressing violations and contributing to the understanding, dissemination, and development of IHL.[32] The consensus reports from the UN processes consisting of norms and recommendations for State behaviour in cyberspace is also valuable guidance within this scope.

With the objective to present a comprehensive addition to this research field, legal doctrine, such as books and journal articles of practitioners, will be consulted to better understand the interpretation of the aforementioned sources. Additionally, thoroughly evaluated sources such as reports and statements from stakeholders, strategic documents and articles will be referenced.

1.4 State of Research

As connectivity has progressed and the world is facing greater exposure to threats stemming from cyberspace, the research in turn has become more extensive. Areas of uncertainty within international law have emerged in the wake of the Russo-Ukrainian war, not least with regards to the regulation of hybrid warfare and wartime cyber operations. The applied scope by scholars varies from addressing jus ad bellum and jus in bello, to addressing different parts of the expanding range of hybrid warfare. Limited research has been conducted with the aim to analyse IHL and its application to cyberspace through the lens of the Russo-Ukrainian war.

Legal practitioners who specialize in the field of cyberspace frequently publish research attempting to sort out grey areas. The rapidly evolving nature of cyber operations with high frequency of attacks against governmental and non-governmental entities present new angels to scrutinize. National statements and positions from States together with the progression of multilateral and regional discussions on the topic are also closely observed

[31] Saul, Ben and Akande (2020), p. 26.
[32] United Nations Human Rights Office of the High Commissioner, ‘International legal protection of human rights in armed conflict’, 2011, pp. 13-14.

and analysed in order to make out the lines of State practice. Michael N. Schmitt is a recognized practitioner in the field and has authored numerous contributions to the legal doctrine over the years. He is also the Director of the project at CCDCOE administrating the Tallinn Manuals – so far there has been two editions published, and the third Tallinn Manual is underway. Other scholars who made important contributions to the state of play are Nicholas Tsagourias, Russel Buchan, Marco Roscini and François Delerue.

The reports from the ICRC are imperative guidance since the organization is mandated essentially by the Geneva Conventions to promote adherence to the laws governing armed conflict and strives to increase understanding and advancement of IHL.[33] Of particular importance are the organization's series of regional consultations with States on the topic of IHL and cyber operations in armed conflicts. The purpose of the consultations is to encourage discussions among governments at a regional level with the objective to develop broader common understandings.[34] When understanding and developing the jus in bello regime in cyberspace inclusiveness is key – States and stakeholders from all regions must be consulted.

The research explicitly dealing with IHL and wartime cyber operations express that it is undetermined if the legal framework is sufficiently applied in the cyber domain. Academia, governments, and organizations such as the ICRC urges for further discussion to identify potential inadequacies and grey zones. According to ICRC, there are several key issues that remain controversial and are not yet agreed upon by States and other experts, or that require further analysis. These issues include the definition of an 'attack' in the context of cyber operations, the protection of civilian data from harm during cyber operations, and the application of the rules of IHL regarding the

[33] United Nations Human Rights Office of the High Commissioner, 'International legal protection of human rights in armed conflict', 2011, pp.13-14.
[34] ICRC, 'Regional state consultations on international humanitarian law and cyber operations during armed conflicts', 29 June 2022, <https://www.icrc.org/en/document/regional-state-consultations-ihl-cyber-operations>, accessed 26 December 2022.

conduct of hostilities to objects that are used for both civilian and military purposes (commonly referred to as 'dual-use objects').[35]

1.5 Scope and Delimitations

This research is focused on jus in bello and wartime cyber operations. In order to align with the objective, several delimitations have been made. The thesis will focus on core issues in the debate as pointed out by the ICRC[36] and scholars[37]; the principle of distinction, proportionality and precaution; the notion of 'attack'; the issue of 'dual-use' objects, data as an 'object'; and participation.[38] This delimitation is motivated also with regards to occurring cyber hostilities in the Russo-Ukranian war. Other regulations within the jus in bello regime will not be subject for further analysis.

At the outset, the UN Charter regulating the jus ad bellum regime, i.e. the conditions under which States may resort to the use of force, will not be discussed other than mentioning its complementarity to IHL. The complexities stemming from the nature of cyberspace such as attribution and the grey zone of peace and war is necessary to mention as a prerequisite for key aspects of the research. The section on cyber policy in multilateral fora will be limited to the context of the United Nations where a majority of States are represented.

With regards to IHL the main body of law will be of central importance and known complimentary branches of law will not be consulted. Noteworthy for this section is that the term 'cyber operation' has a broader interpretation than the notion '[cyber] attack', which also has a legal connotation. This will be explained more thoroughly in the following chapters.[39]

[35] Twenty years on, p. 311.
[36] Ibid.
[37] E.g. Geiss and Lahmann, 'Working Papers: Protecting Societies - Anchoring A New Protection Dimension In International Law In Times Of Increased Cyber Threats', Geneva Academy, February 2021.
[38] Twenty years on, p. 311.
[39] Schmitt and Vihul (ed.) (2017) p. 376 [Tallinn Manual 2.0].

Since the Russo-Ukrainian war will set the frame for the analysis of the development of IHL the research will be limited to international armed conflicts and exclude considerations of non-international armed conflicts. Even though the Russo-Ukrainian war is characterized by a nexus of attack surfaces, being describes as hybrid warfare[40], this research's sole focus will be the cyber elements.

The thesis aims to provide a comprehensive overview of the main considerations apparent in the current legal landscape. However, the research does not set out to be exhaustive.

1.6 Disposition

This research is divided into six chapters. Following the introductory chapter, *Chapter 2* presents the relevant terminology of cyber warfare.

Chapter 3 provides an overview of the Russo-Ukrainian cyber activities dating back to the Russian annexation of Crimea in 2014 and continuing into the setting of full-scale war. This case will set the scene for the aftercoming chapters where the jus in bello regime will be studied.

Chapter 4 will examine the current status of the application of the jus in bello regime in cyberspace within the presented research scope.

Chapter 5 gives an in-depth analysis of the findings from the previous chapters, including answers to the posed research questions.

Finally, *Chapter 6* will outline the conferred conclusions together with some final remarks.

[40] Pijpers, 'Exploiting cyberspace: International legal challenges and the new tropes, techniques and tactics in the Russo-Ukraine War', Hybrid CoE, 20 October 2022, p. 8.

2 The Terminology of Cyber Warfare

2.1 Cyberspace

The concept of 'cyberspace' was coined by novelist William Gibson to describe the vast amount of data on all interconnected computer networks which form the global digital landscape. Today, the term is commonly used to refer to any large collection of network-accessible computer-based data.[41]

Cyberspace is interconnected by nature. As such, cyber attacks launched against one State can have widespread impacts, either intentionally or incidentally, and can affect other States regardless of their geographical location.[42]

Several States consider cyberspace to be an operational domain similar to land, sea, air, or outer space. However, unlike these physical domains, cyberspace is an entirely man-made ecosystem, which is constantly evolving in a hyper-dynamic manner. Every device that connects to cyberspace alters the domain, together with updates and changes to its physical or logical structures.[43] Throughout this thesis the term 'cyberspace' will be defined as in the Tallinn Manual 2.0: '[t]he environment formed by physical and non-physical components to store, modify, and exchange data using computer networks'.[44]

[41] A Dictionary of Computer Science (7 ed.) (2016), p. 66.
[42] ICRC, 'Cyber Warfare: does International Humanitarian Law apply?', 25 February 2021, <https://www.icrc.org/en/document/cyber-warfare-and-international-humanitarian-law>, accessed 29 December 2022.
[43] The Potential Human Cost of Cyber Operation, pp. 32-33.
[44] Tallinn Manual 2.0, p. 564.

2.2 Wartime Cyber Operations

One of the earliest uses of the term 'cyberwar' can be traced back to the 1993 article 'Cyberwar Is Coming!' by John Arquilla and David Ronfeldt, researchers with the RAND Corporation, which was published in the journal Comparative Strategy.[45]

Cyber warfare is not a legally recognized term, rather it is a concept broadly used to describe a range of harmful actions carried out by States in cyberspace or by groups whose actions can be attributed to States.[46] Notably, the term is frequently used in relation to the armed conflict in Ukraine.[47]

IHL does not provide a definition for cyber operations, cyber warfare, or cyberwar neither do other branches of international law. Definitions used by States can range from a narrow focus corresponding to the use of cyber capabilities to achieve goals in cyberspace, to broader interpretations such as the concept of information warfare, encompassing some elements of what is commonly understood as cyber warfare. The ICRC defines cyber operations during armed conflict as 'operations against a computer system or network, or another connected device, through a data stream, when used as means or method of warfare in the context of an armed conflict'.[48] The Tallinn Manual 2.0 defines 'means of cyber warfare' as 'cyber weapons and their associated cyber systems' and 'methods of cyber warfare' as 'cyber tactics, techniques, and procedures by which hostilities are conducted'.[49]

There are various ways in which cyber operations can be used during conflicts, including espionage; target identification; information operations to demoralize the enemy and weaken their will to fight; interference with or

[45] Britannica Academic, s.v. 'Cyberwar', accessed December 31, 2022, <https://academic-eb-com.ludwig.lub.lu.se/levels/collegiate/article/cyberwar/488833>, accessed 27 December 2022.
[46] Benatar, M. (2014). Cyber Warfare. In A. Carty (Ed.), Oxford Bibliographies in International Law (pp. 1-23). Oxford University Press.
[47] CyberPeace Institute, 'Law & Policy', <https://cyberconflicts.cyberpeaceinstitute.org/law-and-policy>, accessed 28 December 2022.
[48] EUISS, p. 61; Twenty years on, p. 297.
[49] Tallinn Manual 2.0, p. 452.

deception of enemy communication systems to disrupt coordination; and cyber operations to support kinetic operations. For example, an enemy's military radar stations could be disabled to support air strikes. Additionally, cyber operations against critical infrastructure such as electricity grids, healthcare systems, or nuclear facilities can potentially cause significant harm to people, even if they are not directly related to an armed conflict. There have been numerous instances of such operations occurring over the past decade.[50]

As displayed, the term 'cyber operations' includes a broad range of cyber activities. The Tallinn Manual 2.0 defines the term as '[t]he employment of cyber capabilities to achieve objectives in or through cyberspace'.[51] Experts have settled that the term 'cyber attack' has a narrower scope but have not yet agreed on the precise scope of the notion. However, the definition provided in the Tallinn Manual 2.0 suggests that 'a cyber attack is a cyber operation, whether offensive or defensive, that is reasonably expected to cause injury or death to persons or damage or destruction to objects'.[52] Not all cyber operations can qualify as cyber attacks – conventional cyber espionage and jamming of radio communication or television broadcast are not considered to fall within the scope.[53]

In this thesis 'cyber warfare' will have the equivalent meaning of 'wartime cyber operation', understood as 'operations against a computer system or network, or another connected device, through a data stream, when used as means or method of warfare in the context of an armed conflict'. The notion 'cyber attack' will hold a narrower interpretation which will be further examined in relation to the provisions of jus in bello in Chapter 4.

[50] Twenty years on, pp, 290-291.
[51] Tallinn Manual 2.0, p. 564.
[52] Ibid., p. 415.
[53] Ibid., pp. 415-420.

3 Cyber Warfare: The Case of the Russo-Ukrainian War

Since an unprecedented number of cyber operations have been deployed in the context of the Russo-Ukrainian conflict[54], it provides a substantial basis for the aftercoming analysis of the application of the jus in bello regime. This Chapter will give an exposition of the documented cyber operations stemming from the conflict relevant to the objective of this research. The Chapter does not set out to provide an exhaustive exposition.

3.1 Before the Use of Kinetic Force

In 2013, General Valery Gerasimov, the Russian Federation's Chief of the General Staff of the Armed Forces and First Deputy Minister of Defence, wrote an article in which it was stated that the lines between war and peace were becoming blurred. The increasing use of non-military means for achieving political and strategic goals was also highlighted. The author argued that these methods were at times proving to be more effective than traditional means of warfare.[55]

For several years, Russia has demonstrated its cyber capabilities through extensive campaigns, both destructive and disruptive, against Ukraine's CNI and information space. Following Russia's annexation of Crimea in 2014 several cyber attacks which caused significant obstruction have been launched.[56]

In 2015, three energy distribution companies in Western Ukraine were targeted and their systems got compromised. Before the outage, the attackers

[54] CyberPeace Institute, A moment of historical significance.
[55] See Valery Gerasimov, 'The Value of Science Is in the Foresight: New Challenges Demand Rethinking the Forms and Methods of Carrying Out Combat Operations', trans. Robert Coalson, Military Review, January– February 2016, pp. 23-9, originally published in Russian in Military-Industrial Kurier, 27 February 2013.
[56] Raffray, 'Ukraine: Beyond Kinetic', CyberPeace Institute, 4 April 2022, <https://cyberpeaceinstitute.org/news/ukraine-beyond-kinetics/>, accessed 29 December 2022 [Raffray, Ukraine: Beyond Kinetic].

launched a distributed denial-of-service (DDoS) attack[57] against the companies' customer call centres. The attack resulted in power outages for approximately 230,000 consumers for 1-6 hours, as it rendered 16 substations unresponsive to remote commands from operators. The customer call centre telephone lines were also disabled, preventing customers from reporting the outage or seeking information.[58]

In 2016, a cyber attack targeted a substation in Kyiv, affecting the capital and the surrounding area. The malware used in the attack is reportedly only the second known case of malicious code that was specifically designed to disrupt physical systems. The malware holds the ability to automate mass power outages, includes plug-in components which allow for it to adapt and is capable of being launched across multiple systems simultaneously. The attack resulted in a power outage that equated to about one-fifth of Kyiv's power consumption and caused a blackout that lasted over an hour. It is believed that the potential impact could have included shutting off power distribution, cascading failures and more severe damage to equipment.[59]

In 2017, the infamous NotPetya wiper malware, i.e. malware that is designed to corrupt or destroy data on infected systems, was launched against public and private sector entities in Ukraine, causing widespread disruption by wiping hard drives. The software was transmitted via a well-established tax-filing service. The wiper malware spread globally and is said to be one of the most destructive cyber attacks in history. The impact was immense, with around 49,000 systems affected in 65 countries and an estimated costs for companies worldwide exceeding $10 billion. Ukrainian entities suffered significant economic losses as the malware encrypted data irreversibly, infiltrating networks including the National Bank of Ukraine, Kyiv Boryspil International Airport, the capital's metro system, and even causing the

[57] i.e. overwhelming the targeted system with traffic making it unable to function properly.
[58] Raffray, Ukraine: Beyond Kinetic.
[59] Ibid.

radiation monitoring system at the Nuclear Power Plant in Chernobyl to go offline.[60]

Microsoft has reported a number of indicators suggesting that Russia-affiliated threat groups began preparing for conflict as early as March 2021. Actors that previously had targeted Ukraine sporadically started to carry out more operations against organizations inside or aligned with Ukraine. According to Microsoft, the combined result appeared to be aimed at gaining access for strategic intelligence extraction and to enable future destructive attacks.[61]

Data from Ukraine's information security service shows that the number of cyber attacks targeting Ukraine in December 2021 was 135, and in January 2022 the number amounted to 262. This represents a sevenfold increase of the number of attacks from the same period in the year prior. The main targets of these attacks are the Ukrainian government, local authorities, security and defence services and the financial institutions.[62]

With the Russian military forces lined up at their borders, Ukraine's Parliament amended its data protection law on the 17th of February to allow the government to transfer data from on-premises servers to the public cloud. This allowed the government to 'evacuate' important data from the country and store it in European data centres. This move turned out to be strategically accurate, given that a Ukrainian government data centre was targeted early on by Russian missile strikes. The storage of digital operations and data in the public cloud has proven useful in limiting the operational impact throughout the course of war.[63]

[60] Raffray, Ukraine: Beyond Kinetic.
[61] Microsoft, 'Special report: Ukraine - An overview of Russia's cyberattack activity in Ukraine', 27 April 2022, p. 5.
[62] Antoniuk and Peterson, 'The invasion of Ukraine started online long before troops marched on Kyiv', The Record by The Recorded Future, 28 February 2022, <https://therecord.media/the-war-for-ukraine-started-online-long-before-troops-marched-on-kyiv/>, accessed 28 December 2022.
[63] Microsoft, 'Defending Ukraine: Early Lessons from the Cyber War', 22 June 2022, p. 5.

3.2 Entering a Full-Scale War

On the 23rd of February 2022, one day before the military invasion, the first attack was launched – a wiper software known as 'Foxblade'. According to Microsoft, operators connected to Russia's military intelligence service (GRU) launched the attack against hundreds of systems within the Ukrainian government affecting sectors such as IT, energy, agriculture and finance. This malware was developed and deployed by the same group that was responsible for the creation and launch of the NotPetya attack in 2017.[64]

The Foxblade operation was the beginning of a range of similar attacks. On 24th of February, the day marking the initiation of Russia's full-scale invasion of Ukraine, a cyber attack disabled modems communicating with Viasat Inc's KA-SAT satellite network. This attack, which was later documented as a wiper attack using the 'AcidRain' malware, resulted in disruptions in Ukraine and had vast spill-over effects in Europe. The malware caused the Internet access to go offline for more than two weeks for some users and affected nearly 9,000 subscribers of a satellite internet service provider in France, around a third of 40,000 subscribers of another satellite internet service provider in Europe (Germany, France, Hungary, Greece, Italy, Poland), and a major German energy company that lost remote monitoring access to over 5,800 wind turbines. The attack has been publicly attributed to the Russian military intelligence service by the EU and additional States.[65] In response to the sabotage of the Viasat satellite system, Elon Musk offered Ukraine his Starlink service as an alternative to prevent future internet disruptions.[66]

[64] Microsoft, 'Special report: Ukraine - An overview of Russia's cyberattack activity in Ukraine', 27 April 2022, p. 2.
[65] CyberPeace Institute, 'Case Study Viasat', June 2022, <https://cyberconflicts.cyberpeaceinstitute.org/law-and-policy/cases/viasat>, accessed 29 December 2022.
[66] Pijpers, 'Exploiting cyberspace: International legal challenges and the new tropes, techniques and tactics in the Russo-Ukraine War', Hybrid CoE, 20 October 2022, p. 5, pp. 8-10.

Microsoft's Threat Intelligence Center (MSTIC) has detected multiple attempts to use eight different malware programs, some of which are wipers and others which are destructive malware, against 48 Ukrainian agencies and businesses since the war began. These attacks have sought to infiltrate network domains by initially compromising hundreds of computers and then spreading malware to thousands of others.[67] According to Microsoft, threat groups believed to have connections to the Russian military intelligence service have developed and deployed destructive wiper malware or similar tools against targeted Ukrainian networks at a rate of two to three incidents per week since the invasion. From the 23rd of February to the 8th of April, there were approximately 40 separate attacks that permanently destroyed files on hundreds of systems across various organizations in Ukraine.[68]

After the initial, mostly kinetic, phase of the war in the days following the 24th of February, cyber operations became more closely integrated with traditional military warfare starting in mid-March.[69] It has also been suggested that the Russian military in some instances coordinated cyber attacks with conventional operations targeting the same objectives. Similar to the simultaneous use of naval and ground forces in previous armed conflicts, it cannot be ruled out that cyber attacks have been coordinated with kinetic use of force from both the Russian and Ukrainian side.[70]

The virtual battlespace has seen the entry of numerous non-State actors, such as hacker groups and commercial enterprises, who align themselves with one of the conflicting States without necessarily being belligerent entities. This has added new complexities and tactics to the already challenging issue of regulating activity in cyberspace, leading to increased legal uncertainty for States.[71] In February, Ukraine established an IT Army with inspiration drawn

[67] Microsoft, 'Defending Ukraine: Early Lessons from the Cyber War', 22 June 2022, p. 7.
[68] Microsoft, 'Special report: Ukraine - An overview of Russia's cyberattack activity in Ukraine', 27 April 2022, p. 3.
[69] Pijpers, 'Exploiting cyberspace: International legal challenges and the new tropes, techniques and tactics in the Russo-Ukraine War', Hybrid CoE, 20 October 2022 p. 5, pp. 8-10.
[70] Microsoft, 'Defending Ukraine: Early Lessons from the Cyber War', 22 June 2022, p. 7.
[71] Pijpers, 'Exploiting cyberspace: International legal challenges and the new tropes, techniques and tactics in the Russo-Ukraine War', Hybrid CoE, 20 October 2022, p. 5.

from Estonia's Cyber Defence League. The Ukrainian IT Army includes Ukrainian and international civilians, private companies, and Ukrainian defence and military personnel. This group is organized through a Telegram channel, where targets are listed for volunteers to attack.[72]

In addition to the attacks by the Ukrainian IT Army, established hacktivist groups, such as Anonymous, Ghostsec, The West, Belarusian Cyber Partisans and RaidForum2, began supporting Ukraine by conducting attacks. Meanwhile, some groups, including members of the Conti ransomware gang, sided with Russia. In the beginning of the war, Anonymous and its affiliates were highly active, temporarily disabling thousands of Russian and Belarusian websites, leaking hundreds of gigabytes of stolen data, hacking Russian TV channels to play pro-Ukrainian content and even offering to pay in Bitcoin for surrendered Russian tanks.[73] During the Russian invasion of Ukraine, some technology companies were seen to be supporting Ukraine in the cyber conflict. The most prominent example being Microsoft, which provided assistance to Ukrainian cybersecurity officials to counter the FoxBlade malware and also provided intelligence and awareness reports on Russian cyber operations. The long-term implications of such alignments with one side of the conflict are not yet clear. Nevertheless, these circumstances have sparked debates about the role and responsibilities of private companies in future conflicts.[74]

The conflict has seen a number of cyber attacks on CNI, such as communication services and electric power stations, in violation of IHL.[75] Microsoft reported on the 28th of February that there is particular concern about cyber attacks on Ukrainian civilian digital targets, including the financial sector, agriculture sector, emergency response services, humanitarian aid efforts, and energy sector organizations and enterprises. The

[72] ENISA, 'ENISA Threat Landscape 2022', October 2022, pp.28-29 [ENISA Threat Landscape]; Microsoft Digital Defense Report, p. 58.
[73] Microsoft Digital Defense Report, p. 28.
[74] ENISA Threat Landscape, p. 29.
[75] Raffray, 'Ukraine: 100 days of war in cyberspace', CyberPeace Institute, 2 June 2022, <https://cyberpeaceinstitute.org/news/ukraine-100-days-of-war-in-cyberspace/>, accessed 23 December 2022.

company stated that '[t]hese attacks on civilian targets raise serious concerns under the Geneva Convention'.[76] Cyber attacks against Ukrainian civilian targets have taken many forms, including wiper malware attacks, SMS spam campaigns, DDoS attacks and website defacements. Many of the affected sectors are considered essential infrastructure, vital to civilians.[77]

Since before the invasion, there have been reports of DDoS attacks on financial institutions in Ukraine. These attacks have caused issues with online payments, banking apps, and, in a few cases, access to ATMs. Additionally, one of the attacks was accompanied by fraudulent SMS messages sent to Ukrainian phones. The impact of these attacks is especially concerning during the invasion, as people are trying to access their financial assets to purchase necessities and protect themselves and their communities from harm.[78]

On the day of the invasion, the Kyiv Post experienced DDoS attacks that disabled their systems. As a result, the newspaper had to use alternative methods, such as posting shortened versions of their stories on Facebook, Twitter, and LinkedIn, to continue publishing news. During an armed conflict, access to news and information is essential for the public. It allows for the dissemination of official information from national or local authorities and helps civilians to make informed decisions about their safety, whether to flee or stay in an area and where to access humanitarian aid.[79]

On the 9th of March, a cyber attack on Ukrainian telecommunications company Triolan brought its network down across several regions in Ukraine for 12 hours. Cyber attacks on telecommunications and internet service providers have a direct impact on civilians, who rely on these services to contact loved ones, seek medical support, access online services, coordinate rescue efforts, and much more.[80] During the same month, Ukraine's largest

[76] Smith,'Digital technology and the war in Ukraine', Microsoft, 28 February 2022, <https://blogs.microsoft.com/on-the-issues/2022/02/28/ukraine-russia-digital-war-cyberattacks/?preview_id=65075>, accessed 25 December 2022.
[77] Raffray, Ukraine: Beyond Kinetic.
[78] Ibid.
[79] Ibid
[80] Ibid.

fixed line telecommunications provider, Ukrtelecom, experienced a severe cyber attack which is said to have reduced services to 13% of its pre-war levels.[81]

Russia is not only trying to seize Ukrainian territory but is also attempting to assert control over the virtual sovereignty of occupied Eastern provinces in Ukraine. By changing the country code from .ua to .ru, internet traffic can be redirected to follow different routes and gateway protocols, potentially resulting in traffic being subject to Russian digital control and jurisdiction.[82]

Given the history of Russian cyber operations against Ukraine, cyber and legal experts expected to see more destructive and visible cyber offensives following Russia's military aggression against Ukraine in February. Experts have been trying to explain why there have not yet been more severe cyber attacks in Ukraine, and why they predict that such attacks are still to come.[83] However, not everyone agrees. Christian-Marc Lifländer, Head of the Cyber and Hybrid Policy Section at the Emerging Security Challenges Division at NATO, argues that suggestions that Russia's cyber operations against Ukraine has been minor are a 'dangerous misdiagnosis'.[84]

The US has been assisting Ukraine in strengthening its cyber defences for years, following the 2015 attack on its power grid. Experts warn that Russia may still launch a devastating online attack on Ukrainian infrastructure, which has been a concern among officials for some time. However, years of preparation and the early efforts to bolster Ukrainian networks may be the reason behind the country's ability withstand attacks so far.[85]

---

[81] Microsoft, 'Special report: Ukraine - An overview of Russia's cyberattack activity in Ukraine', 27 April 2022, p. 14.
[82] Pijpers, 'Exploiting cyberspace: International legal challenges and the new tropes, techniques and tactics in the Russo-Ukraine War', Hybrid CoE, 20 October 2022, p. 5, pp. 8-10.
[83] Raffray, Ukraine: Beyond Kinetic.
[84] CyberPeace Institute, 'Shields up': Top insights from cyber experts on the threats of 2022', <https://cyberpeaceinstitute.org/news/ukraine-top-insights-from-cyber-experts-threats-2022/>, accessed 27 December 2022.
[85] Srivastava, Murgia and Murphy, 'The secret US mission to bolster Ukraine's cyber defences ahead of Russia's invasion', The Financial Times, 9 March 2022,

Despite the Russo-Ukrainian not escalating to the level of a 'cyber Pearl Harbor' as feared, the use of cyber operations in conjunction with other forms of influence such as diplomacy, information, law and economics serves as a prime example of modern hybrid warfare.[86] The war demonstrated that the use of cyber means is blurring the lines between State and non-State actors, the virtual and physical world and the notion of war and peace. This presents a challenge for the application of international law, which is based on the concepts of State, territory, and the distinction between war and peace.[87]

<https://www.ft.com/content/1fb2f592-4806-42fd-a6d5-735578651471>, accessed 28 December 2022.

[86] Pijpers, 'Exploiting cyberspace: International legal challenges and the new tropes, techniques and tactics in the Russo-Ukraine War', Hybrid CoE, 20 October 2022, p 8.

[87] Ibid., p. 15.

4 State of Play: Jus in Bello and Its Application to Wartime Cyber Operations

The question of whether, and how, international humanitarian law applies to cyber operations during an armed conflict has been the subject of discussion for more than two decades.[88] Overlapping categories of change, such as novel technology, new and changing domains of conflict, evolving roles of actors besides States, and shifting geopolitical realities, will impact the way in which IHL is developed, interpreted, enforced, and applied in future conflicts. As the context in which it is applied changes, international law must adapt and evolve. This can happen in three ways: by the creation of new treaty law, the development of new customary international law norms, and through the interpretation of existing treaty or customary law. This is necessary to ensure that the normative framework of international law remains relevant and effective.[89]

This Chapter will examine the jus ad bello regime and the current status of its application to key issues that are yet to be further analysed and discussed amongst States, scholars and other stakeholders. At the outset the main legal instruments of the jus in bello regime will be presented, to be followed by an overview of the dynamics in the multilateral context where States and other stakeholders gather to discuss cyber issues. The key subtopics are; the principle of distinction, proportionality and precaution; the notion of 'attack'; the issue of 'dual-use' objects, data as an 'object'; and participation. In closing, this Chapter will touch upon the complexities of attribution, a prerequisite for the application of several provisions in the IHL framework.

[88] Twenty years on, p. 1, p. 301.
[89] Waxman, 'Introduction: The Future Law of Armed Conflict', in Matthew C. Waxman, and Thomas W. Oakley (eds) (2022), p. 2.

4.1 The Jus in Bello Regime

International humanitarian law is a body of rules that aim to minimize the impact of armed conflict on individuals, including civilians, non-combatants, and those who are actively participating in the conflict. To achieve this goal, IHL addresses two main areas: the protection of individuals and objects and the limitations on the means and methods of warfare. This law is based on both treaties and customary international law and is codified in a series of conventions and protocols. The following instruments are considered the core regulations of international humanitarian law[90]:

- The Hague Regulations (1899 and 1907) respecting the Laws and Customs of War on Land;
- The Geneva Convention (I) for the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field;
- The Geneva Convention (II) for the Amelioration of the Condition of Wounded, Sick and Shipwrecked Members of Armed Forces at Sea;
- The Geneva Convention (III) relative to the Treatment of Prisoners of War;
- The Geneva Convention (IV) relative to the Protection of Civilian Persons in Time of War;
- The Additional Protocol to the Geneva Conventions and relating to the Protection of Victims of International Armed Conflicts (Protocol I); and
- The Additional Protocol to the Geneva Conventions and relating to the Protection of Victims of Non-International Armed Conflicts (Protocol II). [91]

The Hague Regulations are generally recognized as corresponding to customary international law and are binding on all States regardless of formal ratification. The Geneva Conventions have attained universal ratification, and many of the provisions are considered to be part of customary international

[90] United Nations Human Rights Office of the High Commissioner, 'International legal protection of human rights in armed conflict', 2011, pp. 12-13.
[91] Ibid.

law. In addition, other international treaties relating to the production, use, and stockpiling of certain weapons can also be considered part of the jus in bello framework if they regulate the conduct of armed hostilities and place limits on the use of specific weapons.[92] However, these regulations relating to certain weapons fall outside the scope of this thesis.

4.2 Cyber Policy in Multilateral Fora

The process of creating international law is typically a matter of State diplomacy and practice. In addition to traditional subjects of international law, a growing number of non-State actors, such as non-governmental organizations and multinational enterprises, are influencing and participating in international relations and to some extent in the process of establishing international legal norms. This is also the case regarding norms related to cyber affairs.[93]

Discussions on developments in the field of information and telecommunications in the context of international security started when the Russian Federation introduced the first resolution on the subject at the UN General Assembly in 1998. It has been reported that these discussions have become more intense in recent years. Since 2004, governmental experts have convened in six consecutive Groups of Governmental Experts (GGE) to address issues related to information and telecommunications in the context of international security. The GGE reports contain recommendations on confidence-building measures to preserve the security and stability of cyberspace, as well as measures of international cooperation and assistance that States can implement, and most importantly, norms of responsible state behaviour in cyberspace.[94]

[92] United Nations Human Rights Office of the High Commissioner, 'International legal protection of human rights in armed conflict', 2011, pp. 12-13.
[93] Delerue (2020), p. 22.
[94] Twenty years on, p. 292.; Douzet F, Géry A and Delerue F, 'Building Cyber Peace While Preparing for Cyber War' in Scott J Shackelford, Frederick Douzet and Christopher Ankersen (eds), 'Cyber Peace: Charting a Path Toward a Sustainable, Stable, and Secure Cyberspace', Cambridge University Press, 2022 [Building Cyber Peace While Preparing for Cyber War].

In 2018, the UN General Assembly adopted a resolution on the establishment of the Open-ended Working Group on security of and in the use of information and communications technologies (OEWG), which operated concurrently with the GGEs. Both groups were given the mandate, among other tasks, to examine 'how international law applies to the use of information and communications technologies by States'.[95]

In recent years, States and international organizations have become more aware of the risks and challenges posed by cyber security and the need to address these issues with a sense of urgency.[96] However, the UN negotiations on the topic have proven to be a source of conflict. Despite progress made by previous GGEs, particularly in 2013[97] and 2015[98], affirming the application of international law to cyberspace, fundamental disagreements continue to exist due to conflicting views and political interests.[99]

In June 2017, the fifth GGE was unable to reach consensus on its final report. Some States contested the applicability of certain branches of international law to cyberspace, including the law of armed conflict, the right to self-defence and the law regulating countermeasures.[100] However, the GGE report from 2021[101] made a historic reference to the application of IHL, stating that IHL only applies in situations of armed conflict. Some experts have interpreted this as indicating a consensus among participating States on the applicability of IHL to cyber operations.[102] While some states have expressed opposition to the application of IHL with the argument that it potentially could legitimize military cyber operations in the cyber domain, the ICRC and other scholars stand firm behind its application. The ICRC states that asserting that IHL applies to cyber operations during armed conflict is not an

[95] Twenty years on, p. 292.
[96] Harrison (2012), p. 2.
[97] 2013 UNGGE Report.
[98] 2015 UNGGE Report.
[99] Building Cyber Peace While Preparing for Cyber War; Delerue (2020), pp. 14-17.
[100] Delerue (2020), p. 5.
[101] UNGA, Report of the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security (14 July 2021) UN Doc A/76/135, para. 70(f) [2021 UNGGE Report].
[102] EUISS, pp. 62-64.

endorsement of militarizing cyberspace and should not be interpreted as legitimizing cyber warfare. The ICRC underscores that the use of force by States, whether cyber or kinetic in nature, is always governed by the UN Charter and customary international law, particularly the prohibition of the use of force. The legal frameworks are in that way complementary to one another. In addition, international disputes must be resolved peacefully. This principle applies in cyberspace as in all other domains. The rules of IHL do not supersede the fundamental principles of the UN Charter, but if a conflict occurs, IHL provides protections for non-combatants and those who are no longer participating in hostilities (such as wounded soldiers or prisoners of war) and restricts the methods and means that parties to the conflict can use in warfare.[103]

This was reflected in the 2021 GGE report[104] where it was emphasized that invoking IHL principles does not necessarily legitimize or encourage conflict. The ICRC reiterates that IHL, in fact, imposes limits on the militarization of cyberspace by prohibiting the development of military cyber capabilities that would violate IHL.[105] In addition, all States have recognized that ICT activity against critical infrastructure has become 'increasingly serious' and that the human cost could be substantial. The ICRC agrees that cyber operations that disrupt medical facilities, cut energy, interrupt or poison water supplies pose a significant risk to civilian populations. Such operations can have serious consequences for the safety and well-being of civilians.[106]

The 2015 GGE report[107] also mentioned 'established international legal principles, including, where applicable, the principles of humanity, necessity, proportionality, and distinction'. While the report does not mention IHL explicitly, it has been noted that these are 'the core principles of IHL'. This was later recalled in the 2021 GGE report. In support of this conclusion, an

[103] Twenty years on, p. 306.
[104] 2021 UNGGE Report, para. 70(f).
[105] EUISS, p. 64.; Twenty years on, pp. 298-300.
[106] ICRC, Briefing by the International Committee of the Red Cross, Dr Helen Durham, Director of International Law and Policy – United Nations Security Council, 20 December 2021, <https://www.icrc.org/en/document/briefing-helen-durham-international-law-policy-united-nations-security-council-cyber-operations>, accessed 28 December 2022.
[107] 2015 UNGGE Report.

increasing number of States and international organizations have publicly stated that IHL applies to cyber operations during armed conflict. This includes the EU and NATO. In addition, the Paris Call for Trust and Security in Cyberspace, which has been endorsed by 78 States as of April 2020, has reaffirmed the applicability of IHL to cyber operations during armed conflict.[108]

In recent years, Microsoft has been working on and promoting two proposals related to international law: the Digital Geneva Convention and the creation of an international mechanism for attributing cyber operations.[109] At State level, Russia has generally been advocating for the adoption of a new treaty, while the United States and European countries have strongly opposed this idea.[110]

In October 2020, France and Egypt, supported by 40 States, proposed a solution to operationalise what States have agreed upon; the creation of a UN Programme of Action (PoA) for advancing responsible State behaviour in cyberspace.[111] During the UN General Assembly 2022 the resolution for the initiative was adopted.[112] The main objective of the PoA is to move beyond discussion and into the implementation phase of the 11 voluntary non-binding norms that were agreed upon in 2015 and re-endorsed in 2021. These norms aim to advance cyber security by addressing a range of issues, including the protection of CNI, State cooperation against cyber attacks, efforts to protect the integrity of supply chains, measures against malicious cyber activities and cyber capacity building.[113]

The Member States have made progress in the past, but practitioners argue that achieving cyber peace is a difficult task due to States often prioritising

[108] Twenty years on, p. 299.
[109] Delerue (2020) p. 24.
[110] Ibid., p. 27.
[111] Building Cyber Peace While Preparing for Cyber War.
[112] UNGA, 'Developments in the field of information and telecommunications in the context of international security, (13 October 2022), A/C.1/77/L.73.
[113] Weber, 'How to Strengthen the Program of Action for Advancing Responsible State Behavior in Cyberspace', 10 February 2022, <https://www.justsecurity.org/80137/how-to-strengthen-the-programme-of-action-for-advancing-responsible-state-behavior-in-cyberspace/>, accessed 28 December 2022.

maintaining their ability to carry out cyber attacks over promoting peace. The dynamics of cyber peacebuilding at the UN reflect fundamental disagreements on how to ensure the security and stability of cyberspace.[114]

4.3 The Application of the Jus in Bello Regime to Wartime Cyber Operations

The guidance provided from the UN processes are that 'IHL only applies in situations of armed conflict'; that the group 'recalls the established international legal principles including, where applicable, the principles of humanity, necessity, proportionality'; and that '[t]he Group recognised the need for further study on how and when these principles apply to the use of ICTs by States and underscored that recalling these principles by no means legitimizes or encourages conflict'.[115] There is widespread consensus among practitioners that IHL applies to cyber operations during armed conflicts. The drafting of the Tallinn Manuals, further illustrates this agreement among experts.[116]

It is also worth recalling that the ICJ has stated that IHL 'applies to all forms of warfare and to all kinds of weapons, those of the past, those of the present and those of the future', in spite of the 'qualitative as well as quantitative difference' in relation to traditional weapons.[117]

4.3.1 Defining 'international armed conflict'

The International Group of Experts confirms that the law of armed conflict applies to cyber operations undertaken in the context of an armed conflict.[118] The term 'armed conflict' is not defined in the Geneva Conventions or their

[114] Building Cyber Peace While Preparing for Cyber War.
[115] EUISS, p. 62-64.
[116] Twenty years on, pp. 290-291; ICRC, 'Cyber Warfare: does International Humanitarian Law apply?', 25 February 2021, < https://www.icrc.org/en/document/cyber-warfare-and-international-humanitarian-law>, accessed 28 December 2022.
[117] *Legality of the Threat or Use of Nuclear Weapons*, Advisory Opinion, 8 July 1996, ICJ Reports 1996 ('*Nuclear Weapons*'), para. 86.
[118] Tallinn Manual 2.0, p. 375.

Additional Protocols,[119] but the Experts have agreed that armed conflict refers to a situation involving hostilities, including those conducted using cyber means. To exemplify, during the 2008 Russo-Georgian war, Georgia experienced several cyber attacks that were believed to have been conducted or sponsored by Russia. The armed conflict between the two countries activated the laws of war, which would therefore apply to the cyber operations that took place during the conflict, even if the cyber operations themselves did not amount to the threshold of an 'armed conflict'.[120]

The criteria for determining the existence of an international armed conflict are generally accepted and are based on customary international law. These criteria are found in Common Article 2 of the 1949 Geneva Conventions, which states:

> *The present Convention shall apply to all cases of declared war or of any other armed conflict which may arise between two or more of the High Contracting Parties even if the state of war is not recognised by one of them. The Convention shall also apply to all cases of partial or total occupation of the territory of a High Contracting Party, even if the said occupation meets with no armed resistance.*[121]

An armed conflict as defined by this rule must involve both an 'international' element and the use of 'armed' force.[122] The Experts have defined 'armed' force as 'hostilities presuppose the collective application of means and methods of warfare'. The hostilities that are part of the conflict may include a combination of kinetic and cyber operations, or they may consist solely of cyber operations. So long as the armed and international criteria have been met, an international armed conflict exists.[123]

It is worth noting that there has never been a cyber armed conflict of either an international or non-international character that has been recognized as

[119] Harrison (2012), p. 119.
[120] Delerue (2020), p. 42.
[121] Geneva Conventions I–IV, Art. 2.
[122] Tallinn Manual 2.0, p. 380.
[123] Ibid., pp. 382-384.

such to date.[124] Experts, including the ICRC, generally agree that cyber operations independently attain the ability to amount to the threshold of an international armed conflict under IHL. In a rare expression of a State's position on the topic, France stated that '[c]yberoperations that constitute hostilities between two or more States may characterise the existence of international armed conflict'. It remains unsettled where this threshold lies.[125]

4.3.2 The notion of 'attack'

Article 49(1) of Additional Protocol I define an 'attack' as 'acts of violence against the adversary, whether in offence or in defense'. Essentially, an 'attack' refers to any military operation that involves the use of 'violence'. It is generally accepted that a cyber operation that causes or is likely to cause loss of life, injury to persons, or more than minimal material damage to property would qualify as an 'attack' and the principle of distinction would be applicable. The Tallinn Manual 2.0 defines 'attack' as '[…] a cyber operation, whether offensive or defensive, that is reasonably expected to cause injury or death to persons or damage or destruction to objects'.[126]

The concept of an 'attack' serves as a foundation for various limitations and prohibitions in the laws of armed conflict. For example, civilians and civilian objects may not be subject to an 'attack'. According to the widely accepted definition, it is the use of 'violence' that distinguishes an attack from other military operations. 'Acts of violence' should not be narrowly interpreted as referring only to activities that involve the release of kinetic force. However, operations that do not involve the use of violence, such as psychological cyber operations and cyber espionage, do not qualify as attacks.[127]

The essence of the concept of an attack lies in the effects it causes. In other words, it is the consequences of an operation, rather than its nature, that generally determine whether it is considered an attack. 'Violence' should be understood in terms of the violent consequences it produces, rather than being

[124] Delerue (2020). p. 43.
[125] Twenty years on, p. 304.
[126] Tallinn Manual 2.0, p. 415.
[127] Ibid.

limited to violent acts. For example, a cyber operation that alters the operation of a SCADA[128] system controlling an electrical grid, thus causing a fire would be considered an attack, because it has destructive consequences. According to the International Group of Experts, the text of several articles of Additional Protocol I, along with the commentary provided by the ICRC, support the conclusion that the consequences of an operation, rather than its nature, generally determine whether it is considered an 'attack'.[129]

The International Group of Experts agree that the concept of an attack should be extended to include serious illness and severe mental suffering that are equivalent to physical injury, given the humanitarian purposes underlying the laws of armed conflict. It is worth noting that Article 51(2) of Additional Protocol I prohibit 'acts or threats of violence the primary purpose of which is to spread terror among the civilian population', and that terror is a psychological condition that can cause mental suffering. Therefore, the Experts found it reasonable to include such suffering within the scope of the rule in the Manual by analogy.[130]

However, during the discussion among the International Group of Experts, there was disagreement about whether interference through cyber means with the functionality of an object constitutes damage or destruction within the scope of the Manual rule. While some Experts believed that it does not, the majority of them believed that interference with functionality counts as damage if physical components need to be replaced in order to restore functionality. As an example, consider a cyber operation that targets the computer-based control system of an electrical distribution grid and causes it to stop functioning. In order to restore the grid, either the control system or vital components of it must be replaced. The majority of the Experts would consider this cyber operation to be an 'attack'.[131]

[128] i.e. Supervisory control and data acquisition (SCADA).
[129] Tallinn Manual 2.0, p. 415-416.
[130] Ibid., p. 416.
[131] Ibid., p. 417.

The International Group of Experts considered the characterization of a cyber operation that does not cause the type of damage described above, but that has significant negative consequences, such as disrupting all email communication in a country (as opposed to damaging the system used for transmission). The majority of the Experts believed that while it might be logical to consider such an operation an 'attack', the current laws of armed conflict do not allow for such interpretations.[132]

Not all cyber operations qualify as attacks, and there are some clear-cut cases. For example, it is clear that the term 'attack' does not encompass cyber espionage in and of itself, unless the means or method used to conduct the espionage result in consequences that qualify as an 'attack'. The Experts noted that there is general agreement that cyber operations that merely cause inconvenience or irritation to the civilian population do not qualify as attacks, although they cautioned that the scope of the term 'inconvenience' is uncertain.[133]

Cyber operations can be a key part of an operation that qualifies as an 'attack'. For instance, a cyber operation might be used to disable the defences of a target that is being attacked using kinetic force, such as by disabling the target's ability to use electronic countermeasures that prevent a weapon from locking onto it. In this case, the cyber operation is just one aspect of an operation that qualifies as an 'attack', similar to how laser designation enables the use of laser-guided bombs. The laws of armed conflict on attacks apply fully to such cyber operations.[134]

The ICRC believes that there is a need for further examination of the rules that provide general protection to civilians and civilian objects from the impact of cyber operations that do not constitute attacks. This is especially important if it is believed that only operations that cause physical damage are considered attacks, as this would leave a large category of cyber operations subject to a limited set of rules under IHL. Such a conclusion could raise

[132] Tallinn Manual 2.0, p. 418.
[133] Ibid.
[134] Tallinn Manual 2.0, p. 419.

serious concerns about the protection of civilians and civilian infrastructure.[135] For example, if those who interpret the concept of 'attack' narrowly accept that a cyber operation that simply disables objects is a 'military operation' that must therefore be directed only at military targets, it would at least provide a certain level of protection. Operations other than attacks are not completely unregulated, however, the legal regime governing military operations is less comprehensive, precise, and strict compared to the legal regime governing operations that qualify as attacks under IHL. To address this protection gap to some extent, Michael N. Schmitt has proposed that States adopt an adapted proportionality assessment as policy for cyber operations that do not constitute attacks.[136]

4.3.3 Participation in an 'armed conflict'

According to customary international law, there is no prohibition on individuals participating in an armed conflict, whether it is international or non-international. It is worth noting that Article 43(2) of Additional Protocol I states that 'members of the armed forces of a Party to a conflict (other than medical personnel and chaplains covered by Article 33 of Geneva Convention III) are combatants, that is to say they have the right to participate directly in hostilities.' This provision, which applies in international armed conflicts, confirms that combatants are immune for their actions during hostilities. It does not prohibit others from participating in these hostilities.[137]

A civilian who directly participates in hostilities loses certain protections attendant to civilian status for such time as he or she so participates.[138] This rule is derived from Article 51(3) of Additional Protocol I and Article 13(3) of Additional Protocol II, and is recognized as customary international law.[139] The Tallinn Manual 2.0 further states that '[c]ivilians are not prohibited from

[135] Twenty years on, p. 323.
[136] Ibid., p. 326.
[137] Tallinn Manual 2.0, p. 401.
[138] Ibid.
[139] Tallinn Manual 2.0, p. 428.

directly participating in cyber operations amounting to hostilities, but forfeit their protection from attacks for such time as they so participate'.[140]

Most members of the International Group of Experts agreed that civilians maintain their civilian status even if they directly engage in cyber hostilities. For example, in an international armed conflict, civilian hackers who independently carry out offensive cyber operations against enemy forces would not be afforded combatant immunity for their actions and could be legally targeted, unless they qualify as members of a 'levée en masse', i.e. inhabitants of unoccupied territory 'who on the approach of the enemy spontaneously take up arms to resist invading forces, without having time to form themselves into regular armed units'. A minority of the group held the position that these individuals do not qualify as either civilians or combatants.[141]

The International Group of Experts largely agreed on cumulative criteria for determining when an act constitutes direct participation in hostilities, as outlined in the ICRC Interpretive Guidance.[142] These criteria are:

1. The act (or a series of closely related acts) must have the intended or actual effect of negatively impacting the adversary's military operations or capabilities, or causing death, physical harm, or damage to protected persons or objects. This threshold of harm does not require actual physical damage or harm to individuals, and actions that do not qualify as a cyber attack can still meet this criterion as long as they negatively affect the enemy militarily. An example of an operation that meets this criterion is a cyber operation that disrupts the enemy's command and control network. Some members of the International Group of Experts also argued that actions that strengthen one's own military capacity are included, as they necessarily weaken

[140] Tallinn Manual 2.0, p. 413.
[141] Ibid.
[142] Tallinn Manual 2.0, pp. 429-430.

an adversary's relative position. An example of this would be maintaining passive cyber defences for military cyber assets.

2. There must be a direct causal link between the act in question and the harm intended or inflicted (causal link).

3. The acts must be directly related to the hostilities (belligerent nexus). In the example given, the fact that the system is used to direct enemy military operations fulfils this condition. While the majority of the Experts agreed on these criteria, there were differences of opinion on their precise application to specific actions.[143]

If the criteria are fulfilled, the civilian no longer holds protection from attacks as provided by IHL.[144]

4.3.4 The principle of distinction

The ICRC has emphasized on 'the obligation of all parties to conflicts to respect the rules of international humanitarian law if they resort to means and methods of cyberwarfare, including the principles of distinction, proportionality and precaution'.[145]

The St. Petersburg Declaration of 1868 establishes that the only acceptable objective of warfare is to weaken the enemy's military forces.[146] This principle serves as the foundation for the principle of distinction, which is recognized by the ICJ as one of the two 'cardinal' principles of the law of armed conflict. The Court states that 'States must never make civilians the object of attack and must consequently never use weapons that are incapable of distinguishing between civilian and military targets'.[147] The Court considers these principles to be fundamental, one of the 'intransgressible

[143] Tallinn Manual 2.0, p. 429-430.
[144] Tallinn Manual 2.0, p. 428.
[145] Roscini (2014), p. 166.
[146] Preamble to the 1868 Saint Petersburg Declaration; Tallinn Manual 2.0, p. 420.
[147] *Nuclear Weapons advisory opinion*, para. 78.

principles of international customary law'.[148] Intentionally attacking civilians is considered a war crime.[149]

Article 48 of Additional Protocol I codifies the rule. Parties to a conflict must distinguish between civilian objects and military objectives in order to safeguard the civilian population and civilian objects. The Parties must always differentiate between the civilian population and combatants, and between civilian objects and military objectives. All operations must be directed solely at military objectives.[150]

However, certain actions that target the civilian population are allowed under the law. For example, psychological operations like dropping leaflets or making propaganda broadcasts are not prohibited, even if civilians are the intended audience. Similarly, sending emails to the enemy population urging surrender during cyber warfare would also be in compliance with IHL. It is only when a cyber operation against civilians or civilian objects (or other protected persons or objects) is considered an 'attack' that it is prohibited by the principle of distinction and related rules of the law of armed conflict.[151] Similarly, this threshold of 'armed attack' is applied for cyber operation in relation to Article 51(2) of Additional Protocol I and Article 1 of Additional Protocol II, stipulating the prohibition of attacking civilians.[152]

4.3.5 The principle of proportionality

The principle of proportionality is widely recognized as customary international law. Civilians and civilian objects may be incidentally hit as the collateral result of an attack directed against military objectives.[153] The proportionality rule in the Tallinn Manual 2.0 states that 'a cyber attack that may be expected to cause incidental loss of civilian life, injury to civilians, damage to civilian objects, or a combination thereof, which would be

[148] *Nuclear Weapons advisory opinion*, para. 79; Tallinn Manual 2.0, p. 420.
[149] Droege, 'Armed conflict in Ukraine: a recap of basic IHL rules', ICRC, 17 March 2020, <https://blogs.icrc.org/law-and-policy/2022/03/17/armed-conflict-in-ukraine-a-recap-of-basic-ihl-rules/>, accessed 29 December 2022.
[150] Harrison (2012), p. 180.
[151] Tallinn Manual 2.0, p. 421-422.
[152] Ibid., p. 422-423.
[153] Roscini (2014), p. 220.

excessive in relation to the concrete and direct military advantage anticipated is prohibited'. The rule is based on Articles 51(5)(b) and 57(2)(iii) of Additional Protocol I and is commonly referred to as the principle of proportionality, although technically it pertains to excessiveness rather than proportionality.[154]

The rule addresses situations where a cyber attack against a military objective could result in harm to civilian objects such as computers, networks, or other cyber infrastructure, or to civilians, which cannot be avoided through precaution. It is worth noting that cyber attacks on military objectives may be launched through civilian communications cables, satellites, or other infrastructure, which could be damaged as a result. In other words, a cyber attack can cause collateral damage both during transit and due to the attack itself. Both types of collateral damage should be considered when applying this rule.[155]

Cyber operations can lead to discomfort, irritation, stress, or fear, but these effects do not qualify as collateral damage because they do not constitute 'incidental loss of civilian life, injury to civilians, damage to civilian objects'. The International Group of Experts agreed that 'damage to civilian objects' may, in some situations, include loss of functionality. When this occurs, it should be taken into account in the proportionality assessment.[156]

For example, if Global Positioning Satellite data is blocked or disrupted, transportation systems that rely on this data may experience accidents in the short term, until alternative navigational aids and techniques are implemented. Similarly, an attacker who inserts malware into a specific military computer system may not only disable that system, but also potentially spread the malware to a limited number of civilian computer

[154] Tallinn Manual 2.0, p. 471.
[155] Ibid.
[156] Tallinn Manual 2.0, p. 472.

systems, resulting in collateral damage that meets the qualifications for such damage.[157]

4.3.6 The principle of precaution

Article 57 of Additional Protocol I require that attackers take precautionary measures when conducting military operations and attacks. The International Criminal Tribunal for the former Yugoslavia (ICTY) has recognized the customary nature of these precautions in both the Kupreškić and Tadić cases.[158] The Appeals Tribunal in the Tadić case specifically cited UN General Assembly Resolution 2675, which states that 'all necessary precautions should be taken to avoid injury, loss, or damage to civilian populations', and noted that this resolution represents customary international law 'in armed conflicts of any kind'.[159]

The rule in the Tallinn Manual 2.0 states that '[d]uring hostilities involving cyber operations, constant care shall be taken to spare the civilian population, individual civilians, and civilian objects.' Article 57(1) of Additional Protocol I, which it adheres to, is recognized as customary international law. The International Group of Experts agreed that in cyber operations, commanders and all other personnel involved in the operations have a duty to be constantly aware of the impact of their actions on the civilian population and civilian objects, and to try to avoid any unnecessary consequences.[160]

Due to the complexity of cyber operations, the likelihood of impacting civilian systems, and the limited understanding of the nature and effects of these operations by those responsible for approving them, the Experts conveys that it is advisable for mission planners to have technical experts available to help determine if appropriate precautions have been taken when feasible.[161]

---

[157] Tallinn Manual 2.0, p. 472-473.
[158] Tadic (Interlocutory Appeal), para. 111–12; Kupreškic´, para. 524.
[159] Harrison (2012), p. 209; Tadic (Interlocutory Appeal), paras 111–12, citing GA Res. 2675 (XXV) Basic Principles.
[160] Tallinn Manual 2.0, pp. 476-477.
[161] Ibid., p. 477.

4.3.7 The issue of 'dual-use' objects

Objects used for civilian and military purposes, i.e. 'dual-use' objects are assessed to be a military objective. The International Group of Experts have formulated it as '[c]yber infrastructure used for both civilian and military purposes is a military objective.' An object that is being used, or is intended to be used, to effectively contribute to military action is considered a military objective if its destruction, capture, or neutralization would offer a definite military advantage in the current circumstances. The status of an object as either a civilian object or a military objective is mutually exclusive, meaning that an object cannot be both at the same time. Therefore, all dual-use objects and facilities are considered military objectives without exception. However, when a military objective that is also being used for civilian purposes is attacked, the rule of proportionality and the requirement to take precautions in applies. This means that an attacker must consider the potential harm to protected civilians or civilian objects, or to clearly distinguishable civilian components of the military objective, when deciding whether an attack would be lawful.[162]

Cyber operations present unique challenges when it comes to distinguishing between military and civilian objects. For example, if a network is being used for both military and civilian purposes, it may be impossible to determine which parts of the network are being used for military transmissions. In such cases, the entire network (or at least those parts where transmission is likely) would be considered a military objective. Nonetheless, the Tallinn Manual 2.0 states that there is no reason to treat computer networks differently from physical military objective. It is seen as highly unlikely that the whole Internet would become a military objective due to usage for military purposes.[163]

On the other hand, cyber operations may, under certain circumstances, enable the achievement of a specific objective while causing less destruction or damage that can be more easily repaired compared to traditional military actions. This can be particularly relevant when it comes to objects that have

[162] Tallinn Manual 2.0, p. 445.
[163] Ibid., p. 446.

both civilian and military uses, such as in the case of a military force attempting to disable an enemy underground command bunker by cutting its electricity supply, which also provides power to civilian infrastructure. A cyber operation may allow the attacker to selectively disconnect certain parts of the network, potentially enabling the desired outcome to be achieved while minimizing harm to the civilian population's access to electricity.[164]

4.3.8 Data as an 'object'

In rule 100 the Tallinn Manual 2.0 stipulates:

> *Civilian objects are all objects that are not military objectives. Military objectives are those objects which by their nature, location, purpose, or use, make an effective contribution to military action and whose total or partial destruction, capture or neutralisation, in the circumstances ruling at the time, offers a definite military advantage. Cyber infrastructure may qualify as a military objective.*[165]

Under Article 52(1) of Additional Protocol I, civilian objects are defined as 'all objects which are not military objectives'. The concept of an 'object' is crucial for understanding the rules outlined in the Manual. According to the 1987 Commentary on the ICRC's Additional Protocols, an object is something that is 'visible and tangible'.[166]

Imagine a hypothetical cyber attack in which no physical damage is done to the target, but the data storage devices and connections to the internet are compromised, causing the loss of all data and backups. This attack could lead to economic and potentially political chaos, but the majority of the International Group of Experts determined that it would not be considered an attack under IHL. A minority of the Experts disagreed with this assessment.[167]

This rule should not be interpreted as excluding cyber operations against data (which are non-physical entities) from the definition of an 'attack'. If a cyber

[164] Twenty years on, p. 322.
[165] Tallinn Manual 2.0, p. 435.
[166] Ibid., p. 435-437.
[167] Stephan, 'Big Data and the Future Law of Armed Conflict in Cyberspace', in Matthew C. Waxman, and Thomas W. Oakley (eds) (2022), p. 69.

attack on data is likely to result in injury, death to individuals, damage or destruction to physical objects, then those individuals or objects can be considered the 'object of attack' and the operation would qualify as an 'attack'. Additionally, an operation against data that is essential for the functioning of physical objects can sometimes be considered an 'attack'.[168]

According to the International Group of Experts, the physical hardware involved in cyber operations can be considered an 'object' and therefore entitled to protection under the principle of distinction during attacks. However, a majority of the Experts concluded that data itself does not qualify as an object. This means that, in their view, actions that destroy or damage data but do not have any direct physical effects do not meet the definition of an 'attack'.[169]

Data plays a vital role in the digital realm and is an integral part of many societies. Examples of civilian data that are critical to the functioning of society include medical records, social security information, tax records, bank accounts, customer files for businesses, and election lists and records. As the reliance on data is likely to grow in the coming years, there is increasing concern about safeguarding such vital civilian data.[170]

There are differing opinions on whether data should be considered a protected 'object' under IHL. One argument is that the 'modern meaning' of the concept of objects, and the interpretation of this term in relation to its purpose, leads to the conclusion that data is an 'object' for the purposes of the IHL rules on targeting. This interpretation is supported by the more extensive traditional understanding of the concept of 'objects' in IHL, which includes locations and animals in addition to physical objects. Another proposal is to distinguish between 'operational-level data' or 'code' and 'content-level data.' In this model, it has been suggested that operational-level data could potentially qualify as a military objective and therefore also as a civilian

[168] Tallinn Manual 2.0, p. 416.
[169] Stephan, 'Big Data and the Future Law of Armed Conflict in Cyberspace', in Matthew C. Waxman, and Thomas W. Oakley (eds) (2022), p. 69.
[170] Twenty years on, p. 317.

object. However, this approach has been criticized for providing either a too narrow or too broad interpretation.[171]

The ICRC has emphasized the need to protect essential civilian data, arguing that in cyberspace, tampering with or deleting data could severely disrupt government services and private businesses, causing more harm to civilians than the destruction of physical objects. The ICRC has also pointed out that the transition from paper documents to digital data should not result in a decrease in protection under IHL. According to ICRC, the exclusion of essential civilian data from the protection afforded to civilian objects under IHL would create a significant gap in protection.[172]

4.4 The Fog of Attribution

Attribution is the process of identifying the party responsible for a particular action or behaviour. Determining the actor responsible for a cyber operation is crucial for ensuring accountability in cyberspace and upholding the rules-based international order, as it is often a necessary precondition for taking any responsive action.[173] It is worth noting that applying the law of armed conflict to cyber operations can be challenging because of the difficulties in determining the details of an operation, such as its origin, target and impact. However, these factual questions do not prevent the law of armed conflict from being applied in such cases.[174]

The International Group of Experts applies The International Law Commission's Articles on State Responsibility[175] which is commonly recognized as a reflection of customary international law.[176] The Tallinn Manual 2.0 interprets it as:

[171] Twenty years on, p. 318-319.
[172] Ibid.
[173] Delerue, (2020), p. 51; EUISS p. 11.
[174] Tallinn Manual 2.0, p. 377.
[175] Draft Articles on Responsibility of States for Internationally Wrongful Acts with commentaries, Yearbook of the International Law Commission, vol. II, Part Two, 2001.
[176] Henriksen (2019), p. 121.

Cyber operations conducted by organs of a State, or by persons or entities empowered by domestic law to exercise elements of governmental authority, are attributable to the State.[177]

The term 'organs of a state' should be broadly interpreted to include any person or entity that holds an official status under the domestic law of the State.[178]

During times of war, States may utilize non-State actors, such as private military companies or non-State armed groups, to carry out certain actions, including cyber operations. The unique features of cyberspace, including the potential for actors to conceal or falsify their identity, can make it difficult to attribute actions to specific individuals or parties to armed conflicts. This creates challenges in determining the applicability of IHL. If the perpetrator of a cyber operation cannot be identified, it becomes difficult to determine whether IHL is relevant to the operation. For example, different levels of violence are required to qualify a State or non-State cyber attack as an 'armed conflict', and if the State or non-State origin of a cyber operation outside of an ongoing armed conflict is unknown, it is unclear which threshold that applies.[179]

Additionally, even when an armed conflict is taking place, cyber attacks that have no connection to the conflict (such as criminal acts unrelated to the conflict) are not regulated by IHL, and the inability to identify the perpetrator of a cyber operation may prevent a determination of whether such a connection exists. These examples illustrate that identifying the actor responsible for a cyber operation and whether the operation can be attributed to a State or non-State party to the conflict has significant legal implications.[180]

It is important to remember that there are three different levels of attribution: technical, political, and legal. These types of attribution can be conveyed through various means, such as security alerts, official statements, and

[177] Tallinn Manual 2.0, p. 87.
[178] Ibid.
[179] Twenty years on, p. 309.
[180] Twenty years on, p. 309.

regulatory and legal documents. They can also be applied to different types of entities, including individuals, threat actors, companies, and States. Attribution serves different purposes, including enforcement, defence, deterrence, and the establishment of norms. It is both the outcome of an investigation to identify the perpetrator and a process in itself.[181]

In recent years, several States have attributed cyber operations to other States, sometimes qualifying them as wrongful acts, but they neither detailed which norms of international law had been breached, nor used the international legal framework to respond to these acts.[182] The European Union Agency for Cybersecurity (ENISA) predicts that as cyber operations have gained importance for States, efforts will be made to publicly attribute cyber campaigns, disrupt the infrastructure of adversaries and use indictments to 'name and shame' operators. In the near to mid-term future, ENISA expect that more States will take legal action against cyber threat actors.[183]

This was also addressed in the GGE 2021 report:

> *The Group reaffirms that States must meet their international obligations regarding internationally wrongful acts attributable to them under international law. It also reaffirms that States must not use proxies to commit internationally wrongful acts using ICTs, and should seek to ensure that their territory is not used by non-State actors to commit such acts. At the same time, the Group recalls that the indication that an ICT activity was launched or otherwise originates from the territory or the ICT infrastructure of a State may be insufficient in itself to attribute the activity to that State; and notes that accusations of organizing and implementing wrongful acts brought against States should be substantiated. The invocation of the responsibility of a State for an internationally wrongful act involves complex technical, legal and political considerations.*[184]

Notably, not all responses require attribution. Retorsion, i.e. actions that do not violate international law, can be used to respond to unfriendly acts that do

[181] EUISS, p. 42.
[182] Delerue (2020), p. 1.
[183] ENISA Threat Landscape , p. 26.
[184] UNGGE 2021 Report, para. 71(g).

not breach any international obligations. In these cases, legal attribution is not required.[185]

[185] EUISS, p. 46.

5 The Way Forward: Cyber Warfare in Ukraine and Beyond

The man-made ecosystem called cyberspace is expanding into gray zones we did not even know existed. And as it expands, the attack surface grows larger. To the public's knowledge, there has been no 'cyber Pearl Harbor' as of yet, but the question is, is there legal interpretations in place for it to be sufficiently responsive? The jus in bello regime has as its objective to protect civilians and civilian objects from the effects of hostilities – the cyber domain should not be a domain of legal ambiguity where the necessary legal safeguards cannot be sufficiently applied.

5.1 In the Light of the Russo-Ukrainian War: The Current Status of the Jus in Bello Regime

The Russo-Ukrainian war is taking place on multiple battlefields, with the cyber domain being one of them. Many of the wartime cyber operations raises judicial considerations with regards to international humanitarian law which is to be analysed further in this Chapter.

At the outset, the first consideration which needs to be addressed is whether international law, and IHL in particular, does apply to cyberspace. The GGE consensus reports adopted in the UN General Assembly, dating back to 2013 and 2015, established that international law does apply to cyberspace. However, the application of the jus in bello regime has proven to be more controversial. In 2017, the GGE failed to adopt its fifth consensus report due to some States questioning whether certain branches of international law applied to cyberspace, with one of the branches being IHL. Some Member States are concerned that the recognition of the framework in the domain will legitimize cyber warfare. This group of States would prefer to negotiate a new treaty that explicitly would regulate ICTs. Despite the colliding views, the

GGE and the OWEG have successfully adopted consensus reports with explicit references to IHL. Nevertheless, the consensus on the jus in bello regimes application to cyberspace remains strong amongst experts and the multi-stakeholder community. The International Group of Experts drafting the Tallinn Manuals and the ICRC stands firmly behind the approach of application. Against the backdrop of the extensive cyber elements of the Russo-Ukrainian war, it is evident that there is a need for such regulations that IHL provide. It would be preferable if States, practitioners and the multi-stakeholder community fully committed to the discussions on *how* the laws of armed conflict apply.

When it comes to the current status of the practical application of the jus in bello framework in cyberspace, there are several challenging considerations that need to be studied further. The core regulations of the jus in bello regime came about in a time when cyberspace as we know it today was unimaginable. Today, the lines between war and peace are becoming difficult to outline and the digital realm is being used by States actors to gain advantage against its adversaries.

Article 2 of the 1949 Geneva Conventions provides the criteria for an international armed conflict. There must be an 'international' element and an element amounting to the use of 'armed' force. In line with the International Group of Expert's assessment the hostilities that are part of the conflict may include a combination of kinetic and cyber operations, or they may consist solely of cyber operations as long as the criteria in Article 2 are fulfilled. When studying the case of the Russo-Ukrainian war, one interesting aspect is the launch of the Foxblade wiper software one day before the initiation of the military aggression. The Tallinn Manual Experts seem to apply a slightly more restrictive approach than the ICRC which holds the view that cyber operations independently can attain the ability to amount to the threshold of an international armed conflict under IHL. However, since the threshold is unspecified, it would be difficult to apply if Russia would have continued to launch cyber attacks as their sole method of warfare.

With regards to the notion of ‘attack’, Article 49(1) of Additional Protocol I defines an ‘attack’ as ‘acts of violence against the adversary, whether in offence or in defense’. The Tallin Manual 2.0 defines ‘attack’ as ‘[…] a cyber operation, whether offensive or defensive, that is reasonably expected to cause injury or death to persons or damage or destruction to objects’. Since the concept of an ‘attack’ serves as a foundation for various limitations and prohibitions in the laws of armed conflict, the author agrees with the ICRC that this would need further consideration. To this day, there has been no person that has fallen victim to a cyber attack physically, still they cause severe damage and destress to both civilians and societies at large. In the Russo-Ukrainian case, the cyber attacks on CNI, including sectors that civilians rely on, are concerning. These sorts of attacks should not fall short of legal regulation.

In the Russo-Ukrainian war there has been a large-scale involvement from hacktivist groups and private companies. Most members of the International Group of Experts agreed that civilians maintain their civilian status even if they directly engage in cyber hostilities. However, a minority of Experts were of the view that these individuals do not qualify as either civilians or combatants. It is immanent that civilians choosing to participle in cyber hostilities know the terms for such an engagement. Most likely, this trend of voluntary online involvement will continue as our interconnectivity increases.

One challenge with cyber operations is determining the difference between military and civilian targets. This can be difficult due to the nature of the Internet and the interconnectedness of various systems and networks. It is important to accurately identify and distinguish between military and civilian objects in order to adhere to the principles of distinction and proportionality. An additional issue in this equation is the increase of objects used for civilian and military purposes. This could be detrimental for civilians on the one hand, but on the other hand it could function as a safeguard for civilians. When deploying a cyber operation, the attacker may have the ability to selectively disconnect certain parts of a network, potentially achieving the desired outcome while minimizing the disruption for civilians. Unfortunately, as

shown by the exposition of the wartime cyber operations against Ukraine, the perpetrator could have little interest in minimizing harm to civilians.

Finally, concerning data as an 'object' it is clear that wiper software can have an immense effect on societies and civilians. Data is highly valued in the digital world and is a crucial asset to many societies. Given that reliance on data is likely to increase in the future, it is concerning that data, under the current interpretation, is not assessed to meet the criteria of a civilian object. This is a gap through interpretation that can cause severe negative effects to civilians and societies. States should acknowledge these areas of IHL in multilateral fora and publish national statements and positions in order to form a general approach.

5.2 Developments Going Forward

The findings from the previous section demonstrate that the current application of IHL leaves gaps that potentially can expose people or vital objects to harm. The Russo-Ukrainian war provides an example of the massive disruptions and destructions that cyber warfare can cause. Even if the cyber activities in this particular war have not yet amounted to the, by experts, predicted severity, it discloses the need for safeguards in the cyber domain. The partaken Parties can take advantage of the gray areas and gain strategical advantage. The difficulty in attributing hostile cyber operations is also exploited.

If we allow the concept of 'cyber' to be ambiguous, with wartime and peacetime blending together, it can introduce risk and inefficiency. This risk includes the possibility of escalation between States if peacetime operations are seen as having hostile intentions. It further includes leeway for malicious targeting of civilians.

However, in the current geopolitical landscape, it would be a difficult endeavour to agree upon a treaty or additional norms relating to IHL. It is challenging to engage in fruitful discussions on how to further strengthen the international rule-based order when States at the negotiating table are actively

breaching international law with lacking motivation to preserve neither peace, nor human rights. Tensions are rising, rhetoric is shifting and political agendas are being pushed more urgently in multilateral settings. With this taken into regard, States need to commit to discussions on the *interpretation* of existing treaty and customary law to ensure that the normative framework of IHL remains relevant and effective.

Going forward, it would be advisable to focus on the core principles and rules of the jus in bello regime in the OWEG and the PoA. States should address the objective of the framework and the gaps that the current interpretation presents. It is clear that developments in the application of IHL to cyberspace is needed to properly serve the purpose that the framework embodies.

6 Concluding Remarks

The purpose of this thesis has been to investigate the use of cyber operations in international armed conflicts and the application of the jus in bello framework. The study has provided a critical examination of the current legal landscape of IHL in the light of the cyber elements in the Russo-Ukrainian war. With regards to shifting geopolitical realities, suggestions on ways forward to advance the application of the jus in bello framework have been presented.

As observed in Chapter 3, the effects of cyber operations during the Russo-Ukrainian war on societal functions critical to civilians have been substantial. Cyber offensives have disrupted critical infrastructure and essential services, such as power supply, financial and healthcare systems, and communication networks. These disruptions have had a direct impact on the daily lives of civilians, potentially putting their health and safety at risk.

Despite the repeated assertion that international law applies to cyberspace, the jus in bello framework remains a subject of debate. The analysis unveils that the current application of IHL, as outlined in guiding documents such as the Tallinn Manual 2.0, does not adequately address the complexities of wartime cyber operations. The author therefore calls for further efforts to enforce the jus in bello regime in the cyber domain, in order to safeguard the objective of the framework.

As a way forward, it is suggested that States actively engage in multilateral discussions on *how* IHL applies to cyberspace. One of the main points for discussion in the UN processes, such as the OEWG and the PoA, should be the fundamental principles and rules of the jus in bello regime. States, practitioners and the multi-stakeholder community should acknowledge areas of international humanitarian law that are ambiguous, and States are advised to publish national statements and positions in order to form a general approach.

Bibliography

Literature

Delerue, Francois, *Cyber Operations and International Law*, Cambridge University Press, Cambridge, 2020.

Harrison, Dinniss, Heather, *Cyber Warfare and the Laws of War*, Cambridge University Press, Cambridge, 2012.

Henriksen, Anders, *International law*, Second edition, Oxford University Press, Oxford, 2019.

Korling, Fredrick and Zamboni, Mauro (red.), *Juridisk metodlära*, 2nd ed., Studentlitteratur, Lund, 2018.

Matthew C. Waxman, and Thomas W. Oakley (eds), *The future law of armed conflict*, Oxford University Press, New York, 2022.

Saul, Ben & Akande, Dapo (red.), *The Oxford guide to international humanitarian law*, Oxford University Press, Oxford, 2020.

Schmitt, Michael N. and Vihul, Liis (red.), *Tallinn manual 2.0 on the international law applicable to cyber operations: prepared by the international group of experts at the invitation of the NATO cooperative cyber defence centre of excellence*, Second edition., Cambridge University Press, Cambridge, 2017.

Tsagourias, Nikolaos K. & Buchan, Russell (red.), *Research handbook on international law and cyberspace*, 2. ed., Edward Elgar Publishing, Cheltenham, 2021.

Roscini, Marco, *Cyber operations and the use of force in international law*, Oxford University Press, Oxford, 2014.

International Treaties and Instruments

United Nations, *Statute of the International Court of Justice*, 18 April 1946.

The International Law Commission, *Draft Articles on Responsibility of States for Internationally Wrongful Acts*, 2001.

International Committee of the Red Cross (ICRC), *Geneva Convention for the Amelioration of the Condition of the Wounded and the Sick in Armed Forces in the Field* (First Geneva Convention), 12 August 1949, 75 UNTS 31 [Geneva Conventions].

International Committee of the Red Cross (ICRC), *Geneva Convention for the Amelioration of the Condition of Wounded, Sick and Shipwrecked Members of Armed Forces at Sea* (Second Geneva Convention), 12 August 1949, 75 UNTS 85 [Geneva Conventions].

International Committee of the Red Cross (ICRC), *Geneva Convention Relative to the Treatment of Prisoners of War* (Third Geneva Convention), 12 August 1949, 75 UNTS 135 [Geneva Conventions].

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 [Geneva Conventions].

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 [Additional Protocol I].

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, 1125 UNTS 609 [Additional Protocol II].

International Committee of the Red Cross (ICRC), *Declaration Renouncing the Use, in Time of War, of Explosive Projectiles Under 400 Grammes Weight*, 29 November/11 December 1868 [St. Petersburg Declaration].

International Conferences (The Hague), *Hague Convention (II) with Respect to the Laws and Customs of War on Land and its Annex: Regulations Concerning the Laws and Customs of War on Land*, 29 July 1899.

International Conferences (The Hague), *Hague Convention (IV) Respecting the Laws and Customs of War on Land and Its Annex: Regulations Concerning the Laws and Customs of War on Land*, 18 October 1907.

Table of cases

International Court of Justice

Legality of the Threat or Use of Nuclear Weapons, Advisory Opinion, ICJ Reports 1996.

Prosecutor v. Kupreskic et al. (Trial Judgement), IT-95-16-T, International Criminal Tribunal for the former Yugoslavia (ICTY), 14 January 2000.

*Prosecutor v. Dusko Tadic aka "Dule" (Decision on the Defence Motion for Interlocutory Appeal on Jurisdiction), IT-94-1, International Criminal Tribunal for the former Yugoslavia (*ICTY), 2 October 1995.

Journals

Benatar M (2014), 'Cyber Warfare', In A. Carty (Ed.), Oxford Bibliographies in International Law (pp. 1-23). Oxford University Press.

Douzet F, Géry A and Delerue F (2022), 'Building Cyber Peace While Preparing for Cyber War' in Scott J Shackelford, Frederick Douzet and Christopher Ankersen (eds), *Cyber Peace: Charting a Path Toward a Sustainable, Stable, and Secure Cyberspace*, Cambridge University Press.

Gisel L, Rodenhäuser T and Dörmann K (2020), 'Twenty Years on: International Humanitarian Law and the Protection of Civilians against the Effects of Cyber Operations during Armed Conflicts', 102 International Review of the Red Cross 287.

Geiss R and Lahmann H (2021), ‘Working Papers: Protecting Societies - Anchoring A New Protection Dimension In International Law In Times Of Increased Cyber Threats’, Geneva Academy.

Official Documents

European Commission, Joint Communication to the European Parliament and the Council: EU Policy on Cyber Defence, JOIN(2022) 49 final, 10 November 2022.

Council of the European Union, A Strategic Compass for Security and Defence - For a European Union that protects its citizens, values and interests and contributes to international peace and security, 7371/22, 21 March 2022.

Resolutions

UNGA, ‘Developments in the field of information and telecommunications in the context of international security’, (13 October 2022), A/C.1/77/L.73.

Reports

ENISA, ‘ENISA Threat Landscape 2022’, October 2022.

ICRC, ‘Digitalizing the Red Cross, Red Crescent and Red Crystal Emblem – Benefits, risks and possible solution’, 3 November 2022.

ICRC, ‘The Potential Human Cost of Cyber Operation’, 12 June 2020.

Microsoft, ‘Defending Ukraine: Early Lessons from the Cyber War’, 22 June 2022.

Microsoft, ‘Microsoft Digital Defense Report 2022’, 4 November 2022.

Microsoft, ‘Special report: Ukraine - An overview of Russia’s cyberattack activity in Ukraine’, 27 April 2022.

Pijpers, ‘Exploiting cyberspace: International legal challenges and the new tropes, techniques and tactics in the Russo-Ukraine War’, Hybrid CoE, 20 October 2022.

The European Union Institute for Security Studies (EUISS), ‘A Language of Power: Cyber defence in the European Union’, 2022.

UNGA, ‘Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security’ (24 June 2013), UN Doc. A/68//98.

UNGA, ‘Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security’ (22 July 2015), UN Doc. A/70/174.

UNGA, ‘Chair’s Summary of the Open-ended working group on developments in the field of information and telecommunications in the context of international security’ (10 March 2021), UN Doc. A/AC.290/2021/CRP.3.

UNGA, Report of the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security (14 July 2021) UN Doc A/76/135.

United Nations Human Rights Office of the High Commissioner, 'International legal protection of human rights in armed conflict', 2011.

Internet sources

A Dictionary of Computer Science (ed. Butterfield & Ngondi), 7th edition, Oxford University Press, Online version published 2016, accessed 23 December 2022.

Antoniuk and Peterson, 'The invasion of Ukraine started online long before troops marched on Kyiv', The Record by The Recorded Future, 28 February 2022, <https://therecord.media/the-war-for-ukraine-started-online-long-before-troops-marched-on-kyiv/>, accessed 28 December 2022.

Britannica Academic, s.v. 'Cyberwar', accessed December 31, 2022, <https://academic-eb-com.ludwig.lub.lu.se/levels/collegiate/article/cyberwar/488833>, accessed 28 December 2022.

Bumillier, Shanker, 'Panetta Warns of Dire Threat of Cyberattack on U.S', The New York Times, 11 October 2012 <https://www.nytimes.com/2012/10/12/world/panetta-warns-of-dire-threat-of-cyberattack.html>, accessed 28 December 2022.

CyberPeace Institute, 'A moment of historical significance – Russia's invasion of Ukraine underlines the need for cyber peace', 23 June 2022, <https://cyberpeaceinstitute.org/news/a-moment-of-historical-significance-russias-invasion-of-ukraine-underlines-the-need-for-cyber-peace/>, accessed 28 December 2022.

CyberPeace Institute, 'Case Study Viasat', June 2022, <https://cyberconflicts.cyberpeaceinstitute.org/law-and-policy/cases/viasat>, accessed 29 December 2022.

CyberPeace Institute, 'Law & Policy', <https://cyberconflicts.cyberpeaceinstitute.org/law-and-policy>, accessed 28 December 2022.

CyberPeace Institute, 'Shields up: Top insights from cyber experts on the threats of 2022', <https://cyberpeaceinstitute.org/news/ukraine-top-insights-from-cyber-experts-threats-2022/>, accessed 27 December 2022.

Droege, 'Armed conflict in Ukraine: a recap of basic IHL rules', ICRC, 17 March 2020, <https://blogs.icrc.org/law-and-policy/2022/03/17/armed-conflict-in-ukraine-a-recap-of-basic-ihl-rules/>, accessed 29 December 2022.

ICRC, Briefing by the International Committee of the Red Cross, Dr Helen Durham, Director of International Law and Policy – United Nations Security Council, 20 December 2021, <https://www.icrc.org/en/document/briefing-helen-durham-international-law-policy-united-nations-security-council-cyber-operations>, accessed 28 December 2022.

ICRC, ‘Cyberspace is not a legal vacuum, including during armed conflict’, 8 December 2022, <https://www.icrc.org/en/document/cyberspace-not-legal-vacuum-including-during-armed-conflict>, accessed 28 December 2022.

ICRC, ‘Cyber Warfare: does International Humanitarian Law apply?’, 25 February 2021, <https://www.icrc.org/en/document/cyber-warfare-and-international-humanitarian-law>, accessed 28 December 2022.

ICRC, ‘Regional state consultations on international humanitarian law and cyber operations during armed conflicts’, 29 June 2022, <https://www.icrc.org/en/document/regional-state-consultations-ihl-cyber-operations>, accessed 26 December 2022.

ICRC, ‘The potential human cost of cyber operations’, <https://www.icrc.org/en/document/potential-human-cost-cyber-operations>, accessed 28 December 2022.

Internet World Stats: Usage and Population Statistics, <https://www.internetworldstats.com/stats.htm>, accessed 28 December 2022.

Matishak, ‘Biden signs $858 billion defense policy bill into law, expanding gov’t cyber operations’, The Record by Recorded Future, 23 December 2022 <https://therecord.media/biden-signs-858-billion-defense-policy-bill-into-law>, accessed 28 December 2022.

NATO, ’Cyber defence’, <https://www.nato.int/cps/en/natohq/topics_78170.htm>, accessed 2 January 2023.

Raffray, 'Ukraine: Beyond Kinetic', CyberPeace Institute, 4 April 2022, <https://cyberpeaceinstitute.org/news/ukraine-beyond-kinetics/>, accessed 29 December 2022.

Srivastava, Murgia and Murphy, 'The secret US mission to bolster Ukraine's cyber defences ahead of Russia's invasion', The Financial Times, 9 March 2022, <https://www.ft.com/content/1fb2f592-4806-42fd-a6d5-735578651471>, accessed 27 December 2022.

Smith, 'Cyber attacks set to become 'uninsurable', says Zurich chief', Financial Times, 26 December 2022, <https://www.ft.com/content/63ea94fa-c6fc-449f-b2b8-ea29cc83637d>, accessed 25 December 2022.

Smith, 'Digital technology and the war in Ukraine', Microsoft, 28 February 2022, <https://blogs.microsoft.com/on-the-issues/2022/02/28/ukraine-russia-digital-war-cyberattacks/?preview_id=65075>, accessed 25 December 2022.

Smith, 'Lloyd's of London defends cyber insurance exclusion for state-backed attacks', Financial Times, 5 September 2022, <https://www.ft.com/content/e865a3d1-5652-41aa-990a-bb5ad57288c6>, accessed 25 December 2022.

Statista Research Department, 'Share of households with internet access in the European Union (EU) from 2008 to 2021', 11 August 2022 <https://www.statista.com/statistics/377585/household-internet-access-in-eu28/> accessed 2 January 2023.

Tiirmaa-Klaar, ‘Cyber Symposium – Diplomatic considerations for armed attack’, Lieber Institute, 27 July 2022, <https://lieber.westpoint.edu/diplomatic-considerations-armed-attack/>, accessed 23 December.

Weber, ‘How to Strengthen the Program of Action for Advancing Responsible State Behavior in Cyberspace’, 10 February 2022, <https://www.justsecurity.org/80137/how-to-strengthen-the-programme-of-action-for-advancing-responsible-state-behavior-in-cyberspace/>, accessed 28 December 2022.