



**Russia's Cyber Warfare In Georgia and Ukraine:
How does it challenge International Humanitarian Law?**

Author: Elisabedi Koridze

Supervisor: Marika Ericson

Master's Program in International Operational Law

Swedish Defence University

May 2025

Word count: 15,735

Declaration

I, Elisabedi Koridze, hereby declare that I am the sole author and composer of this thesis. To the best of my knowledge, this thesis do not contain any material that has been published previously by any other person except where the acknowledgements has been made. I also declare that my thesis has not been prepared for another examination or assignment, moreover, no part of this thesis was previously presented for another degree or diploma at this or any other institution.

I also declare, that during the writing process, I used Grammarly to check my grammar mistakes.

Abstract:

This thesis explores how International Humanitarian Law (IHL) applies to cyber operations during armed conflicts, focusing on the legal challenges and gaps exposed by Russia's cyber operations in Georgia (2008) and Ukraine (2014, 2022). Cyber warfare has become a critical element of modern armed conflict, but IHL struggles to regulate this new form of warfare.

The thesis examines how the core principles of IHL, distinction, proportionality, and military necessity, are challenged when applied to the cyber domain. It also discusses the issue of attribution, which remains one of the most difficult legal problems in cyber warfare. Using real-life examples, including the Kyivstar attack, the thesis shows how dual-use infrastructure and cyber-tech unpredictability create legal uncertainty. The analysis further shows that while IHL applies to cyber operations during armed conflict, the rules are not always easy to implement.

The main conclusion is that IHL must evolve to stay relevant in the age of cyber warfare and must offer the same level of protection to civilians, whether the attack comes from a missile or from a computer system.

Declaration.....	2
Abstract:.....	3
List of Acronyms:.....	5
Introduction.....	6
1.1 Research Background and Significance.....	6
1.2 Defining Cyber Warfare and Its Role in Modern Conflicts.....	8
1.3 Case studies: Why Georgia and Ukraine?.....	10
1.4 Research question and structure.....	11
2. Cyber Warfare and International Humanitarian Law.....	12
2.1 The Legal Classification of Cyber Operations Under International Humanitarian Law.....	13
3. Legal Challenges in Applying IHL to Cyber Warfare.....	18
3.1 The principle of distinction - Can cyberattacks distinguish between military and civilian targets?...	20
3.2 The principle of proportionality - How can cyberattacks be assessed for excessive harm?.....	27
3.3 The principle of necessity - Are cyberattacks militarily necessary or excessive?.....	32
3.4 Attribution challenges - How can states be held accountable for cyberattacks under IHL?.....	35
Effective Control.....	40
Overall control.....	42
Cases.....	44
Georgia (2008).....	44
Ukraine (2017).....	45
Conclusion.....	47
4. Future of Cyber Warfare and IHL.....	48
4.1 Legal gaps in IHL regarding cyberattacks.....	49
4.2 Should IHL be modified to regulate cyberattacks explicitly?.....	52
5. Conclusion.....	56
Bibliography:.....	60
Articles.....	60
Books.....	63
Case Law.....	64
International Court of Justice (ICJ).....	64
International Criminal Tribunal for the former Yugoslavia (ICTY).....	64
Law and Soft Law.....	64
Newspaper Articles.....	65
Other Electronic Resources.....	65
Position Papers.....	66
Reports.....	67
Other Sources.....	67

List of Acronyms:

API – Additional Protocol I to the Geneva Conventions

ARSIWA – Articles on Responsibility of States for Internationally Wrongful Acts

DDoS – Distributed Denial of Service

IAC - International Armed Conflict

ICJ – International Court of Justice

ICRC – International Committee of the Red Cross

ICTY – International Criminal Tribunal for the Former Yugoslavia

ILC – International Law Commission

IHL – International Humanitarian Law

IT – Information Technology

SBU – Security Service of Ukraine

UNGA – United Nations General Assembly

VPN – Virtual Private Network

Introduction

Traditional armed conflicts are still relevant in the 21st century, but cyber warfare is now becoming a part of modern conflicts, taking many forms from spreading fake information to attacking critically important systems like electricity or hospitals.¹ These types of attacks are now an integral part of military strategy which has proven to be problematic for the current legal rules, especially International Humanitarian Law (IHL), which was developed to regulate kinetic warfare.² As cyberattacks become more advanced, it is important to see how they work under IHL rules.

1.1 Research Background and Significance

In recent years, warfare has evolved beyond traditional battlefields.³ Some authors believe that cyberspace, recognized as the fifth domain of warfare, alongside land, sea, air, and space, presents unique challenges and opportunities for both state and non-state actors.⁴ Unlike

¹ Michael N Schmitt, 'International Humanitarian Law and the Conduct of Cyber Hostilities: Quo Vadis?' (2022) 13(2) *International Humanitarian Legal Studies* 192 https://brill.com/view/journals/ihts/13/2/article-p189_002.xml accessed 9 May 2025.

² Ahmad Khalil, Mhd Bitar and S Anandha Krishna Raj, 'A New Era of Armed Conflict: The Role of State and Non-State Actors in Cyber Warfare with Special Reference to Russia-Ukraine War' (2024) 14(2) *TalTech Journal of European Studies* 50 https://www.researchgate.net/publication/386231399_A_New_Era_of_Armed_Conflict_The_Role_of_State_and_Non-State_Actors_in_Cyber_Warfare_with_Special_Reference_to_Russia-Ukraine_War accessed 9 May 2025.

³ Vakhtang Maisaia, Aliko Guchua and Thornike Zedelashvili, 'The cybersecurity of Georgia and threats from Russia' (2020) 9 *Eastern Review* 105, 106 <https://doi.org/10.18778/1427-9657.09.07> accessed 9 May 2025.

⁴ Ahmad Khalil, Mhd Bitar and S Anandha Krishna Raj, 'A New Era of Armed Conflict: The Role of State and Non-State Actors in Cyber Warfare with Special Reference to Russia-Ukraine War' (2024) 14(2) *TalTech Journal of European Studies* 50 https://www.researchgate.net/publication/386231399_A_New_Era_of_Armed_Conflict_The_Role_of_State_and_Non-State_Actors_in_Cyber_Warfare_with_Special_Reference_to_Russia-Ukraine_War accessed 9 May 2025.

traditional military tactics, cyber warfare operates in the digital domain that creates challenges for international law.

As cyber operations become more integrated into modern warfare, their potential impact on civilians raises concerns.⁵ Civilian infrastructure is especially vulnerable to digital attacks because systems that link the digital and physical worlds like power grids, hospitals, and communication networks are highly exposed to outside interference. This raises serious risks for civilian population during armed conflict, as cyberattacks can cause widespread harm without physical destruction.⁶

IHL gives a legal framework for regulating armed conflicts, and makes sure that civilians are protected by limiting the means and methods of warfare.⁷ But using cyber operations as part of military strategies brings many legal problems. This is even more serious when cyberattacks target civilian infrastructure systems that are used both for civilian and military purposes.⁸ The lack of direct legal provisions that govern cyber warfare caused significant debate among scholars, policymakers, and international bodies. There are several reasons why it can be

⁵ International Committee of the Red Cross, *The Potential Human Cost of Cyber Operations* (ICRC 2021) 32 <https://shop.icrc.org/the-potential-human-cost-of-cyber-operations-pdf-en.html> accessed 9 May 2025.

⁶ Cordula Droege, 'Get Off My Cloud: Cyber Warfare, International Humanitarian Law, and the Protection of Civilians' (2012) 94(886) *International Review of the Red Cross* 538 <https://international-review.icrc.org/sites/default/files/irrc-886-droege.pdf> accessed 9 May 2025.

⁷ Michael Bothe and others, 'Scope of Application of International Humanitarian Law' in Dieter Fleck (ed), *The Handbook of International Humanitarian Law* (4th edn, OUP 2021) 51 <https://doi.org/10.1093/law/9780198847960.003.0003> accessed 9 May 2025.

⁸ Ahmad Khalil, Mhd Bitar and S Anandha Krishna Raj, 'A New Era of Armed Conflict: The Role of State and Non-State Actors in Cyber Warfare with Special Reference to Russia-Ukraine War' (2024) 14(2) *TalTech Journal of European Studies* 49–50 https://www.researchgate.net/publication/386231399_A_New_Era_of_Armed_Conflict_The_Role_of_State_and_Non-State_Actors_in_Cyber_Warfare_with_Special_Reference_to_Russia-Ukraine_War accessed 9 May 2025.

challenging to regulate cyber operations under IHL, for example, the complex nature of attribution, or the difficulties to distinguish between civilian and military targets.⁹

This thesis seeks to explore how cyber operations challenge the application of IHL by using Russia's cyber operations in Georgia (2008) and Ukraine (2014, 2022) as examples. By analyzing these case studies, the research aims to assess how cyber warfare challenges the application of IHL and to what extent the existing legal framework is capable of addressing this emerging form of warfare.

1.2 Defining Cyber Warfare and Its Role in Modern Conflicts

Currently, there is no legal definition of cyber warfare in international law that everyone would agree on. Some scholars argue that the terms “cyber war” or “cyber attack” lack legally binding definitions, and additionally, there is no specific treaty, relevant case law or established customary law that could serve as legal doctrine in this area.¹⁰

According to the International Committee of the Red Cross (ICRC), cyber warfare is “a means and method of warfare that consist of cyber operations amounting to, or conducted in the context of, an armed conflict, within the meaning of IHL.”¹¹ Cyber warfare refers to the use of a data stream to gain access to a computer system and transmit viruses to gain access or destroy the

⁹ Hannah Gray, ‘Cyberwarfare and the Challenges It Poses to the International Governance of Armed Conflict with Particular Reference to Attribution, Distinction, and Self-Defence’ (2024) 66 <https://doi.org/10.2218/ccj.v5.9346> accessed 9 May 2025.

¹⁰ David Turns, ‘Cyber War and the Concept of Attack in International Humanitarian Law’ in Dan Saxon (ed), *International Humanitarian Law and the Changing Technology of War* (Brill Nijhoff 2013) 211 <https://research-ebSCO-com.proxy.annalindhbiblioteket.se/c/cxt7bo/search/view/uy76oqhtfv?db=e00xww> accessed 9 May 2025.

¹¹ International Committee of the Red Cross, ‘International Humanitarian Law and Cyber Operations during Armed Conflict: ICRC Q&A and Commentary’ (21 June 2013) 1 <https://www.icrc.org/sites/default/files/external/doc/en/assets/files/2013/130621-cyberwarfare-q-and-a-eng.pdf> accessed 9 May 2025.

data, more specifically using cyber operations, such as hacking, malware deployment, and Distributed Denial of Service attacks (DDoS), to achieve military or political objectives.¹² There are different categories of cyber attacks, and their classifications are crucial in determining whether a cyber operation falls within the scope of IHL, as not all cyber operations amount to an "attack" in the legal sense.¹³ The applicability of IHL depends on whether a cyber operation results in tangible harm or disruption comparable to kinetic attacks.¹⁴

The Tallinn Manual on the International Law Applicable to Cyber Warfare provides one of the most comprehensive analyses of how international law applies to cyber operations.¹⁵ Rule 92 of the Manual defines cyberattacks as operations that are reasonably expected to cause injury or death to persons and damage or destruction to objects.¹⁶ These attacks can target governmental institutions, military infrastructure, communication networks, and critical civilian services, and they can cause injury or death to humans or damage or destruction to objects¹⁷. Unlike traditional

¹² Jason Andress and Steve Winterfeld, *Cyber Warfare: Techniques, Tactics and Tools for Security Practitioners* (Syngress 2014) 21–30 <https://research-ebSCO-com.proxy.annalindhbliblioteket.se/linkprocessor/plink?id=8e7ca649-3633-3b4c-b2f2-0660606afcd2> accessed 9 May 2025.

¹³ Lukasz Olejnik and Tilman Rodenhäuser, 'Malware: A Selection of Essential Cyber Notions and Concepts' (ICRC Humanitarian Law & Policy Blog, 23 May 2019) <https://blogs.icrc.org/law-and-policy/2019/05/23/malware-essential-cyber-notions-concepts/> accessed 9 May 2025.

¹⁴ Heather Harrison Dinniss, *Cyber Warfare and the Laws of War* (Cambridge University Press 2012) 113 <https://research-ebSCO-com.proxy.annalindhbliblioteket.se/c/cxt7bo/ebook-viewer/pdf/rdqnchnaf?location=https%3A%2F%2Fresearch-ebSCO-com.proxy.annalindhbliblioteket.se%2Fc%2Fcxt7bo%2Fdetails%2Frdqnchnaf> accessed 9 May 2025.

¹⁵ Michael N Schmitt (ed), *Tallinn Manual on the International Law Applicable to Cyber Warfare* (Cambridge University Press 2013) 106 <https://research-ebSCO-com.proxy.annalindhbliblioteket.se/c/cxt7bo/ebook-viewer/pdf/7m3vylje7j?location=https%3A%2F%2Fresearch-ebSCO-com.proxy.annalindhbliblioteket.se%2Fc%2Fcxt7bo%2Fdetails%2F7m3vylje7j> accessed 9 May 2025.

¹⁶ Michael N Schmitt (ed), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (2nd edn, Cambridge University Press 2017) 415 <https://www-cambridge-org.proxy.annalindhbliblioteket.se/core/books/tallinn-manual-20-on-the-international-law-applicable-to-cyber-operations/E4FFD83EA790D7C4C3C28FC9CA2FB6C9> accessed 9 May 2025.

¹⁷ Rohit Bokil, 'Cyber Warfare: Taking War to Cyberspace and Its Implications for International Humanitarian Law' (2023) 5(1) *International Journal For Multidisciplinary Research* 2, 3 <https://doi.org/10.36948/ijfmr.2023.v05i01.1494> accessed 9 May 2025.

warfare, cyber operations often involve secret actions which makes it difficult to attribute responsibility and respond within existing legal frameworks. Moreover, many cyber operations fall into a legal grey area, as the destructions are not always tangible but can still have significant consequences for national security and civilian well-being.¹⁸

Russia's use of cyber warfare during its conflicts with Georgia and Ukraine shows how cyber operations have become an essential part of modern military strategy. In both cases, cyberattacks were launched alongside kinetic military operations. In order to evaluate the adequacy of IHL in addressing cyber warfare, it is very important to understand how these cyber attacks were conducted.

1.3 Case studies: Why Georgia and Ukraine?

This thesis focuses on Russia's cyber operations in Georgia (2008) and Ukraine (2014, 2022) for several reasons.

Firstly, the Russia-Georgia war was one of the first documented instances where cyberattacks were used alongside kinetic warfare.¹⁹ During the five-day conflict, Georgian government websites, media outlets, and communication systems were targeted and the attacks disrupted government functions and spread misinformation.²⁰ Although these cyberattacks were not officially attributed to the Russian government, they were widely believed to be state-sponsored

¹⁸ Dominika Dziwisz, 'Rethinking Future Conflicts: The Cyber Grey Zone from the Russian Perspective' (2024) 21 *Politeja* 281, 285–90 <https://doi.org/10.12797/Politeja.21.2024.92.13> accessed 9 May 2025.

¹⁹ Hannah Gray, 'Cyberwarfare and the Challenges It Poses to the International Governance of Armed Conflict with Particular Reference to Attribution, Distinction, and Self-Defence' (2024) 68 <https://doi.org/10.2218/ccj.v5.9346> accessed 9 May 2025.

²⁰ Vakhtang Maisaia, Aliko Guchua and Tornike Zedelashvili, 'The Cybersecurity of Georgia and Threats from Russia' (2020) 9 *Eastern Review* 111 <https://doi.org/10.18778/1427-9657.09.07> accessed 9 May 2025.

or carried out by affiliated actors.²¹ It should also be noted that those attacks did not cause any physical damage.²²

The annexation of Crimea in 2014 and the full-scale invasion of Ukraine in 2022 saw an escalation in Russia's cyber warfare tactics.²³ Cyber operations targeted Ukraine's power grid, banking system, government institutions, and military network. The 2022 invasion featured more sophisticated cyberattacks, including wiper malware and satellite hacking, which demonstrated an evolution in Russia's cyber warfare strategy.²⁴ Today, it is safe to say that in 2008, Russia tested the ground for its future cyber operations.

1.4 Research question and structure

After careful consideration and exploration of different angles, the thesis research question has been designed as follows:

To what extent and in what way does Russia's cyber warfare challenge the application of international humanitarian law?

To address this question, the thesis is structured as follows:

- **Chapter 2** defines cyber warfare and examines how it is regulated under IHL.

²¹ Michael Connell and Sarah Vogler, 'The Challenge of Attribution for Cyber Attacks' (2016) https://www.cna.org/archive/CNA_Files/pdf/dop-2016-u-014231-1rev.pdf accessed 9 May 2025.

²² Andria Gotsiridze, 'The Cyber Dimension of the 2008 Russia-Georgia War' (GFSIS, 9 August 2019) <https://gfsis.org.ge/blog/view/970> accessed 9 May 2025.

²³ R Kolodii, 'The Pedagogy of Cyber-WAR: Explaining Ukraine's Resilience Against Russian Cyber-Aggression' (2024) 40(2) *Defense & Security Analysis* 270, 274–279 <https://doi-org.proxy.annalindhbiblioteket.se/10.1080/14751798.2024.2326313> accessed 9 May 2025.

²⁴ Aika Guchua and Tornike Zedelashvili, 'Challenges Arising from Cyber Security in the Dimension of Modern Global Security (on the Example of the Russia-Ukraine War)' (2022) 11(2) *Eastern Review* 83–84 <https://www.proquest.com/scholarly-journals/challenges-arising-cyber-security-dimension/docview/3126075929/se-2> accessed 9 May 2025.

- **Chapter 3** analyses the legal challenges in applying IHL to cyber warfare, including issues of attribution, the principle of distinction, and proportionality.
- **Chapter 4** explores the future of cyber warfare and IHL
- **Chapter 5** will conclude the final observations.

By examining these aspects, this thesis aims to contribute to the ongoing discussions on cyber warfare and international law, and to provide a critical assessment of whether existing legal norms are adequate for addressing cyber conflicts in the modern era.

2. Cyber Warfare and International Humanitarian Law

As mentioned in the introduction, in recent years, cyberspace became a fifth domain of warfare next to the traditionally recognized domains.²⁵ For IHL to remain effective, it must remain responsive to the context in which it applies.²⁶ Therefore, the question of to what extent existing international law applies to the cyber domain becomes more and more important. In this chapter, the thesis aims to answer what constitutes cyberattacks under IHL and how it is regulated under a current legal framework.

²⁵ Nils Melzer, *Cyberwarfare and International Law: Legal Challenges and Restraints* (Center for Security Studies 2011) 3 <https://unidir.org/publication/cyberwarfare-and-international-law/> accessed 9 May 2025.

²⁶ Ahmad Khalil, Mhd Bitar and S Anandha Krishna Raj, 'A New Era of Armed Conflict: The Role of State and Non-State Actors in Cyber Warfare with Special Reference to Russia-Ukraine War' (2024) 14(2) *TalTech Journal of European Studies* 50 https://www.researchgate.net/publication/386231399_A_New_Era_of_Armed_Conflict_The_Role_of_State_and_Non-State_Actors_in_Cyber_Warfare_with_Special_Reference_to_Russia-Ukraine_War accessed 9 May 2025.

2.1 The Legal Classification of Cyber Operations Under International Humanitarian Law

IHL was originally developed to regulate kinetic warfare, but over time, its broad and well-established formulation allowed it to adapt to evolving methods of warfare, including new technologies, like cyber operations.²⁷ Moreover, although IHL provisions do not explicitly mention cyber operations, it is widely accepted that when cyber operations are carried out in the context of and related to an armed conflict, they fall within the scope of IHL.²⁸

IHL regulates all forms of warfare, whether the means and methods are traditional or innovative. According to Article 49 of Additional Protocol I (AP I), an attack is defined as “acts of violence against the adversary, whether in offense or defense.”²⁹ The application of this definition to cyber warfare is not always easy because many cyber operations do not involve direct physical violence or destruction.³⁰ Traditionally, attacks under IHL have been understood as physical acts, such as bombing, shelling, shooting, that directly harm persons or objects.³¹ However, in cyber warfare, many operations involve disrupting or disabling digital infrastructure which often happens without kinetic effects.³² For example, a cyber operation that disables a hospital’s power

²⁷ Ibid 51-52 <https://doi.org/10.2478/bjes-2024-0016> accessed 9 May 2025.

²⁸ Cordula Droege, ‘Get Off My Cloud: Cyber Warfare, International Humanitarian Law, and the Protection of Civilians’ (2012) 94(886) *International Review of the Red Cross* 540 <https://international-review.icrc.org/sites/default/files/irrc-886-droege.pdf> accessed 9 May 2025.

²⁹ Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflicts (Protocol I) (adopted 8 June 1977, entered into force 7 December 1978) 1125 UNTS 3, art 49 https://www.icrc.org/sites/default/files/external/doc/en/assets/files/other/icrc_002_0321.pdf accessed 9 May 2025.

³⁰ Lilian O Aluede and Engr Peace B Biragbara, ‘Cyber Attack: An Emerging War’ (2020) 8(1) *GSJ* 301 https://www.researchgate.net/publication/338558828_CYBER_ATTACK_AN_EMERGING_WAR accessed 9 May 2025.

³¹ Nils Melzer, *Cyberwarfare and International Law: Legal Challenges and Restraints* (Center for Security Studies 2011) 21 <https://unidir.org/publication/cyberwarfare-and-international-law/> accessed 9 May 2025.

³² Michael N Schmitt (ed), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (2nd edn, Cambridge University Press 2017) 415–416

or communications system may not physically destroy anything, but could still endanger patients lives.³³

Some states and legal experts have different views on cyber operations that do not cause immediate physical damage but still impact civilian objects. For example, Germany defines cyberattacks more broadly, including harmful effects on communication, information, or electronic systems, even without physical damage.³⁴ France has offered a more detailed assessment. They consider that a cyber operation is an attack where the targeted equipment or systems no longer provide the service for which they were implemented, whether the disruption is temporary or permanent, reversible or irreversible.³⁵

Undoubtedly, the legal classification of a cyber attack against an information system as a use of force or as an armed attack is still problematic. The Tallinn Manual is a widely recognised but non-binding expert commentary on how international law applies to cyber operations, which explores how existing international law applies to cyber warfare.³⁶ Manual supports the broader view to a certain extent. Rule 69 of the manual states that a cyber operation can constitute a “use of force” if its effects are similar in scale and consequences to non-cyber military attacks.³⁷ Rule

<https://www.cambridge.org/core/books/tallinn-manual-20-on-the-international-law-applicable-to-cyber-operations/E4FFD83EA790D7C4C3C28FC9CA2FB6C9> accessed 9 May 2025.

³³ Michael N Schmitt, ‘International Humanitarian Law and the Conduct of Cyber Hostilities: Quo Vadis?’ (2022) 13(2) *International Humanitarian Legal Studies* 207 https://brill.com/view/journals/ihts/13/2/article-p189_002.xml accessed 9 May 2025.

³⁴ Federal Republic of Germany, *On the Application of International Law in Cyberspace* (10 October 2018) 8 https://ccdcoe.org/uploads/2018/10/Germany_on-the-application-of-international-law-in-cyberspace-data_English.pdf accessed 9 May 2025.

³⁵ Michael N Schmitt, ‘International Humanitarian Law and the Conduct of Cyber Hostilities: Quo Vadis?’ (2022) 13(2) *International Humanitarian Legal Studies* 207 https://brill.com/view/journals/ihts/13/2/article-p189_002.xml accessed 9 May 2025.

³⁶ Michael N Schmitt (ed), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (2nd edn, Cambridge University Press 2017) 1–6 <https://www.cambridge.org/core/books/tallinn-manual-20-on-the-international-law-applicable-to-cyber-operations/E4FFD83EA790D7C4C3C28FC9CA2FB6C9> accessed 9 May 2025.

³⁷ *Ibid* 330-337

92 affirms that cyber operations resulting in death, injury, or destruction qualify as attacks under IHL.³⁸ Rule 99 further clarifies that civilian objects cannot be targeted unless they have become military objectives.³⁹ While the experts contributing to the Manual could not reach a full consensus, they agreed that the permanent loss of functionality of targeted infrastructure may constitute an attack, even without physical damage.⁴⁰ ICRC also supports the broader interpretation. It argues that cyber operations leading to a loss of functionality, such as preventing a civilian system from working, should be classified as attacks under IHL.⁴¹

However, not all cyber operations fall within the scope of IHL. IHL applies only when cyber operations are conducted in the context of armed conflict.⁴² This means that peacetime cyber espionage or isolated cyber incidents do not automatically trigger IHL protections. But when cyberattacks are used in combination with traditional military force, they are subject to IHL.⁴³ A good example is the Russia-Georgia conflict in 2008, where cyberattacks on Georgian government and media websites occurred simultaneously with kinetic attacks by Russian forces.⁴⁴ In such a case, cyber operations are clearly part of the conduct of hostilities and should be governed by the same legal rules.

³⁸ Ibid 415

³⁹ Ibid 434-435

⁴⁰ Michael N Schmitt, 'International Humanitarian Law and the Conduct of Cyber Hostilities: Quo Vadis?' (2022) 13(2) *International Humanitarian Legal Studies* 207 https://brill-com.proxy.annalindhbiblioteket.se/view/journals/ihts/13/2/article-p189_002.pdf accessed 9 May 2025

⁴¹ International Committee of the Red Cross, 'International Humanitarian Law and Cyber Operations during Armed Conflicts' (2021) 102(913) *International Review of the Red Cross* 489 <https://international-review.icrc.org/sites/default/files/reviews-pdf/2021-03/ihl-and-cyber-operations-during-armed-conflicts-913.pdf> accessed 9 April 2025.

⁴² Ashutosh Pandey, 'Application of International Humanitarian Law in Changing Dimensions of Armed Conflict Vis-à-Vis Cyber Warfare' (2025) 6(1) *Unity Journal* 289-290 <https://doi.org/10.3126/unity.v6i1.75698> accessed 9 April 2025.

⁴³ Cordula Droege, 'Get Off My Cloud: Cyber Warfare, International Humanitarian Law, and the Protection of Civilians' (2012) 94(886) *International Review of the Red Cross* 542 <https://international-review.icrc.org/sites/default/files/irrc-886-droege.pdf> accessed 9 May 2025.

⁴⁴ Stephen W Kornis and Joshua E Kastenber, 'Georgia's Cyber Left Hook' (2008) 38(4) *Parameters* 60 <https://doi.org/10.55540/0031-1723.2455> accessed 9 May 2025.

Despite the effort to interpret existing rules in the cyber context, there is currently no binding international treaty that provides a definition of “cyber attack” or sets clear legal standards for cyber warfare.⁴⁵ Some scholars even argue that IHL, designed for conventional conflict, is ill-adapted to the cyber realm.⁴⁶ Some of them point to the absence of case law or customary law defining what constitutes a cyberattack,⁴⁷ and the fact that many cyber tools have effects that differ radically from traditional weapons. These critics argue that the existing framework cannot account for cyber operations that disrupt systems, data, or manipulate information without causing physical destruction.

It can also be argued that IHL is broad and flexible enough to accommodate new technologies.⁴⁸ Article 36 of the AP I obliges states to review new weapons to ensure they comply with IHL, this confirms that the law was designed to evolve.⁴⁹ The International Court of Justice’s (ICJ) 1996 advisory opinion on the legality of nuclear weapons reinforces this interpretation because it states that IHL applies to all forms of warfare and all weapons, whether existing or future.⁵⁰ That said, we still do not have clear consensus on how IHL works with cyber warfare. Without shared

⁴⁵ David Turns, ‘Cyber War and the Concept of Attack in International Humanitarian Law’ in Dan Saxon (ed), *International Humanitarian Law and the Changing Technology of War* (Brill Nijhoff 2013) 211 <https://research-ebSCO-com.proxy.annalindhbiblioteket.se/c/cxt7bo/search/view/uy76oqhtfv?db=e000xww> accessed 9 May 2025.

⁴⁶ Cordula Droege, ‘Get Off My Cloud: Cyber Warfare, International Humanitarian Law, and the Protection of Civilians’ (2012) 94(886) *International Review of the Red Cross* 540 <https://international-review.icrc.org/sites/default/files/irrc-886-droege.pdf> accessed 9 May 2025.

⁴⁷ David Turns, ‘Cyber War and the Concept of Attack in International Humanitarian Law’ in Dan Saxon (ed), *International Humanitarian Law and the Changing Technology of War* (Brill | Nijhoff 2013) 211 <https://research-ebSCO-com.proxy.annalindhbiblioteket.se/linkprocessor/plink?id=9cbd1ed3-cfdb-35e5-a8c1-f4d1592af99d> accessed 9 May 2025.

⁴⁸ Cordula Droege, ‘Get Off My Cloud: Cyber Warfare, International Humanitarian Law, and the Protection of Civilians’ (2012) 94(886) *International Review of the Red Cross* 540 <https://international-review.icrc.org/sites/default/files/irrc-886-droege.pdf> accessed 9 May 2025.

⁴⁹ Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflicts (Protocol I) (adopted 8 June 1977, entered into force 7 December 1978) 1125 UNTS 3, art 36 https://www.icrc.org/sites/default/files/external/doc/en/assets/files/other/icrc_002_0321.pdf accessed 9 May 2025.

⁵⁰ *Legality of the Threat or Use of Nuclear Weapons* (Advisory Opinion) [1996] ICJ Rep 226, para 86-87 <https://www.icj-cij.org/sites/default/files/case-related/95/095-19960708-ADV-01-00-EN.pdf> accessed 9 May 2025.

understanding on what is really a cyberattack under IHL, there is risk that different actors will interpret it differently. This brings us to the broader legal framework regulating cyber operations. While the Geneva Conventions (1949) and their Additional Protocols (1977) remain the primary sources of IHL, they do not contain specific rules about cyber operations.⁵¹ The non-binding Tallinn manual remains the most comprehensive effort to adapt IHL principles to the cyber domain, because its rules reflect key IHL concepts like distinction, proportionality, and military necessity, but as mentioned, the Manual lacks legal authority and states are not obligated to follow its guidance.⁵²

Moreover, the case law also provides some insight. The ICJ's judgment in *Nicaragua v. United States* (1986) established the principle that indirect uses of force, such as those carried out by proxy groups, may still constitute unlawful uses of force under international law.⁵³ This reasoning may apply to cyber operations, especially when states rely on non-state actors to conduct cyberattacks on their behalf. However, without a treaty or a clear standard for cyber attribution, holding states accountable remains difficult.

To summarise, IHL does apply to cyber operations conducted during armed conflict, but defining what counts as "cyberattack" is still legally unsettled. The lack of a binding treaty, combined with the evolution of technology and the difficulty of attribution, makes it hard to apply IHL principles in a consistent way. While the Tallinn Manual and state practice are helpful, they

⁵¹ Nils Melzer, *International Humanitarian Law: A Comprehensive Introduction* (ICRC 2019) 17–21 https://www.researchgate.net/profile/Etienne-Kuster/publication/313589999_New_IHL_handbook/links/62e3d2953c0ea8788765ee4e/New-IHL-handbook.pdf accessed 9 May 2025.

⁵² Shutosh Pandey, 'Application of International Humanitarian Law in Changing Dimensions of Armed Conflict Vis-à-Vis Cyber Warfare' (2025) 6(1) *Unity Journal* 290 <https://doi.org/10.3126/unityj.v6i1.75698> accessed 9 May 2025.

⁵³ *Military and Paramilitary Activities in and against Nicaragua (Nicaragua v United States of America)* (Merits) [1986] ICJ Rep 14 <https://www.icj-cij.org/sites/default/files/case-related/70/070-19860627-JUD-01-00-EN.pdf> accessed 9 May 2025.

cannot fully close the existing legal gaps. As cyber operations become a regular part of modern warfare, the need for legal clarity will grow stronger.

3. Legal Challenges in Applying IHL to Cyber Warfare

As mentioned above, IHL was developed to regulate traditional armed conflicts, where military operations involve soldiers, weapons, and physical attacks on the battlefield.⁵⁴ Modern warfare does not only look like this anymore, cyberattacks have become a regular part of armed conflicts, including the Russia-Georgia war in 2008 and the ongoing war in Ukraine. These cyber operations create many legal questions because IHL was not originally made to regulate this type of warfare. When, for example, a missile hits a hospital, it is clear that IHL has been violated, but what about a cyberattack that disables the same hospital's electricity? Is it also an attack under IHL? Who should be responsible if the attackers are anonymous hackers or patriotic volunteers? There are some legal challenges that cyber warfare creates, and they show why applying IHL to cyber attacks is so difficult in most cases.

One of the biggest challenges in cyber warfare is attribution, how do states prove that another state is responsible for a cyberattack?⁵⁵ Unlike kinetic attacks, cyber operations can be and are often carried out by many different actors, including non-state actors like hacktivist groups or

⁵⁴ Ahmad Khalil, Mhd Bitar and S Anandha Krishna Raj, 'A New Era of Armed Conflict: The Role of State and Non-State Actors in Cyber Warfare with Special Reference to Russia-Ukraine War' (2024) 14(2) *TalTech Journal of European Studies* 49–50 https://www.researchgate.net/publication/386231399_A_New_Era_of_Armed_Conflict_The_Role_of_State_and_Non-State_Actors_in_Cyber_Warfare_with_Special_Reference_to_Russia-Ukraine_War accessed 9 May 2025.

⁵⁵ Nicholas Tsagourias and Michael Farrell, 'Cyber Attribution: Technical and Legal Approaches and Challenges' (2020) 31(3) *European Journal of International Law* 944 <https://doi.org/10.1093/ejil/chaa057> accessed 9 May 2025.

proxy groups that may be supported financially or in other ways by a state.⁵⁶ Attribution is crucial in international law because, without proving who is behind the attack, it is impossible to hold any state accountable. This problem has been seen in Russia's cyberattacks against Georgia and Ukraine, because while those attacks were most likely state-directed, Russia denied any direct involvement, which triggered legal loopholes and allowed it to avoid any responsibility under international law.⁵⁷

Another key issue is related to the core principles of the IHL. For instance, IHL requires a distinction between civilian and military targets,⁵⁸ but in cyber warfare, this can be blurred. Cyberattacks on power grids, hospitals, and banking systems affect civilians even if the intended target is military. This raises legal concerns about collateral damage in cyberspace.⁵⁹ Yet another issue is connected to the principle of proportionality. Unlike conventional weapons, cyberattacks can have an unpredictable effect, for example, a virus targeting military infrastructure might spread to civilian systems.. This makes it difficult to ensure compliance with the principle of proportionality under IHL. Moreover, the principle of military necessity becomes even more complicated in cyber warfare because in cyber operations, it is often unclear whether the attack will really bring a concrete and direct military advantage.

⁵⁶ Hannah Gray, 'Cyberwarfare and the Challenges It Poses to the International Governance of Armed Conflict with Particular Reference to Attribution, Distinction, and Self-Defence' (2024) 65 <https://doi.org/10.2218/ccj.v5.9346> accessed 9 May 2025.

⁵⁷ Nina Jankowicz, *How to Lose the Information War: Russia, Fake News, and the Future of Conflict* (I.B. Tauris 2020) 61 <https://research.ebsco.com/linkprocessor/plink?id=79b2ec6e-d64d-3ef8-bd82-e165227f684f> accessed 9 May 2025.

⁵⁸ Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflicts (Protocol I) (adopted 8 June 1977, entered into force 7 December 1978) 1125 UNTS 3, art 48 https://www.icrc.org/sites/default/files/external/doc/en/assets/files/other/icrc_002_0321.pdf accessed 9 May 2025.

⁵⁹ Nils Melzer, *Cyberwarfare and International Law: Legal Challenges and Restraints* (Center for Security Studies 2011) 27-29 <https://unidir.org/publication/cyberwarfare-and-international-law/> accessed 9 May 2025.

This chapter aims to examine the evolving nature of cyber warfare and the legal complexities it presents under IHL. The following chapter and its sub-chapters will delve deeper into these challenges and try to answer the initial question.

3.1 The principle of distinction - Can cyberattacks distinguish between military and civilian targets?

IHL is based on the rules that protect civilians and regulate how wars are fought.⁶⁰ One of its key principles is the principle of distinction.⁶¹ According to Article 48 of the AP I, all parties to a conflict must distinguish at all times between civilian objects and military objectives and may only direct attacks at the latter.⁶² It is based on the recognition that the only legitimate object that states should try to accomplish during war is to weaken the military forces of the enemy, whereas the civilian population and individual civilians shall enjoy general protection against dangers arising from military operations.⁶³ Moreover, neither the civilian population nor individual civilians may be attacked unless and for such time as they directly participate in hostilities.⁶⁴ Attacks must be strictly limited to military objectives. Military objectives are those that make an

⁶⁰ Nils Melzer, *International Humanitarian Law: A Comprehensive Introduction* (ICRC 2019) 17 https://www.researchgate.net/profile/Etienne-Kuster/publication/313589999_New_IHL_handbook/links/62e3d2953c0ea8788765ee4e/New-IHL-handbook.pdf accessed 9 May 2025.

⁶¹ Ibid

⁶² Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflicts (Protocol I) (adopted 8 June 1977, entered into force 7 December 1978) 1125 UNTS 3, art 48 https://www.icrc.org/sites/default/files/external/doc/en/assets/files/other/icrc_002_0321.pdf accessed 9 May 2025.

⁶³ Nils Melzer, *International Humanitarian Law: A Comprehensive Introduction* (ICRC 2019) 19 https://www.researchgate.net/profile/Etienne-Kuster/publication/313589999_New_IHL_handbook/links/62e3d2953c0ea8788765ee4e/New-IHL-handbook.pdf accessed 9 May 2025.

⁶⁴ Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflicts (Protocol I) (adopted 8 June 1977, entered into force 7 December 1978) 1125 UNTS 3, art 51 https://www.icrc.org/sites/default/files/external/doc/en/assets/files/other/icrc_002_0321.pdf accessed 9 May 2025.

effective contribution to military action and whose destruction offers a military advantage.⁶⁵ However, if civilian objects are used for military purposes, like transporting weapons, they may be considered lawful targets.

While this seems clear in traditional warfare, it is much more complex in cyberspace. Cyber operations must also follow IHL and target only military objectives, such as networks that make an effective contribution to military operations.⁶⁶ Therefore, a “lawful” cyberattack is one that only attacks military cyber infrastructures, while civilian infrastructure, like public servers and data centers, should be protected.⁶⁷

But in reality, the principle of distinction becomes extremely hard to apply because military and civilian cyber systems are often connected to each other.⁶⁸ Many critical systems, such as power grids, telecommunication networks, or transport systems, are dual-use, which means that they can be used for both civilian and military purposes.⁶⁹ For example, data centers that are primarily used for civilians to store information will inevitably carry military data and information. Under IHL, this makes the civilian data center a military objective and a legitimate target of attack.⁷⁰ Cyberattacks often involve systemic consequences that are difficult to predict. For example, if a cyberattack disables a country’s electricity grid to disrupt military operations, it is very likely that civilian objects, such as hospitals, schools, and homes, will also be affected. This raises

⁶⁵ Ibid art 52(2)

⁶⁶ Nils Melzer, *Cyberwarfare and International Law: Legal Challenges and Restraints* (Center for Security Studies 2011) 29–32 <https://unidir.org/publication/cyberwarfare-and-international-law/> accessed 9 May 2025.

⁶⁷ Rohit Bokil, ‘Cyber Warfare: Taking War to Cyberspace and Its Implications for International Humanitarian Law’ (2023) *International Journal for Multidisciplinary Research* 6 <https://www.ijfmr.com/papers/2023/1/1494.pdf> accessed 9 May 2025.

⁶⁸ Nils Melzer, *Cyberwarfare and International Law: Legal Challenges and Restraints* (Center for Security Studies 2011) 30 <https://unidir.org/publication/cyberwarfare-and-international-law/> accessed 9 May 2025.

⁶⁹ Eitan Diamond, ‘Applying International Humanitarian Law to Cyber Warfare’ in Pnina Sharvit Baruch and Anat Kurz (eds), *Law and National Security: Selected Issues* (Institute for National Security Studies 2014) 77–78 <http://www.jstor.org/stable/resrep08957.8> accessed 9 May 2025.

⁷⁰ Zen Chang, ‘Cyberwarfare and International Humanitarian Law’ (2017) 9(1) *Creighton International and Comparative Law Journal* 38 <https://ssrn.com/abstract=2973182> accessed 9 May 2025.

serious legal concerns under IHL, which requires not only distinguishing between targets but also taking into account the indirect but foreseeable effects on the civilian population. In cyberspace, the principle of distinction sometimes holds little promise for the protection of civilian cyber infrastructure and all civilian infrastructures that rely on it.

The ICRC has raised concerns many times about the increasing use of cyber operations during armed conflicts, especially because of the risks they bring to civilians and the possible damage to civilian infrastructure⁷¹. In its 2020 report, ICRC emphasized that even in cyber operations, all IHL principles still apply.⁷² This also shows that technological complexity cannot serve as an excuse to disregard fundamental humanitarian obligations. Hannah Gray points out that cyberattacks usually target public services or websites that people use in daily life. They sometimes also aim to spread disinformation and perpetrate psychological warfare, which fails to distinguish between civilian and combatant targets clearly.⁷³ These types of operations, though non-kinetic, may still constitute unlawful attacks under IHL when they are designed to disrupt civilian life.

Looking at real-world examples will help understanding how the principle of distinction is challenged in cyber warfare. The Russia-Georgia war in 2008 was unique in the sense that it was the first time when cyber attacks were employed together with a large-scale military invasion in

⁷¹ International Committee of the Red Cross, 'International Humanitarian Law and Cyber Operations during Armed Conflicts' (2021) 102(913) *International Review of the Red Cross* 489 <https://international-review.icrc.org/sites/default/files/reviews-pdf/2021-03/ihl-and-cyber-operations-during-armed-conflicts-913.pdf> accessed 9 May 2025.

⁷² Laurent Gisel, Tilman Rodenhäuser and Knut Dörmann, 'Twenty Years On: International Humanitarian Law and the Protection of Civilians Against the Effects of Cyber Operations During Armed Conflicts' (2020) 102(913) *International Review of the Red Cross* 301 <https://international-review.icrc.org/sites/default/files/reviews-pdf/2021-03/twenty-years-ihl-effects-of-cyber-operations-during-armed-conflicts-913.pdf> accessed 9 May 2025..

⁷³ Hannah Gray, 'Cyberwarfare and the Challenges It Poses to International Governance of Armed Conflict' (2024) 67 <https://doi.org/10.2218/ccj.v5.9346> accessed 9 May 2025.

the context of warfare.⁷⁴ During the war, Russia invaded the three traditional battlefields, air, land, and sea, and by using their cyber operations, they were able to invade Georgian cyberspace as well.⁷⁵ They spread misinformation to cause panic in society, attacked English-language news portals, tried to create an information vacuum and prevent Georgian agencies from spreading information, also trying to spread Russian propaganda.⁷⁶ It could not be proven that the Russian government was involved, although the timing of the attacks strongly suggested that the Kremlin was at least supporting or enabling them.⁷⁷

By using various methods of cyber attacks, the hackers managed to get hundreds of Georgian web portals out of order, among them were the web pages of the President and the Parliament of Georgia.⁷⁸ The attacks also caused the national phone network to go offline, disrupted other public services like banking, and hindered Georgian government's communication ability.⁷⁹ The Russian hackers mostly used DDoS attacks, meaning that they used hundreds or thousands of botnets to generate huge floods of traffic and paralyze a target system, which were Georgian government websites and media platforms.⁸⁰ In addition, hackers also used SQL INJECTION method, which takes advantage of weak spots in web applications, harmful code is inserted into a

⁷⁴ Madelena Anna Miniats, 'War of Nerves: Russia's Use of Cyber Warfare in Estonia, Georgia and Ukraine' (2019) *Senior Projects Spring 2019* 44 <https://core.ac.uk/reader/232619240> accessed 9 May 2025.

⁷⁵ Garrett Van Epps, 'Common Ground: US and NATO Engagement with Russia in the Cyber Domain' (2013) 12(4) *Connections* 30 <http://www.jstor.org/stable/26326340> accessed 9 May 2025.

⁷⁶ Vladimeri Napetvaridze and Archil Chochia, 'Cybersecurity in the Making – Policy and Law: A Case Study of Georgia' (2019) 19(2) *International Comparative Law Review* 155, 161 <https://doi.org/10.2478/iclr-2019-0019> accessed 9 May 2025.

⁷⁷ Michael Connell and Sarah Vogler, *Russia's Approach to Cyber Warfare* (CNA 2017) 17–18 https://www.cna.org/archive/CNA_Files/dop/dop-2016-u-014231-1rev.pdf accessed 9 May 2025.

⁷⁸ Vladimeri Napetvaridze and Archil Chochia, 'Cybersecurity in the Making – Policy and Law: A Case Study of Georgia' (2019) 19(2) *International Comparative Law Review* 155, 160 <https://doi.org/10.2478/iclr-2019-0019> accessed 9 May 2025.

⁷⁹ Hannah Gray, 'Cyberwarfare and the Challenges It Poses to International Governance of Armed Conflict' (2024) 68 <https://doi.org/10.2218/ccj.v5.9346> accessed 9 May 2025.

⁸⁰ Vladimeri Napetvaridze and Archil Chochia, 'Cybersecurity in the Making – Policy and Law: A Case Study of Georgia' (2019) 19(2) *International Comparative Law Review* 155, 161 <https://doi.org/10.2478/iclr-2019-0019> accessed 9 May 2025.

website's form and this code tricks the website's database, which allows the hackers to change or steal the data.⁸¹

In the Russia-Georgia war context, although the cyber attacks did not cause death or injury, they had informational and psychological effects on Georgia and its citizens, as the hackers worked to spread the Russian narrative and isolate Georgia from the outside world.⁸² Russian cyber attacks in 2008 purposely targeted civilian infrastructure, which means that their use of cyber warfare potentially violated IHL, at least regarding distinction.

A more recent example of cyber warfare during armed conflict is the ongoing Russia-Ukraine war. The cyber dimension of this conflict, particularly in the 2022 full-scale invasion, is often described as the first wartime cyber conflict between two states with relatively well-matched cyber capabilities.⁸³ This makes Ukraine an important case study for understanding how cyber operations are integrated into modern warfare and how difficult it is to uphold the principle of distinction under IHL.

In the weeks before Russia's full-scale invasion, Ukraine faced a wave of cyberattacks aimed at disrupting public administration and spreading psychological fear among the population.⁸⁴ On January 13-14, 2022, Ukrainian government websites, including the Ministry of Education and Science, the cabinet ministries, and the Ministry of Energy, were hacked and temporarily taken

⁸¹ Paulo Shakarian, Jana Shakarian and Andrew Ruef, *Introduction to Cyber-Warfare: A Multidisciplinary Approach* (Syngress 2013) 24–25 <https://research-ebSCO-com.proxy.annalindhblibloteket.se/c/cxt7bo/ebook-viewer/epub/fkvy3baskf?location=https%3A%2F%2Fresearch-ebSCO-com.proxy.annalindhblibloteket.se%2Fc%2Fcxt7bo%2Fdetails%2Fkv3baskf> accessed 9 May 2025.

⁸² Hannah Gray, 'Cyberwarfare and the Challenges It Poses to International Governance of Armed Conflict' (2024) 69 <https://doi.org/10.2218/ccj.v5.9346> accessed 9 May 2025.

⁸³ Marcus Willet, 'The Cyber Dimension of the Russia–Ukraine War' (2022) 64(5) *Survival* 22 <https://doi.org/10.1080/00396338.2022.2126193> accessed 9 May 2025.

⁸⁴ *Ibid* 11

offline.⁸⁵ This attack carried clear pre-conflict signaling value. Since the beginning of the war in 2022, Russian cybercriminals and government-affiliated hacking groups have targeted Ukrainian civilian services, such as government agencies, energy infrastructure, and media outlets⁸⁶. These attacks aim not only to disable systems but also to spread disinformation and weaken public morale. According to Markus Takama and Martti Lehto, between January 2022 and September 2023, 174 cyberattacks were documented, with 71,3% being DDoS attacks. Public administration was the most targeted sector between July and September 2022.⁸⁷

One of the most serious cyberattacks occurred one hour before Russia's full-scale invasion began.⁸⁸ The Viasat Satellite system was targeted, likely aiming at Ukrainian military communications, but the attack also disrupted civilian users across Europe, including wind farms and private broadband customers. Over 30,000 internet connections were knocked offline, and 5,000 wind turbines in Germany lost remote control access.⁸⁹ This attack vividly demonstrated the blurring of civilian and military targets, a direct challenge to the principle of distinction under IHL. Later, on December 19, 2024, Ukraine suffered its most massive external cyberattack on

⁸⁵ Iryna Fyshchuk, Mette Strange Noesgaard and Jeppe Agger Nielsen, 'Managing Cyberattacks in Wartime: The Case of Ukraine' (2024) *Public Administration Review* 1, 3 <https://doi.org/10.1111/puar.13895> accessed 9 May 2025.

⁸⁶ Hannah Gray, 'Cyberwarfare and the Challenges It Poses to International Governance of Armed Conflict' (2024) 71 <https://doi.org/10.2218/ccj.v5.9346> accessed 9 May 2025.

⁸⁷ Markus Takama and Martti Lehto, 'Cyber Operations in Ukraine: Emerging Patterns in Cases' in *Proceedings of the 23rd European Conference on Cyber Warfare and Security* (2024) 785 <https://papers.academic-conferences.org/index.php/eccws/article/view/2122/2123> accessed 9 May 2025.

⁸⁸ UK Government, 'Russia Behind Cyber Attack with Europe-Wide Impact an Hour Before Ukraine Invasion' (Gov.uk, 2022) <https://www.gov.uk/government/news/russia-behind-cyber-attack-with-europe-wide-impact-an-hour-before-ukraine-invasion> accessed 9 May 2025.

⁸⁹ Ahmad Khalil, Mhd Bitar and S Anandha Krishna Raj, 'A New Era of Armed Conflict: The Role of State and Non-State Actors in Cyber Warfare with Special Reference to Russia-Ukraine War' (2024) 14(2) *TalTech Journal of European Studies* 49–50 https://www.researchgate.net/publication/386231399_A_New_Era_of_Armed_Conflict_The_Role_of_State_and_Non-State_Actors_in_Cyber_Warfare_with_Special_Reference_to_Russia-Ukraine_War accessed 9 May 2025.

state registers, that affected core government databases under the Ministry of Justice.⁹⁰ Ukrainian officials directly attributed this attack to Russia, and framed it as an effort to disrupt critical infrastructure and civil administration. According to the Deputy Prime Minister for European and Euro-Atlantic Integration, Olha Stefanishyna, “As a result of the targeted attack, the operation of the Unified and State Registers under the jurisdiction of the Ministry of Justice of Ukraine was temporarily suspended.”⁹¹ She also stated that this cyberattack was carried out by Russians to disrupt the operation of the state’s critical infrastructure.⁹²

The Ukraine case clearly illustrates how cyber operations make it extremely difficult to distinguish between military and civilian targets, especially when critical national infrastructure plays both civilian and military roles. These examples directly challenge the application of IHL, as the principle of distinction is fundamental to protecting civilians during armed conflict.

3.2 The principle of proportionality - How can cyberattacks be assessed for excessive harm?

Another core principle of international humanitarian law is the principle of proportionality.⁹³ Where the infliction of incidental harm on civilians or civilian objects cannot be avoided, it is subject to the principle of proportionality.⁹⁴ The principle of proportionality becomes especially

⁹⁰ Ukrainska Pravda, ‘Russian Hackers Attack State Systems before Presidential Elections’ (20 December 2024) <https://www.pravda.com.ua/eng/news/2024/12/20/7489933/> accessed 9 May 2025.

⁹¹ Politico, ‘Ukraine Blames Russia for Cyberattack on Critically Important Infrastructure’ (Politico, 2024) <https://www.politico.eu/article/ukraine-blames-russia-for-cyberattack-on-critically-important-infrastructure-olha-stefanishyna/> accessed 9 May 2025.

⁹² Ibid

⁹³ Nils Melzer, *International Humanitarian Law: A Comprehensive Introduction* (ICRC 2019) 100-102 https://www.researchgate.net/profile/Etienne-Kuster/publication/313589999_New_IHL_handbook/links/62e3d2953c0ea8788765ee4e/New-IHL-handbook.pdf accessed 9 May 2025.

⁹⁴ Ibid 19

complex in cyber warfare, where the dual-use nature of most digital infrastructure complicates both target selection and harm assessment.

According to article 51(5)(b) of the AP I, the indiscriminate attack is “an attack which may be expected to cause incidental loss of civilian life, injury to civilians, damage to civilian objects, or a combination thereof, which would be excessive in relation to the concrete and direct military advantage anticipated.”⁹⁵ As Nils Melzer mentioned in his book, the key term to be examined in the proportionality equation is “excessive.”⁹⁶ IHL does not establish an objective threshold above which the infliction of incidental harm would be excessive and this vagueness creates a significant challenge when evaluating proportionality, especially in a cyber context where damage is often indirect, delayed, or intangible.

Nils Melzer further asserts that a proper proportionality assessment must include not only immediate consequences but also the foreseeable second and third-order effects of cyberattacks. For instance, attacks against dual-use infrastructure, such as targeting an electricity grid or telecommunication network, may seem justifiable if used for military purposes, but its shutdown could also deprive civilians of essential services such as hospital access, public safety alerts, clean water, etc., thereby leading to excessive harm. The case of Ukraine has shown exactly this pattern of disruption.⁹⁷

⁹⁵ Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflicts (Protocol I) (adopted 8 June 1977, entered into force 7 December 1978) 1125 UNTS 3, art 51(5)(b) https://www.icrc.org/sites/default/files/external/doc/en/assets/files/other/icrc_002_0321.pdf accessed 9 May 2025.

⁹⁶ Nils Melzer, *International Humanitarian Law: A Comprehensive Introduction* (ICRC 2019) 101 https://www.researchgate.net/profile/Etienne-Kuster/publication/313589999_New_IHL_handbook/links/62e3d2953c0ea8788765ee4e/New-IHL-handbook.pdf accessed 9 May 2025.

⁹⁷ *Ibid* 102

Another author argues that proportionality also applies to the indirect effects of an attack.⁹⁸ A cyber attack is responsible for the indirect effects on a civilian population caused by an attack on the control system of an electrical generator. Additionally, article 56 of the AP I states that “works or installations containing dangerous forces, namely dams, dykes and nuclear electrical generating stations, shall not be the object of an attack, even where those objects are military objectives, if such attack may cause the release of dangerous forces and consequent severe losses among the civilian population.”⁹⁹ States tend to have different approach towards this issue. For example, the US takes the view that “remote harms resulting from the attack do not need to be considered in a proportionality analysis,” while the UK maintains that “regard must also be had to the foreseeable effects of the attack.”¹⁰⁰

One of the legal uncertainties lies in the definition of what counts as “damage” in cyber contexts. If a cyber operation results in the same effect as would a kinetic attack, then it is safe to say that the damage occurred.¹⁰¹ However, many cyber operations have not resulted in the same effects as kinetic force. For example, in the case of Georgia, Russia’s cyberattacks caused psychological terror and fear in society, but they did not cause any physical damage.¹⁰² These effects, while non-kinetic, arguably still contributed to civilian harm and raised questions under the principle of proportionality,

⁹⁸ Rohit Bokil, ‘Cyber Warfare: Taking War to Cyberspace and Its Implications for International Humanitarian Law’ (2023) *International Journal for Multidisciplinary Research* 8 <https://www.ijfmr.com/papers/2023/1/1494.pdf> accessed 9 May 2025.

⁹⁹ Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflicts (Protocol I) (adopted 8 June 1977, entered into force 7 December 1978) 1125 UNTS 3, art 56 https://www.icrc.org/sites/default/files/external/doc/en/assets/files/other/icrc_002_0321.pdf accessed 9 May 2025.

¹⁰⁰ Zen Chang, ‘Cyberwarfare and International Humanitarian Law’ (2017) 9(1) *Creighton International and Comparative Law Journal* 44 <https://ssrn.com/abstract=2973182> accessed 9 May 2025.

¹⁰¹ *Ibid* 42

¹⁰² Heather Harrison Dinniss, *Cyber Warfare and the Laws of War* (Cambridge University Press 2012) 2 <https://research-ebSCO-com.proxy.annalindhblibioteket.se/linkprocessor/plink?id=f63d7260-304c-3725-a488-b600328c5879> accessed 9 May 2025.

In December 2023 Kyivstar, Ukraine's largest telecommunications provider, was targeted by Russian cyber operations. Russian-affiliated hackers launched a destructive cyber operation targeting the core systems of Kyivstar.¹⁰³ This company provides phone and internet services to more than 24 million people, and essential communication infrastructure for the Ukrainian Armed Forces and government agencies.¹⁰⁴ When this system was attacked, it caused a broadscale disruption, air raid alarms did not go off, financial systems were down, and people could not pay for buses. These problems were not accidents. They could have been expected, given Kyivstar's obvious importance to civilian life. On the one hand, if Kyivstar's military communications were the primary target, there could be a military advantage in degrading Ukraine's capabilities, on the other hand, the widespread harm to civilians, who were cut out off from emergency warning, financial services, and basic communications, raises questions about whether this incidental civilian harm outweighed the anticipated military benefit. As mentioned, some targets have dual-use meanings, which may be lawfully targeted if they make an effective contribution to military action, but the attackers must minimize civilian harm. In this case, the scale of disruption to civilian life highlights the risk that the attack violated the principle of proportionality.

The 2017 NotPetya malware attack against Ukraine presents another striking illustration. Although there was no formally declared international armed conflict (IAC)¹⁰⁵ in Ukraine at that time, the country was engaged in a broader ongoing hostilities with Russia, which began with the

¹⁰³ BBC News, 'Ukraine Cyber-Attack: Kyivstar Boss Says Hackers Destroyed Everything' (BBC, 29 December 2023) <https://www.bbc.com/news/world-europe-67691222> accessed 9 May 2025.

¹⁰⁴ Ahmad Khalil, Mohammad Bitar and S Anandha Krishna Raj, 'A New Era of Armed Conflict: The Role of State and Non-State Actors in Cyber Warfare with Special Reference to Russia-Ukraine War' (2024) 14(2) *TalTech Journal of European Studies* 63 <https://doi.org/10.2478/bjes-2024-0016> accessed 9 May 2025.

¹⁰⁵International Committee of the Red Cross (ICRC), Article 2 <https://ihl-databases.icrc.org/en/ihl-treaties/gci-1949/article-2> accessed 9 May 2025.

annexation of Crimea in 2014¹⁰⁶ and continued with the conflict in Eastern Ukraine, it can be argued that there was a connection between this cyber attack and an armed conflict.¹⁰⁷ NotPetya was first designed to hit Ukrainian government, banks, airports, and infrastructure.¹⁰⁸ But the malware spread fast and even affected countries outside Ukraine. The plan was to damage Ukrainian systems that were seen as military targets during the conflict with Russia, but the damage went beyond that.¹⁰⁹

When we look at it from proportionality rule under IHL, the main legal question is if the military gain from damaging Ukrainian systems was more than the harm done to civilians, businesses, and other countries. NotPetya spread uncontrollably, which shows just how difficult it is to control cyberweapons. It makes it harder to meet proportionality requirements when attackers cannot control it.

In conclusion, the principle of proportionality in cyber warfare raises complex legal and operational challenges. Cyberattacks, especially when directed at dual-use systems, risk producing widespread and often unintended harm. The cases of NotPetya and Kyivstar highlight the difficulty of assessing proportionality when digital weapons cannot be precisely controlled. These examples demonstrate that without better predictive capabilities and stricter legal accountability, the principle of proportionality will remain difficult to uphold in cyberspace.

¹⁰⁶ Geneva Academy of International Humanitarian Law and Human Rights, 'Military Occupation of Ukraine' (RULAC, 2024) <https://www.rulac.org/browse/conflicts/military-occupation-of-ukraine> accessed 9 May 2025.

¹⁰⁷ Michael Schmitt and Lieutenant Colonel Jeffrey Biller, 'The NotPetya Cyber Operation as a Case Study of International Law' (*EJIL: Talk!*, 6 August 2020) <https://www.ejiltalk.org/the-notpetya-cyber-operation-as-a-case-study-of-international-law/> accessed 9 May 2025.

¹⁰⁸ Paul Hannon, 'The Day a Mysterious Cyber-Attack Crippled Ukraine' (BBC Future, 4 July 2017) <https://www.bbc.com/future/article/20170704-the-day-a-mysterious-cyber-attack-crippled-ukraine> accessed 9 May 2025.

¹⁰⁹ Andy Greenberg, 'The Untold Story of NotPetya, the Most Devastating Cyberattack in History' (Wired, 22 August 2018) <https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/> accessed 9 May 2025.

3.3 The principle of necessity - Are cyberattacks militarily necessary or excessive?

IHL is based on the balance between military necessity and humanity, ensuring that belligerents use force only to achieve legitimate military objectives.¹¹⁰ IHL recognizes that to defeat an adversary, it may be unavoidable to cause death, injury, or destruction and even to impose harsh security measures that would not be acceptable in peacetime.¹¹¹

According to the AP I, military necessity dictates that an attack must be directed at military objectives that offer a concrete and direct military advantage, and the target's nature, location, purpose or use should contribute effectively to military action and its neutralisation should offer a concrete benefit.¹¹² However, cyber operations do not always cause direct physical damage, they can disrupt communications, financial systems, or infrastructure without kinetic destruction, which may still significantly impact military operations and civilian life.

The Tallinn Manual 2.0 states that cyber capabilities should be assessed like traditional weapons when determining their necessity, they must be evaluated based on their military advantage versus the humanitarian consequences.¹¹³ Some cyberattacks can have long-term cascading

¹¹⁰ Nils Melzer, *International Humanitarian Law: A Comprehensive Introduction* (ICRC 2019) 17 https://www.researchgate.net/profile/Etienne-Kuster/publication/313589999_New_IHL_handbook/links/62e3d2953c0ea8788765ee4e/New-IHL-handbook.pdf accessed 9 May 2025.

¹¹¹ Ibid 17-18

¹¹² Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflicts (Protocol I) (adopted 8 June 1977, entered into force 7 December 1978) 1125 UNTS 3, art 52(2). https://www.icrc.org/sites/default/files/external/doc/en/assets/files/other/icrc_002_0321.pdf accessed 9 May 2025.

¹¹³ Michael N Schmitt (ed), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (2nd edn, Cambridge University Press 2017) 436-445 <https://www.cambridge-org.proxy.annalindhbiblioteket.se/core/books/tallinn-manual-20-on-the-international-law-applicable-to-cyber-operations/E4FFD83EA790D7C4C3C28FC9CA2FB6C9> accessed 9 May 2025.

effects beyond the battlefield. In cyber warfare, many operations target interconnected civilian and military infrastructure. For example, a cyber attack that targets an adversary's military computer systems satisfies the condition of military necessity by their exclusive military association.¹¹⁴ Whether the target creates a definite military advantage is a complicated issue. It is possible that many cyber attackers would not know the possible effects of cyber attacks; for example, an attacker that penetrates the computer systems of an electrical generator might gain a military advantage, but the system may have unforeseen layers that prevent such an advantage from occurring. In this case, the military advantage is not definite enough to satisfy the condition of military necessity. Moreover, it is very hard to tell beforehand whether a successful cyber attack will create a definite military advantage. The challenge lies in determining whether a cyberattack is the least harmful option to achieve a military objective and whether the resulting harm to civilians is justified under IHL.

For the cyberattack to meet the necessity requirement, the cyber operation must therefore satisfy three criteria: (1) the target must be a legitimate military objective, (2) the action must be necessary to achieve a specific and tangible military gain and (3) there must not be a less harmful alternative capable of achieving the same effect.

The cyberattack on Kyivstar illustrates the dilemma. Kyivstar, as mentioned above, plays a dual-use role in national defense and civilian life.¹¹⁵ Disabling the core systems significantly affected emergency warning networks, mobile communications, and digital infrastructure relied

¹¹⁴ Rohit Bokil, 'Cyber Warfare: Taking War to Cyberspace and Its Implications for International Humanitarian Law' (2023) *International Journal for Multidisciplinary Research* 6 <https://www.ijfmr.com/papers/2023/1/1494.pdf> accessed 9 May 2025.

¹¹⁵ BBC News, 'Ukraine Cyber-Attack: Kyivstar Boss Says Hackers Destroyed Everything' (BBC, 29 December 2023) <https://www.bbc.com/news/world-europe-67691222> accessed 9 May 2025.

on by civilians and the Ukrainian Armed Forces.¹¹⁶ If the attackers aimed to degrade military capabilities, the operation might have fulfilled the first element of the military necessity test. But given the widespread civilian harm, the question becomes whether a narrower or alternative attack against strictly military systems could have achieved the same goal with fewer humanitarian consequences.

It seems like balancing the military necessity and humanity in cyber warfare remains an issue, as cyber operations often lack a clear distinction between military and civilian infrastructure, and the effects of cyberattacks must be carefully weighed under IHL to ensure that they are not excessive. The case of Kyivstar clearly highlights the challenge in applying this principle.

In conclusion, the principle of military necessity in cyber warfare must be approached with caution. The digital nature of cyber operations, combined with the unpredictability of its nature, makes it difficult to ensure that operations are both necessary and legal. As the Kyivstar case demonstrates, achieving a military advantage cannot justify attacks that cause broad and foreseeable civilian disruption, especially if less harmful alternatives may exist. As cyber operations continue to evolve, military necessity should be interpreted through a lens that reflects both technological reality and humanitarian limits.

¹¹⁶ NTT Security, 'Russian Hacker Claims Responsibility for Massive Cyberattack in Ukraine' (NTT Security, 22 December 2024) <https://se.security.ntt/en/russian-hacker-claims-responsibility-for-massive-cyberattack-in-ukraine/> accessed 9 May 2025.

3.4 Attribution challenges - How can states be held accountable for cyberattacks under IHL?

Unlike conventional warfare, where military actions and the responsible parties are often clear, in cyberspace it is hard to identify the actors behind attacks and determine whether they can be held accountable under international law.¹¹⁷

One of the most significant issues in applying IHL to cyber warfare is attribution, the process of identifying the entity or state responsible for a cyberattack.¹¹⁸ In traditional military operations, armed forces operate under state command, which makes attribution relatively easy. However, in the cyber domain, operations are often conducted by proxy groups or individual hackers who may or may not have ties to a government.¹¹⁹ The attackers are able to hide their origins and make it difficult to determine whether the attack can be attributed to a specific state because of its decentralized nature.¹²⁰ This, in turn, complicates the process of holding states accountable under IHL.

As Nils Melzer explains, in international law, if someone acts under the control of a state, their actions can be counted as the state's actions.¹²¹ These people are called "state agents." But if

¹¹⁷ Nicholas Tsagourias and Michael Farrell, 'Cyber Attribution: Technical and Legal Approaches and Challenges' (2020) 31(3) *European Journal of International Law* 944 <https://doi.org/10.1093/ejil/chaa057> accessed 9 May 2025.

¹¹⁸ Eitan Diamond, 'Applying International Humanitarian Law to Cyber Warfare' in Pnina Sharvit Baruch and Anat Kurz (eds), *Law and National Security: Selected Issues* (Institute for National Security Studies 2014) 72 <http://www.jstor.org/stable/resrep08957.8> accessed 9 May 2025.

¹¹⁹ Cordula Droege, 'Get Off My Cloud: Cyber Warfare, International Humanitarian Law, and the Protection of Civilians' (2012) 94(886) *International Review of the Red Cross* 544 <https://international-review.icrc.org/sites/default/files/irrc-886-droege.pdf> accessed 9 May 2025.

¹²⁰ Rohit Bokil, 'Cyber Warfare: Taking War to Cyberspace and Its Implications for International Humanitarian Law' (2023) *International Journal for Multidisciplinary Research* 4 <https://www.ijfmr.com/papers/2023/1/1494.pdf> accessed 9 May 2025.

¹²¹ Nils Melzer, *Cyberwarfare and International Law* (Center for Security Studies 2011) 10 <https://unidir.org/publication/cyberwarfare-and-international-law/> accessed 9 May 2025.

people or groups act alone and do not have strong connection to a state, they are "non-state actors."¹²² This chapter focuses on the role of non-state actors in cyber operations and the legal principles governing the attribution of their actions to states.

Attribution is a fundamental requirement for establishing state responsibility under international law.¹²³ Michael Schmitt notes that there are clear conditions that must be met to say that a non-state actor is controlled by the state.¹²⁴ Additionally, for a state to be held liable, the act in question must constitute an internationally wrongful act under international law. Attribution is a multi-layered process that extends beyond forensic evidence and requires legal, political, and strategic assessments to determine state responsibility.¹²⁵

Legal attribution can be categorized into direct and indirect attribution. As Eric Mejjia argues, direct attribution holds a state liable for the acts or omissions of individuals exercising its authority and acting as an extension of state power.¹²⁶ Indirect attribution, on the other hand, involves acts or omissions by non-state actors that are generally not attributable to a state but may engage state responsibility if the state fails to exercise "due diligence" in preventing, stopping, or responding to such acts.¹²⁷

¹²² Ibid

¹²³ International Law Commission, 'Draft Articles on Responsibility of States for Internationally Wrongful Acts' (2001) art 2 https://legal.un.org/ilc/texts/instruments/english/draft_articles/9_6_2001.pdf accessed 9 May 2025.

¹²⁴ Michael N Schmitt, 'Cybersecurity and International Law' in Robin Geiß and Nils Melzer (eds), *The Oxford Handbook of the International Law of Global Security* (Oxford University Press 2021; online edn, 10 March 2021) 674–675 <https://academic-oup-com.proxy.annalindhbiblioteket.se/edited-volume/41308/chapter/352055679> accessed 9 May 2025.

¹²⁵ Kosmas Pipyros *et al*, 'Cyberoperations and International Humanitarian Law: A Review of Obstacles in Applying International Law Rules in Cyber Warfare' (2016) 24(1) *Information and Computer Security* 38, 47 <https://www.proquest.com/docview/2093306070?accountid=8325&sourcetype=Scholarly%20Journals> accessed 9 May 2025.

¹²⁶ E F Mejjia, 'Act and Actor Attribution in Cyberspace: A Proposed Analytic Framework' (2014) 8(1) *Strategic Studies Quarterly* 114, 118 <http://www.jstor.org/stable/26270607> accessed 9 May 2025.

¹²⁷ Ibid

The Articles on Responsibility of States for Internationally Wrongful Acts (ARSIWA), adopted by the International Law Commission (ILC) and endorsed by the United Nations General Assembly (UNGA) in 2001, provide a key framework for determining state responsibility in cyberspace.¹²⁸ Article 1 of ARSIWA establishes the foundational principle that "every internationally wrongful act of a State entails the international responsibility of that State."¹²⁹ Article 2 outlines two essential criteria for state responsibility: first, an act must constitute a breach of an international obligation; second, the breach must be attributable to the state under international law.¹³⁰ These criteria present significant challenges in cyber warfare, where cyber operations are frequently conducted by independent groups, hacktivists, or government-affiliated cyber units because it complicates direct attribution.

Generally, cyber operations conducted by private individuals or groups are not attributable to states.¹³¹ However, Article 8 of ARSIWA, which embodies customary international law, stipulates that "the conduct of a person or group of persons shall be considered an act of a State under international law if the person or group of persons is, in fact, acting on the instructions of, or under the direction or control of, that State in carrying out the conduct."¹³² This means that if a non-state actor carries out a cyber operation under a state's instruction, direction, or control, the act becomes attributable to that state. The crucial element here is the level of connection between the state and the actors conducting the cyber operation.

¹²⁸ International Law Commission, 'Draft Articles on Responsibility of States for Internationally Wrongful Acts' (2001) https://legal.un.org/ilc/texts/instruments/english/draft_articles/9_6_2001.pdf accessed 9 May 2025.

¹²⁹ Ibid art 1

¹³⁰ Ibid art 2

¹³¹ Michael N Schmitt (ed), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (2nd edn, Cambridge University Press 2017) 95 <https://www.cambridge.org/core/books/tallinn-manual-20-on-the-international-law-applicable-to-cyber-operations/E4FFD83EA790D7C4C3C28FC9CA2FB6C9> accessed 9 May 2025.

¹³² International Law Commission, 'Draft Articles on Responsibility of States for Internationally Wrongful Acts' (2001) art 8 https://legal.un.org/ilc/texts/instruments/english/draft_articles/9_6_2001.pdf accessed 9 May 2025.

The Tallinn Manual 2.0, which builds upon ARSIWA, provides additional guidance on attribution in cyberspace. Rule 17 of the Tallinn Manual reflects Article 8 of ARSIWA and states that cyber operations conducted by a non-state actor are attributable to a state when they are:

- Conducted pursuant to its instructions or under its direction or control, or
- Acknowledged and adopted by the state as its own.¹³³

This rule highlights that states may bear responsibility for cyber operations conducted by non-state actors, such as individual hackers, criminal organizations engaged in cybercrime, cyber terrorists, or insurgent groups if they exert a sufficient degree of control over these actors.¹³⁴ The rule should be analyzed in combination with the legal doctrines of "effective control" and "overall control," which are central to assessing whether a state has sufficient influence over non-state cyber actors to be held accountable for their actions.

Rule 14 of the Tallinn Manual further states that "a state bears international responsibility for a cyber-related act that is attributable to the state and that constitutes a breach of an international legal obligation."¹³⁵ This principle aligns with Article 2 of ARSIWA, which specifies that an internationally wrongful act consists of an action or omission that:

1. Constitutes a breach of an international legal obligation applicable to that state, and
2. Is attributable to the state under international law.

¹³³ Michael N Schmitt (ed), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (2nd edn, Cambridge University Press 2017) 95 <https://www.cambridge.org/core/books/tallinn-manual-20-on-the-international-law-applicable-to-cyber-operations/E4FFD83EA790D7C4C3C28FC9CA2FB6C9> accessed 9 May 2025.

¹³⁴ Ibid

¹³⁵ Ibid 84

The absence of either element precludes state responsibility for the act in question.¹³⁶ The ICJ has reaffirmed the customary nature of this principle in several cases, including the Nicaragua Case, which set an important precedent on state attribution in conflicts involving non-state actors. The Tallinn Manual 2.0 also expands this concept by stating that a state can bear responsibility for acts beyond direct cyber operations, including cases where it makes its cyber infrastructure available to non-state groups, fails to take necessary measures to prevent cyber operations originating from its territory, or provides material support, such as hardware or software, to facilitate cyberattacks.¹³⁷

The ICJ and the International Criminal Tribunal for the former Yugoslavia (ICTY) have taken different approaches to the question of attributing internationally wrongful acts conducted by non-state actors to a state. While the ICJ applies a stricter effective control test, the ICTY introduced a more flexible overall control test, which allows for a broader attribution of responsibility.

Effective Control

The effective control test was developed by the International Court of Justice (ICJ) in the Nicaragua v. United States (1986) judgment and it is a standard for attributing actions of non-state actors to a state.¹³⁸ According to the ICJ, a state can be held responsible only if it has direct and specific control over the operations of the group.¹³⁹ While the Contras depended on US funding and supplies, the court concluded that their violations of international humanitarian law

¹³⁶ Ibid 84

¹³⁷ Ibid 84-85

¹³⁸ *Military and Paramilitary Activities in and against Nicaragua (Nicaragua v United States of America)* (Merits) [1986] ICJ Rep 14
<https://www.icj-cij.org/sites/default/files/case-related/70/070-19860627-JUD-01-00-EN.pdf> accessed 9 May 2025.

¹³⁹ Ibid paras 108; 115

could not be attributed to the US unless there was proof of specific operational control over their unlawful acts.¹⁴⁰ This means that the state must not only provide general support, such as funding or training, but must also direct or enforce the specific unlawful actions carried out by the non-state actor, and in this case the court said that financial support alone was insufficient to establish state responsibility.¹⁴¹ This test is important to decide when a state becomes responsible for acts committed by non-state actors. A state may be held accountable or even become a legitimate target if it exerts direct control over non-state actors engaged in hostile activities against another state. However, this test sets a high threshold for attribution, as it requires clear evidence that the state was directly involved in planning, coordinating, or approving specific operations.

This is very important in the cyber context because states often use hacker groups or proxies who act with different degrees of state involvement. The Tallinn Manual 2.0 applies the effective control test to cyber operations. Rule 17 says that state's general support is not enough to establish attribution.¹⁴² The manual also says that many of these hacker groups work semi-independently, and states often deny their connection even when they benefit from the results.¹⁴³ For example, during the war in Georgia, Russia denied all involvement in cyber attacks, and the attribution became very difficult.¹⁴⁴ Even if a state gives malware or cyber infrastructure, this does not mean the state is responsible, it has to be proven that the state also

¹⁴⁰ *Ibid* paras 110-112

¹⁴¹ *Ibid* paras 109-110

¹⁴² Michael N Schmitt (ed), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (2nd edn, Cambridge University Press 2017) 95-100 <https://www.cambridge.org/core/books/tallinn-manual-20-on-the-international-law-applicable-to-cyber-operations/E4FFD83EA790D7C4C3C28FC9CA2FB6C9> accessed 9 May 2025.

¹⁴³ *Ibid* 99

¹⁴⁴ Nina Jankowicz, *How to Lose the Information War: Russia, Fake News, and the Future of Conflict* (I.B. Tauris 2020) 61 <https://research.ebsco.com/linkprocessor/plink?id=79b2ec6e-d64d-3ef8-bd82-e165227f684f> accessed 9 May 2025.

approved or directed the specific operation.¹⁴⁵ The ICJ also explained that support like weapons or training is not enough, what matters is if the state was directly involved in unlawful acts.¹⁴⁶

Legal scholars such as François Delerue think that the effective control test is a strict rule for attributing responsibility.¹⁴⁷ It is very difficult to prove that a government controlled a hacker group directly. The Tallinn Manual shows this problem and says that international law may need to adapt or change to respond to these new challenges.¹⁴⁸

Overall control

In the Tadić case, the Appeals Chamber of the ICTY adopted a different approach. The difference was in introducing the overall control test. This test is thought to be more flexible and less restrictive than the effective control test set by the ICJ in Nicaragua. The overall control test was established in the ICTY case Prosecutor v. Tadić (1999) to determine when the actions of a non-state actor can be attributed to a state.¹⁴⁹ Dusko Tadic, a Bosnian Serb, was tried for crimes committed in 1992 at several detention camps in Prijedor.

¹⁴⁵ Michael N Schmitt (ed), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (2nd edn, Cambridge University Press 2017) 91 <https://www.cambridge.org/core/books/tallinn-manual-20-on-the-international-law-applicable-to-cyber-operations/E4FFD83EA790D7C4C3C28FC9CA2FB6C9> accessed 9 May 2025.

¹⁴⁶ *Military and Paramilitary Activities in and against Nicaragua (Nicaragua v United States of America)* (Merits) [1986] ICJ Rep 14, para 115 <https://www.icj-cij.org/sites/default/files/case-related/70/070-19860627-JUD-01-00-EN.pdf> accessed 9 May 2025.

¹⁴⁷ François Delerue, *Cyber Operations and International Law* (Cambridge University Press 2020) 130 https://www-cambridge-org.proxy.annalindhbiblioteket.se/core/services/aop-cambridge-core/content/view/FC97677A3B551311148C74CAAE8F781D/9781108490276c4_111-188.pdf/attribution_to_a_state.pdf accessed 9 May 2025.

¹⁴⁸ Michael N Schmitt (ed), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (2nd edn, Cambridge University Press 2017) 79-83 <https://www.cambridge.org/core/books/tallinn-manual-20-on-the-international-law-applicable-to-cyber-operations/E4FFD83EA790D7C4C3C28FC9CA2FB6C9> accessed 9 May 2025.

¹⁴⁹ *Prosecutor v Dusko Tadić* (Judgment) ICTY-94-1-A (15 July 1999) para 120 <https://www.refworld.org/jurisprudence/caselaw/icty/1999/en/40180> accessed 9 May 2025.

Unlike the effective control test, which requires a state to direct specific operations, the overall control test allows attribution when the state plays significant role in organising, coordinating, or planning the military actions.¹⁵⁰ The ICTY ruled that this includes providing material support, such as funding, training, and equipment, but does not require the state to give direct orders for every attack.¹⁵¹ In Tadic, the tribunal held that if a state was involved in the general planning and coordination, responsibility could arise under international law.¹⁵²

This ruling emphasized that states cannot avoid responsibility by simply using proxy forces without giving precise orders. The test expands the scope of attribution beyond the strict conditions of the effective control test and has influenced how scholars and practitioners approach cyber operations..

Christian Henderson argues that the overall control test is sometimes more appropriate, especially since it requires a lower threshold. It applies when a state equips and finances a group and helps coordinate or plan its activities.¹⁵³ Antonio Cassese suggests that both tests have their place. The effective control test is better for situations involving individual actors acting on behalf of a state,¹⁵⁴ while the overall control test suits structured armed groups.¹⁵⁵ Although, the ICJ has remained with the stricter standard, the ICTY and several scholars believe the broader test better fits modern conflicts. However, as Delerue notes, the ICJ later rejected the overall control test in the Bosnian Genocide case and reaffirmed the effective control standard from Nicaragua, considering it more appropriate for questions of attribution.¹⁵⁶

¹⁵⁰ Ibid para 145

¹⁵¹ Ibid para 131

¹⁵² Ibid para 137-145

¹⁵³ Christian Henderson, *The Use of Force and International Law* (Cambridge University Press 2018) 405.

¹⁵⁴ Antonio Cassese, 'The Nicaragua and Tadić Tests Revisited in Light of the ICJ Judgment on Genocide in Bosnia' (2007) 18(4) *European Journal of International Law* 649, 652 <https://doi.org/10.1093/ejil/chm029> accessed 9 May 2025.

¹⁵⁵ Ibid 657

¹⁵⁶ François Delerue, *Cyber Operations and International Law* (Cambridge University Press 2020) 141 https://www-cambridge-org.proxy.annalindhblibioteket.se/core/services/aop-cambridge-core/content/view/FC97677A3B551311148C74CAAE8F781D/9781108490276c4_111-188.pdf/attribution_to_a_state.pdf accessed 9 May 2025.

In the context of cyber warfare, attribution becomes even harder. Cyber actors like hacktivist groups often lack clear command structures. Proving a state issued specific orders, as required under the effective control test, is almost impossible when groups act with state approval but no direct instructions. The overall control test, which focuses more on general support like funding or infrastructure, offers a more realistic way to establish state responsibility. Understanding the difference between these two tests is important in assessing whether cyber operations violate IHL. The ICJ's narrow approach limits accountability unless explicit orders can be shown, while the ICTY's broader test allows for responsibility even with indirect involvement. Given how states increasingly rely on cyber proxies, the overall control test may offer a better legal tool for addressing modern challenges in cyber warfare.

Cases

Georgia (2008)

One of the primary objectives of this research is to examine Russia's cyberattacks against Georgia and Ukraine and explore the extent to which these attacks can be attributed to Russia. In most cases, Russian cyber actions have been an addition to the already developing conflict situation rather than a separate attack. This pattern was evident during the Russia-Georgia war in 2008 when cyber operations were launched alongside kinetic military actions.¹⁵⁷ These cyberattacks included computer network operations designed to disable or degrade Georgia's infrastructure. Government computer systems, websites, and media outlets were targeted through large-scale DDoS attacks, resulting in a virtual cyber blockade.¹⁵⁸ On the day the war began,

¹⁵⁷ Stephen W Korns and Joshua E Kastenber, 'Georgia's Cyber Left Hook' (2008) 38(4) *Parameters* 60 <https://doi.org/10.55540/0031-1723.2455> accessed 9 May 2025.

¹⁵⁸ *Ibid*

Russian hacktivist websites circulated lists of Georgian sites to attack, providing instructions, downloadable malware, and after-action assessments.¹⁵⁹ Georgian networks faced repeated intrusions, with forensic investigations later revealing that hackers had been probing and testing government servers since at least July 20, 2008. Connell and Vogler argue that the degree of coordination among the attackers suggests that the cyber operations were part of a premeditated campaign plan. The scale, timing, and sophistication of the attacks indicate that they were likely coordinated with conventional military operations.¹⁶⁰

Still, in many cyberattacks like these, Russia never claimed responsibility.¹⁶¹ Even if the timing and clues pointed to Russian involvement, there was no strong proof to attribute the actions to Russia.¹⁶² This shows how hard it is to connect a cyberattack to a state. This inconsistency allows the states to exploit attribution challenges and operate in cyberspace with relative impunity.¹⁶³

Ukraine

Even before Russia's full-scale invasion of Ukraine in 2022, Ukraine had already endured years of Russian cyberattacks targeting critical infrastructure, public services, and military networks.¹⁶⁴

¹⁵⁹Michael Connell and Sarah Vogler, *The Challenge of Attribution for Cyber Attacks* (CNA 2016) 17 https://www.cna.org/archive/CNA_Files/pdf/dop-2016-u-014231-1rev.pdf accessed 9 May 2025.

¹⁶⁰ Ibid 18

¹⁶¹ Hannah Gray, 'Cyberwarfare and the Challenges It Poses to the International Governance of Armed Conflict with Particular Reference to Attribution, Distinction, and Self-Defence' (2024) 68 <https://doi.org/10.2218/ccj.v5.9346> accessed 9 May 2025.

¹⁶² Michael Connell and Sarah Vogler, *The Challenge of Attribution for Cyber Attacks* (CNA 2016) 17 https://www.cna.org/archive/CNA_Files/pdf/dop-2016-u-014231-1rev.pdf accessed 9 May 2025.

¹⁶³ Ibid

¹⁶⁴ Alika Guchua and Tornike Zedelashvili, 'Challenges Arising from Cyber Security in the Dimension of Modern Global Security (on the Example of the Russia-Ukraine War)' (2022) 11(2) *Eastern Review* 82-83 <https://www.proquest.com/scholarly-journals/challenges-arising-cyber-security-dimension/docview/3126075929/se-2> accessed 9 May 2025.

Russia carried out several major cyber operations against Ukraine, including the NotPetya attack in 2017.¹⁶⁵

NotPetya was a highly destructive malware attack that initially targeted Ukrainian government institutions, banks, and infrastructure but quickly spread worldwide.¹⁶⁶ The attack exploited existing VPN connections between foreign companies and their Ukrainian branches, allowing it to propagate globally. Maersk, the Danish shipping company, was among the victims, suffering billions of dollars in damage due to a near-total shutdown of its IT systems.¹⁶⁷

In July 2017, the Security Service of Ukraine (SBU) blamed the Russian security services for this attack.¹⁶⁸ Later, in 2018, both the United Kingdom (UK) and the US formally attributed NotPetya to the Russian government. A press release from the UK government stated that the UK National Cyber Security Center had assessed that the Russian military was “almost certainly responsible” for the attack.¹⁶⁹ Similarly, a statement from the White House condemned the attack as “part of the Kremlin’s ongoing effort to destabilise Ukraine,” characterising it as a reckless and indiscriminate.¹⁷⁰ But even with strong political words, neither UK nor US formally

¹⁶⁵ Andy Greenberg, ‘The Untold Story of NotPetya, the Most Devastating Cyberattack in History’ (Wired, 22 August 2018) <https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/> accessed 9 May 2025.

¹⁶⁶ François Delerue, *Cyber Operations and International Law* (Cambridge University Press 2020) 173 https://www-cambridge-org.proxy.annalindhbiblioteket.se/core/services/aop-cambridge-core/content/view/FC97677A3B551311148C74CAAE8F781D/9781108490276c4_111-188.pdf/attribution_to_a_state.pdf accessed 9 May 2025.

¹⁶⁷ Ibid 175

¹⁶⁸ Reuters, ‘Cyber Attack Hits Ukraine Then Spreads Internationally’ (Reuters, 28 June 2017) <https://www.reuters.com/article/us-cyber-attack-ukraine-idUSKBN19M39P/> accessed 9 May 2025.

¹⁶⁹ UK Government, ‘Foreign Office Minister Condemns Russia for NotPetya Attacks’ (Gov.uk, 2018) <https://www.gov.uk/government/news/foreign-office-minister-condemns-russia-for-notpetya-attacks> accessed 9 May 2025.

¹⁷⁰ Ellen Nakashima, ‘Russian Military Was behind NotPetya Cyberattack in Ukraine, CIA Concludes’ (*The Washington Post*, 12 January 2018) https://www.washingtonpost.com/world/national-security/russian-military-was-behind-notpetya-cyberattack-in-ukraine-cia-concludes/2018/01/12/048d8506-f7ca-11e7-b34a-b85626af34ef_story.html accessed 9 May 2025.

characterised the operation as illegal under international law.¹⁷¹ This highlights the key problem in cyber attribution, politicians can blame quickly, but to prove it legally under IHL, a stronger evidence is needed, which is usually hard or often impossible to attain.

The problem is that cyber teams often work without direct orders, so it is hard to say that the state gave command. The overall control test, from Tadić case, offers more flexibility by considering broader forms of state support, this means not just direct orders, but also providing help, money, tools, or intelligence.

Conclusion

Attributing cyber attacks to states remains one of the most significant legal challenges in the application of IHL. As demonstrated by the cases of Georgia, and Ukraine, cyber operations often involve non-state actors, making it difficult to establish direct state responsibility under the effective control test. While forensic evidence, timing, and strategic alignment may strongly suggest state involvement, these factors are often insufficient to meet the strict threshold required for legal attribution.

The overall control test provides a more flexible alternative for holding states accountable when non-state actors conduct cyber operations with significant state support. However, even this broader test does not fully resolve the attribution dilemma in cyberspace, where still pretend they have nothing to do with the attacks while quietly benefiting from cyber operations carried out by proxies.

¹⁷¹ François Delerue, *Cyber Operations and International Law* (Cambridge University Press 2020) 177 https://www-cambridge-org.proxy.annalindhbiblioteket.se/core/services/aop-cambridge-core/content/view/FC97677A3B551311148C74CAAE8F781D/9781108490276c4_111-188.pdf/attribution_to_a_state.pdf accessed 9 May 2025.

In the end, this difficulty makes it even easier for actors to avoid responsibility and adds the bigger problem to impunity in cyber warfare. Without clearer legal standards and mechanisms for accountability, states can exploit attribution challenges to conduct cyber operations with little fear of legal consequences. As cyber warfare continues to evolve, the international community must consider whether existing attribution frameworks under IHL are sufficient or whether new legal mechanisms are needed to address the complexities of state responsibility in cyberspace.

4. Future of Cyber Warfare and IHL

The recent war between Russia and Ukraine has already shown that cyber operations can cause huge damage, not only to military targets but also to civilians.¹⁷² Power plants, hospitals, banks, and other communication systems can be attacked with only a few clicks. Hence, it is arguable whether the current rules of IHL are strong enough to deal with this new reality.¹⁷³

IHL was created to protect civilians during wars and to limit their suffering.¹⁷⁴ But at that time, most likely, nobody was thinking about cyber operations and it is still not clear what counts as an attack in cyberspace, moreover, the third chapter shows that there are some difficulties when it comes to applying the core principles of IHL to the cyberattacks and the problem of attribution makes it even more complicated because sometimes we do not even know who is really behind

¹⁷² European Parliamentary Research Service, *Cyberattacks in the Russia-Ukraine War: Can International Law Cope?* (European Parliament Briefing, 2023) 12 [https://www.europarl.europa.eu/RegData/etudes/BRIE/2023/702594/EXPO_BRI\(2023\)702594_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/BRIE/2023/702594/EXPO_BRI(2023)702594_EN.pdf) accessed 9 May 2025.

¹⁷³ International Committee of the Red Cross, 'International Humanitarian Law and Cyber Operations during Armed Conflicts' (2021) 102(913) *International Review of the Red Cross* 483 <https://international-review.icrc.org/sites/default/files/reviews-pdf/2021-03/ihl-and-cyber-operations-during-armed-conflicts-913.pdf> accessed 9 May 2025.

¹⁷⁴ Nils Melzer, *Cyberwarfare and International Law: Legal Challenges and Restraints* (Center for Security Studies 2011) 21 <https://unidir.org/publication/cyberwarfare-and-international-law/> accessed 9 May 2025.

the cyberattacks. This chapter examines these legal gaps and aims to answer whether IHL should be modified to cover cyberattacks.

4.1 Legal gaps in IHL regarding cyberattacks

As mentioned before, because of its well-established framework, IHL also applies to cyber operations during armed conflicts.¹⁷⁵ However, IHL faces some challenges when it comes to cyber warfare. One reason could be that IHL was created a long time ago, and at that time, almost no one could imagine that cyberspace would become a fifth domain of warfare. Nowadays, cyberattacks can harm civilians just as much as traditional weapons during kinetic warfare.

One of the biggest gaps is about the meaning of a cyber “attack.” Under IHL, an attack is defined as an act of violence that causes death, injury, or destruction.¹⁷⁶ But in cyberspace, a lot of operations do not even cause physical harm or destruction. For example, if the cyber operation disrupts the civilian infrastructure and causes physical damage, then this would be considered an attack, but disabling a country’s banking system or electricity through malware may not kill anyone and, therefore it may not constitute an attack at all. The case of the Russia-Georgia war in 2008 is also a good example because even though Russian cyberattacks took down more than 100 Georgian websites, spread misinformation, and created panic among the population, they did not cause any physical destruction. The Tallinn Manual tries to solve this by saying that cyber

¹⁷⁵ Nils Melzer, *International Humanitarian Law: A Comprehensive Introduction* (ICRC 2019) 17 https://www.researchgate.net/profile/Etienne-Kuster/publication/313589999_New_IHL_handbook/links/62e3d2953c0ea8788765ee4e/New-IHL-handbook.pdf accessed 9 May 2025.

¹⁷⁶ Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflicts (Protocol I) (adopted 8 June 1977, entered into force 7 December 1978) 1125 UNTS 3, art 49 https://www.icrc.org/sites/default/files/external/doc/en/assets/files/other/icrc_002_0321.pdf accessed 9 May 2025.

operations that cause similar effects to physical attacks should be considered as attacks. However, states are not fully agreeing on this definition yet.¹⁷⁷

Moreover, as discussed in the third chapter, cyber operations raise new and complex issues with the core principles of IHL, for example, the principle of distinction, which is designed to ensure that civilians and civilian infrastructure are spared from the effects of hostilities and the attacks are directed solely at military objectives.¹⁷⁸ Therefore, the attacks that are directed at civilian cyber infrastructures would amount to a breach of Article 48 of AP I. However, in the context of cyberspace, the application of this principle becomes highly problematic as a result of the dual-use nature of cyberspace.¹⁷⁹ Unlike traditional warfare, where military and civilian objects are often physically separated and more easily identifiable, digital systems frequently serve both purposes simultaneously. For example, an internet server might be used for military communications, yet also support civilian services such as hospitals, educational institutions, banking systems, etc. Disabling such a server may cause a tactical advantage, but it also risks causing severe harm to civilians who rely on the same digital infrastructure. To conclude, the principle of distinction faces significant interpretative and practical challenges in the cyber domain. The dual-use dilemma, the interconnectivity of modern infrastructure, and the

¹⁷⁷ Chukwudumebi O Joseph-Asoh, Nkechinyere Worluh-Okolie and Jojo Ebibode, 'The Rise of Cyberwarfare: The Applicability of International Humanitarian Law for the Protection of Civilians and Civilian Objects' (2024) 10(2) *International Journal of Law* 92–93 <https://www.lawjournals.org/assets/archives/2024/vol10issue2/10065.pdf> accessed 9 May 2025.

¹⁷⁸ Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflicts (Protocol I) (adopted 8 June 1977, entered into force 7 December 1978) 1125 UNTS 3, art 48 https://www.icrc.org/sites/default/files/external/doc/en/assets/files/other/icrc_002_0321.pdf accessed 9 May 2025.

¹⁷⁹ Chukwudumebi O Joseph-Asoh, Nkechinyere Worluh-Okolie and Jojo Ebibode, 'The Rise of Cyberwarfare: The Applicability of International Humanitarian Law for the Protection of Civilians and Civilian Objects' (2024) 10(2) *International Journal of Law* 94 <https://www.lawjournals.org/assets/archives/2024/vol10issue2/10065.pdf> accessed 9 May 2025.

unpredictability of cyber tools all contribute to a legal environment where compliance with article 48 AP I is extremely difficult.

Another, and perhaps the most important legal gap, is the issue of attribution. As discussed in the third chapter, attribution in cyberspace remains one of the most problematic aspects of enforcing IHL in cyber warfare. Identifying the true origin of a cyberattack is often made difficult by the nature of digital communication. States and non-state actors can employ proxy groups, false flag operations, and spoofed IP addresses to mask their identity. This makes it difficult and sometimes even impossible to prove who launched a particular cyber operation. The threshold of legal attribution in international law relies on demonstrating some kind of control over the actors responsible for the conduct. For instance, even when state-linked hacker groups operate with a government's approval or support, states may deny responsibility due to the absence of evidence. This legal ambiguity creates a permissive environment where states can act through cyber means without clear accountability. If an attack cannot be attributed to a state within a conflict, it becomes impossible to hold the responsible party accountable under IHL, and this on the other hand, weakens the legal protection for civilians. The Georgian and Ukrainian cases illustrate this gap clearly. In both cases, Russia was widely suspected of orchestrating cyberattacks during kinetic military campaigns, but due to a lack of proof, Russia avoided international legal consequences.

To summarise, the principle of distinction and the issue of attribution highlight the fragile applicability of IHL in cyberspace. While the legal framework exists, its applications pose a lot of difficulties. Without clearer standards for attribution and more flexible mechanisms, the ability to protect civilians and enforce accountability in cyber conflicts will remain severely constrained.

4.2 Should IHL be modified to regulate cyberattacks explicitly?

The debates about whether the IHL should be changed or updated to regulate cyberattacks are growing. Nowadays, some experts argue that with cyber operations becoming a normal part of armed conflicts, there is a need for specific rules made only for cyberspace, but this view also has opponents.

One scholar argues that the main problem is that IHL was originally created for conventional warfare at a time when cyberattacks did not exist.¹⁸⁰ Today, this creates serious limitations, and the only way to address them might be either through adopting a new international convention focused entirely on cyber conflicts or through the gradual development of binding customary law based on consistent state practice carried out with a sense of legal obligation.

Hannah Gray, in her article argues that cyberwarfare poses significant challenges to the international governance of armed conflict.¹⁸¹ She states that the current legal framework regarding the non-state actors and attributability must be reviewed to apply them to cyber attacks, or new guidelines for cyber warfare should be discussed. This view has a lot of supporters among scholars. For example, another author suggests that “there should be a new protocol added to the Geneva Conventions of 1949 with respect to cyber warfare and cyber operations.” Moreover, he states that a new treaty document is one way to regulate cyber warfare and that the treaty should provide clear definitions of cyber warfare, cyber operations, and cyber

¹⁸⁰ H Sohail, 'Fault Lines in the Application of International Humanitarian Law to Cyberwarfare' (2022) 17 *Journal of Digital Forensics, Security and Law* 11 <https://www.proquest.com/scholarly-journals/fault-lines-application-international/docview/2661588237/se-2> accessed 9 May 2025.

¹⁸¹ Hannah Gray, 'Cyberwarfare and the Challenges It Poses to International Governance of Armed Conflict' (2024) 74 <https://doi.org/10.2218/ccj.v5.9346> accessed 9 May 2025.

attacks. He believes that until a universally accepted definition is established, the development of an international framework to govern cyber warfare will not happen.¹⁸²

Furthermore, Nils Melzer states that cyberwarfare does not exist in a legal vacuum; in opposite, it is subject to well-established rules and principles, but at the same time, the states should be aware of their moral responsibility toward the next generations.¹⁸³ Nicholas Tsagourias and Michael Farrel believe that international law should face and shape cyber reality by establishing a regulatory framework within which states, individuals, and other entities can operate and be held accountable.¹⁸⁴

Some authors and scholars agree that it is essential to recognise the distinct nature of the cyber domain and establish the legal framework that comprehensively discusses its complexities.¹⁸⁵ However, there are also arguments that IHL is flexible enough. For example, Heather Harrison Dinniss says in her book that even though computer network attacks raise challenging issues for the current laws of armed conflict, for the most part, existing laws are capable of adapting to the new technology. She mentions the Martens Clause, which “was drafted with exactly this eventuality in mind, and ICJ has noted that the clause has proved to be effective means of

¹⁸² Rohit Bokil, 'Cyber Warfare: Taking War to Cyberspace and Its Implications for International Humanitarian Law' (2023) *International Journal for Multidisciplinary Research* 10–11 <https://www.ijfmr.com/papers/2023/1/1494.pdf> accessed 9 May 2025.

¹⁸³ Nils Melzer, *Cyberwarfare and International Law* (Center for Security Studies 2011) 36 <https://unidir.org/publication/cyberwarfare-and-international-law/v> accessed 9 May 2025.

¹⁸⁴ Nicholas Tsagourias and Michael Farrell, 'Cyber Attribution: Technical and Legal Approaches and Challenges' (2020) 31(3) *European Journal of International Law* 967 <https://doi.org/10.1093/ejil/chaa057> accessed 9 May 2025.

¹⁸⁵ Chukwudumebi O Joseph-Asoh, Nkechinyere Worluh-Okolie and Jojo Ebibode, 'The Rise of Cyberwarfare: The Applicability of International Humanitarian Law for the Protection of Civilians and Civilian Objects' (2024) 10(2) *International Journal of Law* 96 <https://www.lawjournals.org/assets/archives/2024/vol10issue2/10065.pdf> accessed 9 May 2025.

addressing the rapid evolution of military technology.” She believes that the new convention that addresses the issue is unnecessary.¹⁸⁶

the Tallinn Manual, although non-binding, remains the most detailed attempt to interpret existing IHL rules in the cyber context. Christopher S Yoo, in his article, states that although the Tallinn Manual is a step in the right direction within its scope, some parts of cyber operations remain unaddressed.¹⁸⁷ Another scholar states that the Tallinn Manual is the only comprehensive document developed by the experts, but it lacks binding effects as it is not made by state consensus.¹⁸⁸ It is also argued that the current IHL does not fully address the challenges posed by new forms of warfare, such as cyberattacks, and despite existing legal instruments, their effectiveness in hybrid conflicts remains limited due to the lack of mechanisms adapted to contemporary challenges.¹⁸⁹

Another important point is the growing use of cyber countermeasures. Many states are now developing their own cyber defence and attack systems. Alike Gochua and Thornike Zedelashvili, in their article, highlight the need for new cyber security strategies in Ukraine and Georgia, which should be based on modern standards.¹⁹⁰

¹⁸⁶ Heather Harrison Dinniss, *Cyber Warfare and the Laws of War* (Cambridge University Press 2012) 28 <https://research-ebSCO-com.proxy.annalindhblibloteket.se/linkprocessor/plink?id=f63d7260-304c-3725-a488-b600328c5879> accessed 9 May 2025.

¹⁸⁷ Christopher S Yoo, ‘Cyber Espionage or Cyberwar?: International Law, Domestic Law, and Self-Protective Measures’ in Jens David Ohlin, Kevin Govern and Claire Finkelstein (eds), *Cyberwar: Law and Ethics for Virtual Conflicts* (Oxford University Press 2015) 31 https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2596634 accessed 9 May 2025.

¹⁸⁸ Ashutosh Pandey, ‘Application of International Humanitarian Law in Changing Dimensions of Armed Conflict Vis-à-Vis Cyber Warfare’ (2025) 6(1) *Unity Journal* 293 <https://doi.org/10.3126/unityj.v6i1.75698> accessed 9 May 2025.

¹⁸⁹ Elvira Orzhynska *et al*, ‘International Humanitarian Law and the Waging of War in Ukraine: Integrative Review’ (2024) 4(4) *Futurity Economics & Law* 272 <https://doi.org/10.57125/FEL.2024.12.25.15> accessed 9 May 2025.

¹⁹⁰ Alike Guchua and Tornike Zedelashvili, ‘Challenges Arising from Cyber Security in the Dimension of Modern Global Security (on the Example of the Russia-Ukraine War)’ (2022) 11(2) *Eastern Review* 87 <https://www.proquest.com/scholarly-journals/challenges-arising-cyber-security-dimension/docview/3126075929/se-2> accessed 9 May 2025.

To sum up, the debates around changing or updating International Humanitarian Law to explicitly regulate cyberattacks are still ongoing and complex. Some scholars strongly believe that new rules are necessary because the nature of cyber warfare is different from traditional wars, and the current legal framework is not enough to protect civilians or hold responsible actors accountable. They argue that a new protocol or even a new treaty is needed, with clear definitions and rules that can address the unique challenges of cyberspace.

At the same time, others believe that the existing IHL is flexible and strong enough to cover cyber operations and that what is really needed is better interpretation and state practice. Instruments like the Tallinn Manual are seen as a good start but still not enough because they are not legally binding.

The ongoing Russia-Ukraine conflict shows that cyber operations are already part of modern wars. Whether through new treaties, protocols, or improved interpretation of existing laws, it is clear that more must be done to make sure civilians are protected and that cyber operations are regulated under international law. States have the responsibility not only to adapt to this new reality but also to act for the sake of future generations.

5. Conclusion

This thesis has examined how IHL applies to cyber operations during armed conflicts, especially in the context of the Russia-Ukraine war. The analysis has shown that IHL is not only relevant, but also necessary to apply in the cyber domain. The main principles of IHL remain essential, but their application in cyberspace is far from simple. At the same time, current events show that legal frameworks must be improved in order to meet the realities of cyber warfare. Several

lessons can be drawn from these developments, and they should be considered in order to protect civilians more effectively.

Even though scholars, international bodies, and the states confirmed that IHL applies to cyber operations during armed conflicts, applying the rules in practice is legally and technically very complex.¹⁹¹ The digital nature of cyber operations, the shared civilian-military infrastructure, and the anonymity of actors create serious challenges to implementing these rules in practice. For example, the principle of distinction becomes very difficult when civilian and military infrastructure are interconnected. Cyber operations often use the same networks that are also used for hospitals, water systems, or public communication. A cyberattack that targets a military server might also damage critical civilian infrastructure. This has been seen in the case of Kyivstar attack in Ukraine, where a communications network was targeted, but the effects were felt not only by the military, but also by civilians and even users in other countries. In such cases, the separation between civilian and military targets becomes very weak, and the protective purpose of IHL is undermined. The same applies to the principle of proportionality. In cyber warfare, it is often hard to predict the effects of an attack. A cyber operation might seem to have a military objective, but in reality, it may result in long-term or indirect damage to civilians, especially when it disables energy systems or medical services. This unpredictability makes it difficult to assess whether the harm caused to civilians is excessive in relation to the military advantage gained. And since cyber effects can be spread across borders, this also raises concerns about how to evaluate harm, especially when consequences are delayed or less visible compared to traditional kinetic attacks.

¹⁹¹ International Committee of the Red Cross, *The Potential Human Cost of Cyber Operations* (ICRC 2021) 68 <https://shop.icrc.org/the-potential-human-cost-of-cyber-operations-pdf-en.html> accessed 9 May 2025.

The principle of military necessity also becomes more unclear in cyber contexts. Many cyber operations aim to disrupt, not destroy, and the military advantage is often not immediate or even certain. For instance, an operation that takes down a power grid might be intended to slow down logistics, but at the same time it could leave entire communities and hospitals without power. In such cases, it is not always possible to say that the operation meets the legal test of necessity, especially when there may be other less harmful options available.

One important lesson from recent conflicts is that cyber warfare could directly affect civilians and their survival. Attacks on civilian objects like hospitals, water systems, or banking networks can have consequences that are just as serious as traditional military operations. Therefore, legal frameworks must do more to address these risks. IHL already provides protection for civilian infrastructure in kinetic warfare, but cyber operations are more difficult to control and often go unnoticed until it is too late.¹⁹² Specific legal rules should clarify that cyber operations against critical civilian infrastructure are prohibited, even if they do not cause physical destruction. The current silence of the law in this area creates space for harmful actions that escape responsibilities.

Another, and perhaps the biggest issue is attribution. This thesis has discussed the legal standards used to attribute cyberattacks to states, focusing on the effective control test from Nicaragua case and the overall control test from the Tadić case. Both of these standards are very difficult to apply in cyber warfare. In practice, it is almost impossible to prove who was behind an attack, especially when states use proxies, hackers, or even false flag operations to hide their

¹⁹² Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflicts (Protocol I) (adopted 8 June 1977, entered into force 7 December 1978) 1125 UNTS 3, art 52 https://www.icrc.org/sites/default/files/external/doc/en/assets/files/other/icrc_002_0321.pdf accessed 9 May 2025.

involvement. This was also seen in the Russia-Georgia war, where strong suspicion existed about Russian involvement in cyberattacks but no direct proof could be found. The standard for attribution is too high for modern cyber conflicts, and this allows states to act indirectly and avoid accountability. Even though Tadić offered a broader test, the ICJ later rejected it in the Bosnian Genocide case, making the effective control standard the main legal test.¹⁹³ In cyber warfare, this standard is often impossible to meet, as the attackers are anonymous and the command structures are unclear.

A potential way forward is through the development of new legal mechanisms for attribution. These could involve international cooperation on evidence collection, shared technical tools or even the creation of an international body to assess cyber incidents. Lowering the standard of proof in cyber attribution could also be considered, as long as it does not compromise legal certainty. While this would represent a shift from traditional standards, it may be necessary to ensure accountability in a domain where perfect evidence is rarely available. Another path could be through state practice and *opinio juris*, which, over time, can create customary international law. If more and more states come to agreement that IHL should cover cyber operations and act like that, it can help solidify those rules faster. But this is very slow and uncertain route of development. On the other hand, the ICJ could also play a role by clarifying how IHL applies to cyber operations. For example, if the ICJ were to accept a case about state-backed cyberattacks it could develop a new test for attribution or offer guidance on applying the existing principles of IHL in cyberspace. This would help close the legal gaps. However, this process depends largely on political circumstances and the willingness of states.

¹⁹³ François Delerue, *Cyber Operations and International Law* (Cambridge University Press 2020) 141 https://www-cambridge-org.proxy.annalindhbiblioteket.se/core/services/aop-cambridge-core/content/view/FC97677A3B551311148C74CAAE8F781D/9781108490276c4_111-188.pdf/attribution_to_a_state.pdf accessed 9 May 2025.

It can be concluded that without a new treaty or binding consensus, legal uncertainty will persist. States interpret rules in different ways, apply them selectively, and often prioritise military advantage over humanitarian considerations. As a result, IHL risks becoming ineffective in cyber warfare, which is increasingly common in modern conflicts. This thesis has discussed the possibility of developing a new international treaty or legal doctrine for cyber warfare. While this is the most logical solution, it can also be politically difficult. States can be reluctant to agree on new conventions that would limit their cyber capabilities. A binding treaty would impose legal obligations, require more transparency, and potentially expose states to liability for actions they currently conduct with impunity. However, the lack of binding norms comes at a cost.

In conclusion, this thesis has shown that the legal framework of IHL, while applicable to cyber warfare, faces serious difficulties in practice. The principles of distinction, proportionality, and military necessity are hard to implement when targets are digital, dual-use, and invisible. The legal standard for attribution is too high for cyber conflicts, allowing states to escape accountability by acting indirectly or through proxies, and non-state actors playing an increasing role further complicates the scenario. There is no binding treaty to regulate cyber operations, and while instruments like the Tallinn Manual help, they cannot enforce compliance. Moving forward requires some kind of innovation, new doctrines, stronger state cooperation, and perhaps even the development of an international agreement. States must also recognise that cyberspace is no longer just a technical domain, it is a battlefield, and as such, it must be governed by rules that protect civilians and promote peace. If IHL is to remain relevant in the 21st century, it must evolve to address the realities of cyber warfare. Sitting still is not an option anymore because the next war might not begin on the ground or air but from the cyber domain.

Bibliography:

Articles

Akimenko, Valeriy, and Keir Giles. "Russia's Cyber and Information Warfare." *Asia Policy* 15, no. 2 (2020): 67–75

Ahmad Khalil, Mhd Bitar and S Anandha Krishna Raj, 'A New Era of Armed Conflict: The Role of State and Non-State Actors in Cyber Warfare with Special Reference to Russia-Ukraine War' (2024) 14(2) *TalTech Journal of European Studies*

Alika Guchua and Tornike Zedelashvili, 'Challenges Arising from Cyber Security in the Dimension of Modern Global Security (on the Example of the Russia-Ukraine War)' (2022) 11(2) *Eastern Review*

Antonio Cassese, 'The Nicaragua and Tadić Tests Revisited in Light of the ICJ Judgment on Genocide in Bosnia' (2007) 18(4) *European Journal of International Law*

Ashutosh Pandey, 'Application of International Humanitarian Law in Changing Dimensions of Armed Conflict Vis-à-Vis Cyber Warfare' (2025) 6(1) *Unity Journal*

Brian T. O'Donnell and James C. Kraska, 'Humanitarian Law: Developing International Rules for the Digital Battlefield' (2003) 8(1) *Journal of Conflict and Security Law*

Chukwudumebi O Joseph-Asoh, Nkechinyere Worluh-Okolie and Jojo Ebibode, 'The Rise of Cyberwarfare: The Applicability of International Humanitarian Law for the Protection of Civilians and Civilian Objects' (2024) 10(2) *International Journal of Law*

Christopher S Yoo, 'Cyber Espionage or Cyberwar?: International Law, Domestic Law, and Self-Protective Measures' in Jens David Ohlin, Kevin Govern, and Claire Finkelstein (eds), *Cyberwar: Law and Ethics for Virtual Conflicts* (OUP 2015)

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

Dawa Choden and Ramesh Kumar, 'Relevance of International Law in Preventing International Conflict: A Case Study of Russia-Ukraine' (2023) 8(1) *Legal Research Development*

David Turns, 'Cyber War and the Concept of Attack in International Humanitarian Law' in Dan Saxon (ed), *International Humanitarian Law and the Changing Technology of War* (Brill Nijhoff 2013)

Deibert, Ronald J., Rafal Rohozinski, and Masashi Crete-Nishihata. "Cyclones in Cyberspace: Information Shaping and Denial in the 2008 Russia–Georgia War." *Security Dialogue* 43, no. 1 (2012): 3–24

Dominika Dziwisz, 'Rethinking Future Conflicts: The Cyber Grey Zone from the Russian Perspective' (2024) 21 *Politeja* 28

E F Mejia, 'Act and Actor Attribution in Cyberspace: A Proposed Analytic Framework' (2014) 8(1) *Strategic Studies Quarterly* 114

Eitan Diamond, 'Applying International Humanitarian Law to Cyber Warfare' in Pnina Sharvit Baruch and Anat Kurz (eds), *Law and National Security: Selected Issues* (INSS 2014)

Elvira Orzhynska et al, 'International Humanitarian Law and the Waging of War in Ukraine: Integrative Review' (2024) 4(4) *Futurity Economics & Law*

Franzese, Patrick W., *Cyberwar: Are Civilians Back on the Battlefield?* (Air War College 2015)

Garrett Van Epps, 'Common Ground: US and NATO Engagement with Russia in the Cyber Domain' (2013) 12(4) *Connections*

H Sohail, 'Fault Lines in the Application of International Humanitarian Law to Cyberwarfare' (2022) 17 *Journal of Digital Forensics, Security and Law*

Hannah Gray, 'Cyberwarfare and the Challenges It Poses to the International Governance of Armed Conflict' (2024) 5 *Contemporary Challenges*

Iryna Fyshchuk, Mette Strange Noesgaard and Jeppe Agger Nielsen, 'Managing Cyberattacks in Wartime: The Case of Ukraine' (2024) *Public Administration Review* 1

J A Lewis, *Cyber War and Ukraine* (Center for Strategic and International Studies 2022) <http://www.jstor.org/stable/resrep41883>

K. Giles, 'Information Troops – A Russian Cyber Command?' (2011) *3rd International Conference on Cyber Conflict*

Kilinskas, K., 'Hybrid Warfare: An Orientating or Misleading Concept in Analysing Russia's Military Actions in Ukraine?' (2016) 14(1) *Lithuanian Annual Strategic Review*

Kolodii R, 'The Pedagogy of Cyber-WAR: Explaining Ukraine's Resilience Against Russian Cyber-Aggression' (2024) 40(2) *Defense & Security Analysis* 270

Kosmas Pipyros et al, 'Cyberoperations and International Humanitarian Law' (2016) 24(1) *Information and Computer Security*

Laurent Gisel, Tilman Rodenhäuser and Knut Dörmann, 'Twenty Years On: IHL and Protection of Civilians Against Cyber Operations' (2020) 102(913) *IRRC*

Lilian O Aluede and Peace B Biragbara, 'Cyber Attack: An Emerging War' (2020) 8(1) *GSIJ*

Lin, Herbert, 'Russian Cyber Operations in the Invasion of Ukraine' (2022) 7(4) *Cyber Defense Review*

Lukasz Olejnik and Tilman Rodenhäuser, 'Malware: Essential Cyber Notions' (ICRC Blog, 23 May 2019)

Madelena Anna Miniats, 'War of Nerves: Russia's Cyber Warfare in Estonia, Georgia and Ukraine' (2019) *Senior Projects Spring*

Marcus Willet, 'The Cyber Dimension of the Russia–Ukraine War' (2022) 64(5) *Survival*

Markus Takama and Martti Lehto, 'Cyber Operations in Ukraine: Emerging Patterns in Cases' in Proceedings of the 23rd European Conference on Cyber Warfare and Security (2024)

Michael Bothe et al, 'Scope of Application of IHL' in Dieter Fleck (ed), *Handbook of IHL* (4th edn, OUP 2021)

Michael Connell and Sarah Vogler, 'The Challenge of Attribution for Cyber Attacks' (2016)

Michael N Schmitt, 'Cybersecurity and International Law' in Robin Geiß and Nils Melzer (eds), *Oxford Handbook of International Law of Global Security* (OUP 2021)

Michael N Schmitt, 'IHL and the Conduct of Cyber Hostilities: Quo Vadis?' (2022) 13(2) *International Humanitarian Legal Studies*

Michael Schmitt and Jeffrey Biller, 'The NotPetya Cyber Operation' (EJIL: Talk!, 6 August 2020)

Nicholas Tsagourias and Michael Farrell, 'Cyber Attribution: Legal and Technical Challenges' (2020) 31(3) *EJIL*

Rahman M.M. and Das T.K., 'Countering Cyberattacks: Gaps in International Law' (2024) 2(4) *Journal of Digital Technologies and Law*

Rohit Bokil, 'Cyber Warfare and IHL Implications' (2023) 5(1) *International Journal For Multidisciplinary Research*

Ruadze, N., 'Humanitarian Intervention and the 2008 Russia–Georgia War' (2015) 8(1) *Caucasus Journal of Social Sciences*

Shackelford, S. J., and Andres, R. B., 'State Responsibility for Cyber Attacks' (2011) 42(4) *Georgetown Journal of International Law*

Shutosh Pandey, 'Application of IHL to Cyber Warfare' (2025) 6(1) *Unity Journal*

Stephen W Korns and Joshua E Kastenber, 'Georgia's Cyber Left Hook' (2008) 38(4) *Parameters*

Stoddart, Kristan, 'Russia's Cyber Campaigns and the Ukraine War' (2024) 3(1) *Applied Cybersecurity & Internet Governance*

Vakhtang Maisaia, Aliko Guchua and Thornike Zedelashvili, 'Cybersecurity of Georgia and Threats from Russia' (2020) 9 *Eastern Review*

Vladimeri Napetvaridze and Archil Chochia, 'Cybersecurity in the Making – Georgia' (2019) 19(2) *International Comparative Law Review*

Zen Chang, 'Cyberwarfare and IHL' (2017) 9(1) *Creighton International and Comparative Law Journal*

Books

Jason Andress and Steve Winterfeld, *Cyber Warfare: Techniques, Tactics and Tools for Security Practitioners* (Syngress 2014)

François Delerue, *Cyber Operations and International Law* (Cambridge University Press, 2020)

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

Robin Geiß and Nils Melzer (eds), *The Oxford Handbook of the International Law of Global Security* (Oxford University Press, 2021; online edn, Oxford Academic, 10 Mar. 2021)

Christian Henderson, *The Use of Force and International Law* (Cambridge University Press, 2018)

Nina Jankowicz, *How to Lose the Information War: Russia, Fake News, and the Future of Conflict* (I.B. Tauris 2020)

G Lucas, *Law, Ethics and Emerging Military Technologies: Confronting Disruptive Innovation* (1st edn, Routledge 2022)

Nils Melzer, *Cyberwarfare and International Law: Legal Challenges and Restraints* (Center for Security Studies, 2011)

Nils Melzer, *International Humanitarian Law: A Comprehensive Introduction* (ICRC 2019)

N Nilsson and M Weissmann, *Russian Warfare and Influence: States in the Intersection Between East and West* (Bloomsbury Academic, 2024)

Mark Galeotti, *Putin's Wars: From Chechnya to Ukraine* (Osprey Publishing 2022)

Paulo Shakarian, Jana Shakarian, and Andrew Ruef, *Introduction to Cyber-Warfare: A Multidisciplinary Approach* (Syngress 2013)

Dan Saxon, *International Humanitarian Law and the Changing Technology of War* (Brill Nijhoff 2013)

C Whyte and B Mazanec, *Understanding Cyber-Warfare: Politics, Policy and Strategy* (2nd edn, Routledge 2023)

Case Law

International Court of Justice (ICJ)

Case Concerning Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Bosnia-Herzegovina v. Yugoslavia) ICJ, 11 July 1996

Case Concerning Military and Paramilitary Activities In and Against Nicaragua (Nicaragua v. United States of America); Merits, ICJ, 27 June 1986

International Criminal Tribunal for the former Yugoslavia (ICTY)

Prosecutor v Dusko Tadić (Appeal Judgement), IT-94-1-A, ICTY, 15 July 1999

Law and Soft Law

International Committee of the Red Cross (ICRC), *The Geneva Conventions of 1949, the Additional Protocols, and their Commentaries*

International Law Commission, 'Draft Articles on Responsibility of States for Internationally Wrongful Acts' (2001)

Michael N Schmitt (ed), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (2nd edn, Cambridge University Press 2017)

Michael N Schmitt (ed), *Tallinn Manual on the International Law Applicable to Cyber Warfare* (Cambridge University Press 2013)

Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflicts (Protocol I) (adopted 8 June 1977, entered into force 7 December 1978) 1125 UNTS 3

Newspaper Articles

BBC News, 'Ukraine Cyber-Attack: Kyivstar Boss Says Hackers Destroyed Everything' (29 December 2023) <https://www.bbc.com/news/world-europe-67691222>

Ellen Nakashima, 'Russian Military Was behind NotPetya Cyberattack in Ukraine, CIA Concludes' (The Washington Post, 12 January 2018) https://www.washingtonpost.com/world/national-security/russian-military-was-behind-notpetya-cyberattack-in-ukraine-cia-concludes/2018/01/12/048d8506-f7ca-11e7-b34a-b85626af34ef_story.html.

Hannon P, 'The Day a Mysterious Cyber-Attack Crippled Ukraine' (BBC Future, 4 July 2017) <https://www.bbc.com/future/article/20170704-the-day-a-mysterious-cyber-attack-crippled-ukraine>

Politico, 'Ukraine Blames Russia for Cyberattack on Critically Important Infrastructure' (2024) <https://www.politico.eu/article/ukraine-blames-russia-for-cyberattack-on-critically-important-infrastructure-olha-stefanishyna/>

Reuters, 'Cyber Attack Hits Ukraine Then Spreads Internationally' (28 June 2017) <https://www.reuters.com/article/us-cyber-attack-ukraine-idUSKBN19M39P/>

Ukrainska Pravda, 'Russian Hackers Attack State Systems before Presidential Elections' (20 December 2024) <https://www.pravda.com.ua/eng/news/2024/12/20/7489933/>

Other Electronic Resources

Andy Greenberg, ‘The Untold Story of NotPetya, the Most Devastating Cyberattack in History’ (Wired, 22 August 2018)

<https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world>

Center for Strategic and International Studies, ‘Significant Cyber Incidents’ (CSIS, 2024)

<https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents>

Council on Foreign Relations, ‘Cyber Operations Tracker’ (CFR, 2024)

<https://www.cfr.org/cyber-operations/>

CyberPeace Institute, ‘Cyberconflicts Platform’ (CyberPeace Institute, 2024)

<https://cyberconflicts.cyberpeaceinstitute.org/>

Europol, ‘Cybercrime’ (Europol, 2024)

<https://www.europol.europa.eu/crime-areas/cybercrime>

Geneva Academy of International Humanitarian Law and Human Rights, ‘Military Occupation of Ukraine’ (RULAC, 2024) <https://www.rulac.org/browse/conflicts/military-occupation-of-ukraine>

Nadiya Kostyuk and Erik Gartzke, ‘Cyberattacks Have Yet to Play a Significant Role in Russia’s Battlefield Operations in Ukraine – Cyberwarfare Experts Explain the Likely Reasons’ (The Conversation, 5 April 2022)

<https://theconversation.com/cyberattacks-have-yet-to-play-a-significant-role-in-russias-battlefield-operations-in-ukraine-cyberwarfare-experts-explain-the-likely-reasons-178604>

NTT Security, ‘Russian Hacker Claims Responsibility for Massive Cyberattack in Ukraine’ (22 December 2024) <https://se.security.ntt/en/russian-hacker-claims-responsibility-for-massive-cyberattack-in-ukraine/>

UK Government, 'Foreign Office Minister Condemns Russia for NotPetya Attacks' (2018)

<https://www.gov.uk/government/news/foreign-office-minister-condemns-russia-for-notpetya-attacks>

UK Government, 'Russia Behind Cyber Attack with Europe-Wide Impact an Hour Before Ukraine Invasion' (2022)

<https://www.gov.uk/government/news/russia-behind-cyber-attack-with-europe-wide-impact-an-hour-before-ukraine-invasion>

Position Papers

Federal Republic of Germany, *On the Application of International Law in Cyberspace* (10 October 2018)

https://ccdcoe.org/uploads/2018/10/Germany_on-the-application-of-international-law-in-cyberspace-data-English.pdf

International Committee of the Red Cross, *International Humanitarian Law and Cyber Operations during Armed Conflict: ICRC Q&A and Commentary* (21 June 2013) <https://www.icrc.org/sites/default/files/external/doc/en/assets/files/2013/130621-cyberwarfare-q-and-a-eng.pdf>

International Committee of the Red Cross, *International Humanitarian Law and Cyber Operations during Armed Conflicts* (2019)

https://www.icrc.org/sites/default/files/document/file_list/icrc_ihl-and-cyber-operations-during-armed-conflicts.pdf

International Committee of the Red Cross, *International Humanitarian Law and Cyber Operations during Armed Conflicts* (2021) 102(913) *International Review of the Red Cross* 483

<https://international-review.icrc.org/sites/default/files/reviews-pdf/2021-03/ihl-and-cyber-operations-during-armed-conflicts-913.pdf>

International Committee of the Red Cross, *The Potential Human Cost of Cyber Operations* (ICRC 2021)

<https://shop.icrc.org/the-potential-human-cost-of-cyber-operations-pdf-en.html>

Rain Liivoja, 'Technological Change and the Evolution of the Law of War' (2015)

<https://international-review.icrc.org/articles/technological-change-and-evolution-law-war>

Reports

Atlantic Council, *Beyond Attribution: Seeking National Responsibility in Cyberspace* (2021)

<https://www.atlanticcouncil.org/in-depth-research-reports/issue-brief/beyond-attribution-seeking-national-responsibility-in-cyberspace/>

European Parliamentary Research Service, *Cyberattacks in the Russia-Ukraine War: Can International Law Cope?* (2023) [https://www.europarl.europa.eu/thinktank/en/document/EXPO_BRI\(2023\)702594](https://www.europarl.europa.eu/thinktank/en/document/EXPO_BRI(2023)702594)

UN GGE, *Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security: Report A/68/98* (24 June 2013)

UN GGE, *Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security: Report A/70/174* (22 July 2015)

Other Sources

NATO Cooperative Cyber Defence Centre of Excellence, 'National Position' (Cyber Law Toolkit, 2024)

https://cyberlaw.ccdcoe.org/wiki/Category:National_position accessed 6 May 2025