Sandra Melani Mellikov

INTERNATIONAL LEGAL RESPONSES TO CYBERATTACKS: DISTINCTIONS BETWEEN PEACETIME NORMS AND THE LAW OF ARMED CONFLICT

AN ANALYSIS BASED ON CYBERATTACKS AGAINST ESTONIA (2007) AND UKRAINE (2022–2024)

Dissertation to obtain a Master's Degree in
Law, in the specialty in Law & Security

Supervisor:
Dr. Laura Iñigo Álvarez, Professor at the NOVA School of Law

September 2025

Anti-Plagiarism Declaration

I hereby declare that the work I present is my own work and that all my citations are correctly acknowledged. I am aware that the use of unacknowledged extraneous materials and sources constitutes a serious ethical and disciplinary offence.

Sandra Melani Mellikov

Declaration

It is stated that, the body of the present Dissertation, consisting of the Introduction, four Chapters, and Conclusion, consists of a total of 195 533 characters including spaces.

Acknowledgements

I would like to express my heartfelt thanks to my dear tutor, Dr. Laura Iñigo Álvarez, for her guidance and support throughout the writing process. Her insightful feedback and encouragement were invaluable in shaping this thesis, and I am deeply grateful for her dedication.

My sincere thanks also go to my friends and family for their unwavering support and motivation. Their belief in me, especially during challenging times, kept me going. I could not have completed this journey without their love and encouragement. Thank you all for being there every step of the way.

I am especially grateful to my dear friend Francisco, who I could always rely on whenever I had questions or needed to hear someone else's opinion about my ideas. His support, understanding, and thoughtful feedback made this process much easier.

Quoting and Other Conventions

This Master's dissertation follows the American Psychological Association (APA) 7th edition citation style. In-text references include the surname(s) of the author(s) or the name of the responsible organization, the year of publication, and, where relevant, the page number(s).

Direct, word-for-word quotations from source materials are clearly indicated using quotation marks followed by relevant in-text citations. The dissertation is written with the rules of American English, with consistent use of spelling, punctuation, and grammar conventions.

"The use of cyberattacks and operations in peacetime and during armed conflicts is today a reality." –

Stéphane Duguin, Pavlina Pavlova (2023). The role of cyber in the Russian war against Ukraine: Its impact and the consequences for the future of armed conflict. European Parliament.

List of Abbreviations

ARSIWA – Articles on the Responsibility of States for Internationally Wrongful Acts

CCDCOE – Cooperative Cyber Defence Centre of Excellence

CERT – Computer Emergency Response Teams

DDoS attack – distributed denial-of-service attack

DoS attack – denial-of-service attack

ENISA – European Union Agency for Cybersecurity

EU – European Union

ICCPR – International Covenant on Civil and Political Rights

ICJ – International Court of Justice

ICRC – Committee of the Red Cross

ICT – information and communication technology

IHL – international humanitarial law

IHRL – international human rights law

IP address – Internet Protocol address

IT – information technology

NATO – North Atlantic Treaty Organization

NIS2 Directive – Network and Information Security Directive

OECD – Organisation for Economic Co-operation and Development

UDHR – Universal Declaration of Human Rights

UN – United Nations

UN GGE – United Nations Group of Governmental Experts

UN OEWG – United Nations Open-Ended Working Froup

Summary

This Master's thesis investigates the responses provided by international law to cyberattacks both in peacetime and in times of armed conflict. In particular, the thesis takes the 2007 cyberattacks against Estonia and the cyberattacks against Ukraine accompanying Russia's full-scale invasion in 2022-2024 as case studies. These examples are used to analyze how international humanitarian law and international human rights law respond to cyberattacks, and what the limitations of the legal frameworks are. In addition, the analysis includes customary international law, UN norms of responsible state behaviour in cyberspace, the UN Charter, and the application of the Tallinn Manual 2.0 to cyberattacks.

The analysis concluded that some notable shortcomings of international human rights law, the UN Charter and the Tallinn Manual, which are applicable in peacetime, as illustrated by the Estonian example, are threshold problems under the UN Charter, as well as the lack of binding enforcement mechanisms. This allows states to evade legal responsibility and civilians, whose human rights are violated through attacks, remain unprotected. The example of Ukraine illustrates how international humanitarian law is applied in parallel with human rights law during armed conflict. In such a situation some of the existing gaps are the distinction between civilian and military infrastructure and whether the cyber operations qualify as an "attack". However, the main gap in both contexts is attribution, largely due to the anonymity of cyberspace. This is further exacerbated by political obstacles within collective security institutions.

A step forward to addressing these problem is offered by the non-binding UN initiative, the UN norms for the responsible conduct of states in cyberspace. These provide guidance on the challenges arising from cyber operations, but due to their voluntary nature, they do not result in sanctions or set out enforcement mechanisms that can be applied in peacetime and in times of armed conflict. Therefore, this thesis concludes that international law needs major changes not only to address current threats arising from cyberspace but also to stay ahead of them. The thesis offers several proposals, including the hardening of the non-binding initiative in order to become binding and supplement it with the missing specifications. An alternative option would be to create a new treaty that is binding from the outset and imposes obligations and protections on states.
Keywords: Cyberattacks – International Humanitarian Law – International Human Rights Law – UN Charter – Tallinn Manual – Attribution – Estonia – Ukraine

Table of Contents

INTRODUCTION

This thesis investigates the legal responses to cyberattacks under international law, focusing on two prominent cases: the 2007 cyberattacks against Estonia and the cyber operations targeting Ukraine from 2022 to 2024. The author chose these cases because the former occurred in peacetime and the latter during an armed conflict, which creates an opportunity for a comparative analysis, assessing the responses and application of international law in two different situations. The main research question guiding this study is: *How does international law respond to cyberattacks in peacetime and during armed conflict, as illustrated by the cases of Estonia (2007) and Ukraine (2022–2024)?* In order to answer this question, the thesis also addresses the following subquestions:

1. What international legal frameworks govern cyberattacks in peacetime and in situations of armed conflict?
2. How have the cyberattacks against Estonia and Ukraine been addressed under international law?
3. What are the key challenges and limitations in the current international legal response to cyberattacks?

The choice of the specific topic stems from the author's broader academic interest in both cybersecurity and public international law, including international humanitarian law (IHL) and international human rights law (IHRL). The increasing use of cyber operations as a method of attack in both peacetime and armed conflict raises important legal questions about the adequacy and adaptability of existing international frameworks. This choice of thesis topic offered the author the opportunity to explore these questions and the intersection of topics of interest in depth. It also allowed the author to delve into the question of how the two branches of international law respond to a rapidly evolving form of warfare and the exponential developments of the digital age. By combining the legal analysis of cyber operations with real-world case studies, the author set out to contribute to a field of research that represents the intersection of law, technology, and international security.

In addition to the legal significance of the legal regime applicable to cyberattacks, the choice of the Estonian and Ukrainian case studies also stemmed from contextual and personal considerations. The principle of including two case studies at a more descriptive level firstly allows for a comprehensive understanding of their background, political context and domestic responses that shape the legal consequences of each case. Second, they illustrate

how international law is related to real-life events. These case studies examine aspects such as the political context of the attacks, the digital landscape, the triggering events, the nature and execution of the attacks, attribution issues, national responses and reforms, and international reactions. Although these chapters being descriptive, they are factual without being legal, and will be followed by legal evaluation later. By providing these factual parts, the thesis ensures that the legal analysis that follows is based on concrete real-life examples and developments, and not just simple abstract theory. The inclusion of national and international responses allows for a full assessment of how international law is applied and tested in practice. This structure helps maintain the necessary balance between empirical context and legal reasoning and allows to draw an informed comparison between cyberattacks committed in peacetime and wartime. The latter illustrates how international law is challenged in different circumstances.

Additionally, since the author is from Estonia, there was a direct personal interest in learning more about an incident that affected the security of their homeland. In addition, the inclusion of the Estonian cyberattacks offers a unique perspective on what is widely considered to be the first major case of a cyberattack against a sovereign state. The consideration of including Ukraine in particular stemmed from the fact that the armed conflict against the state since 2022 has been accompanied by extensive and complex cyber operations, which particularly highlight the application of IHL. These two cases reflect not only two different legal contexts, peacetime and wartime, but also two important moments in the development of cyberconflict.

Although cyber operations against Ukraine are still ongoing, the analysis of this dissertation is limited to the period 2022–2024, not to the present. This defined time period was chosen for methodological clarity and practical reasons. Such a choice allows us to focus on a specific period that has already ended and can be analyzed comprehensively. It also avoids the situation where events may still be developing and for which there may not yet be sufficient information or conclusions. The study is therefore based on publicly available and verifiable information that has already occurred. As the thesis must be completed before the defense in October of 2025, the use of a limited timeframe (2022–2024) allows for a more structured and coherent legal assessment, while capturing the critical phase of cyber operations during the armed conflict.

The aim of this thesis is to explore how international law responds to cyberattacks during both peacetime and armed conflict. Using the 2007 cyberattacks against Estonia and the ongoing cyber operations against Ukraine since 2022 as case studies, the thesis examines the extent to which current international legal frameworks provide adequate guidance, protection, and accountability for state-sponsored or state-affiliated cyber operations. The aim of the dissertation is to identify the main legal principles applicable in each context and to assess whether existing legal provisions are sufficient to deal with the complex realities of modern cyber conflict. While the legal framework applicable during armed conflict, which also covers cyber operations, is based on well-established principles of IHL, the application of international law to the regulation of cyberattacks in peacetime is much more vague and would require a clearer framework.

Cyberattacks have become real and everyday threats that challenge both international security and international law and its adequacy. As state and non-state actors increasingly use cyber tools to influence, disrupt or undermine the infrastructure and sovereignty of other states, there is a serious need to assess whether existing legal norms and frameworks provide sufficient normative clarity for responding to such incidents. This dissertation is relevant for several reasons. First, because it addresses a serious and increasingly evolving threat to international stability, and second, because it contributes to a nascent field of law. By analysing two landmark cases from different legal contexts, this thesis highlights the strengths and weaknesses of existing legal measures and supports the idea of developing a legal framework for the application of international law to cyberattacks in peacetime.

Although the main objective of this thesis is to address the legal response to cyberattacks based on whether the attack was carried out in times of armed conflict or peace, rather than the issue of attribution, it is also important to note that both Estonia and Ukraine have a complex geopolitical context. Namely, in relation to the Russian Federation, which is widely perceived as the perpetrator of the attacks. As former Soviet republics bordering the Russian Federation, both countries have had turbulent relations with Russia. In the case of Estonia, the final attribution of the 2007 cyberattacks to the Russian state has not been conclusively proven, but the attacks coincided with a period of increased political tensions with Russia and are widely believed to have originated from actors representing Russian interests. (Ottis, 2008, p. 6) On the other hand, the cyberattacks against Ukraine since 2022 have occurred in time with the full-scale military invasion that began on 24th of February 2022, which makes

the potential involvement in cyberattacks more direct. As mentioned above, the aim of this thesis is not to resolve the question of who should be attributed for the attacks, but the connection to Russia is a common denominator in these cyberattacks and helps to understand the legal and political challenges associated with the attacks.

This dissertation uses a doctrinal legal research methodology, focusing on the analysis and interpretation of international legal norms in relation to cyberattacks. The dissertation examines the main sources of international law, including treaties, customary international law, legal principles, as well as academic research. Particular attention is paid to the applicability of IHL and IHRL, as well as academic teachings, such as the non-legally binding Tallinn Manual 2.0, which reflects international law applicable to cyber operations. In order to more closely assess how international law responds to cyberattacks in different contexts, the dissertation also uses a comparative case study approach. The analysis is structured around two case studies, namely the cyberattacks against Estonia (2007) and Ukraine (2022–2024), in order to specifically assess and compare how international law is applied in both peacetime and wartime contexts. While the dissertation relies on factual reports and state responses to contextualize legal issues, it does not engage in technical attribution or cyber forensic analysis, as these fall outside the scope of the research method.

The research problem arises in connection with the rapid increase in state-sponsored cyberattacks, which have clearly highlighted critical gaps in international legal frameworks and their application. The 2007 cyberattacks against Estonia and the ongoing cyber operations against Ukraine since 2022 raise serious questions about how well existing international legal norms address the conduct, accountability and consequences of cyberattacks both in peacetime and in armed conflict. This dissertation examines whether current international law frameworks, including among others IHL and IHRL, are adequately equipped to regulate such cyberattacks, which are international law's responses to such situations, and identifies the legal limitations of the application of these frameworks in the modern digital age, where cyberattacks have become the norm.

This dissertation is divided into four main chapters, supplemented by an introduction and a conclusion. The first chapter serves as a foundational overview. It establishes core concepts (e.g., definitions of cybersecurity, cyberattacks, sovereignty), briefly introduces relevant legal frameworks (UN Charter, Tallinn Manual, etc.), and frames the relevance of cyber operations in international law. The following second chapter covers the 2007 cyberattacks

on Estonia and provides an overview of the background, timeline, types of attacks, and impact of the attacks. The third chapter is structured similarly to the second chapter, but focuses on the cyberattacks against Ukraine from 2022 to 2024. The fourth chapter represents a legal analysis of how international law legally responds to cyberattacks, in which the author applies international law in peacetime (Estonia) and during armed conflict (Ukraine), finds out the challenges and gaps, as well as compares and draws out differences and similarities and evaluates adequacy of current international legal framework. The second and third chapter are descriptive and based on facts, events and outcomes, whereas the fourth chapter is analytical and contains legal and conceptual evaluation.

1. FOUNDATIONS OF CYBERSECURITY AND INTERNATIONAL LAW

1.1 The Modern Cybersecurity Landscape

As technology has advanced rapidly in recent decades, it has also led to more digital services and automation. (Aslan et al., 2023, p. 13) With the growing digitalization of society, a new domain called cyberspace has emerged as a permanent and integral part of daily life and is here to stay. (Mueller et al., 2023, p. 16) This development in turn has led to greater connectivity and interdependence, which has placed more systems in the category of critical infrastructure and deepening modern society's reliance on digital systems and technology. Critical infrastructure is used every day in modern society and allows us to live a secure and uninterrupted life. Examples of such systems include energy production and distribution systems, financial services, communication systems, water and sewage systems, and healthcare. If these systems were to fail, the smooth running of everyday life would be seriously disrupted. However, cyberattacks against these systems have been on the rise. (Aslan et al., 2023, p. 13)

The development of digitalization and globalization has changed the modern security environment, both in theoretical and practical terms. (Štrucl, 2022a, p. 105) The problem in today's world arises when the Internet is actively and daily used in various sectors, such as education, communication and business, and the lack of access to Internet networks as a result of successful cyberattacks begins to negatively affect this active and daily use. The situation is especially harmful when the attacks, due to their severity, make national security vulnerable. (Terlikowski, 2007, p. 79) In response, cybersecurity has a significance in maintaining the availability and integrity of digital networks and infrastructure, as well as the confidentiality of the information they contain. (European Commission, & High Representative of the Union for Foreign Affairs and Security Policy, 2013)

Building on this, cyber systems have increasingly become part of modern warfare. Cyberwarfare is now an inseparable component of military defense and cyber security. (Estonian Ministry of Defence, 2017, p. 12) Technological progress is rapid and accelerating, and its impact is clearly felt in security and warfare, as well as in people's everyday lives and behaviour. Modern smart technologies and their applications are paving the way for the next generation of intelligent technologies that can not only analyse information, but also make

decisions autonomously. (Estonian Ministry of Defence, 2017, p. 21) The benefits of the information age are numerous, but emerging threats to national cybersecurity, such as cyberattacks, put national security at risk. (Herzog, 2011, p. 56)

However, cyberwarfare differs significantly from traditional armed conflict. Namely, the goal of traditional war is to conquer land, expand one's own territory, gain access to useful resources, or achieve political control over the opponent. In the case of cyberwar, on the other hand, the goal cannot be to expand territory, because there is no defined territory in cyberspace and digital battles are not about acquiring resources. However, cyberwar can be related to achieving political power or at least political influence. In addition, cyberwar can be a supporting element in conquering territory or accessing resources, in order to undermine the opponent's necessary systems and means of defending itself during a traditional war. (Inversini, 2020, p. 262)

Cybersecurity is put to the test on a daily basis by malicious cybercrimes, ranging from the simplest to the most technologically sophisticated and devastating cyberattacks. (NATO, 2024) Despite cyberattacks typically being non-kinetic in nature, therefore usually being non-lethal, they can still have significant consequences for civilians and fundamental rights. Specifically, cyberweapons are made of computer code, which means they do not directly cause physical or physiological harm and do not kill, but they still can cause damage. Many cyberattacks cause economic damage or service disruption rather than direct physical harm and can still in some cases violate the right to life, making it more difficult to identify human rights violations. (Fidler, 2014, p. 305) Attacks on internet technology can also leave people without access to critical information, the ability to express themselves, work, learn and access social services, as they could potentially lead to internet shutdowns. (Brown, 2020)

1.2 Definitions and Terminology

As this thesis focuses on the legal frameworks surrounding cyber operations, it is crucial to clarify key concepts such as cybersecurity, cyberspace, cyberattack, and cyberwarfare. These terms are often used in both technical and legal contexts, but they are yet to be defined consistently across different institutions, legal frameworks, or academic literature. For this reason, the following section presents a selection of widely referenced definitions to highlight the varying interpretations of these key words related to the topic.

Starting with cybersecurity, there has been an attempt to find a single global definition to it, but different organizations have taken different approaches to its meaning. For instance, The European Union Agency for Cybersecurity (ENISA) has stated in its 2015 paper "Definition of Cybersecurity – Gaps and overlaps in standardisation" that there is no one concrete definition to the concept. The organization's approach is that: "There does not need to be a definition for Cybersecurity in the conventional sense that we tend to apply to definitions for simple things like authentication of an identity (a security mechanism allowing the verification of the provided identity). The problem is that Cybersecurity is an enveloping term and it is not possible to make a definition to cover the extent of the things Cybersecurity covers." (The European Union Agency for Network and Information Security [ENISA], 2015, p. 28)

Although ENISA admitted that there is no definition to cybersecurity, they explain that: "Cybersecurity shall refer to security of cyberspace, where cyberspace itself refers to the set of links and relationships between objects that are accessible through a generalised telecommunications network, and to the set of objects themselves where they present interfaces allowing their remote control, remote access to data, or their participation in control actions within that Cyberspace." (ENISA, 2015, p. 7)

The EU 2013 Cybercrime Strategy defines cybersecurity as "safeguards and actions that can be used to protect the cyber domain, both in the civilian and military fields, from those threats that are associated with or that may harm its interdependent networks and information infrastructure. Cyber-security strives to preserve the availability and integrity of the networks and infrastructure and the confidentiality of the information contained therein." (European Commission & HR/VP, 2013)

Reference to the term is also found in the NIS2 directive. (European Parliament & Council of the European Union, 2022) It is the EU's updated framework for cybersecurity with an aim to strengthen cybersecurity across the EU by setting a high standard of security for network and information systems. (NIS2 Directive, n.d.) Article 6, point (3) of the directive states that: "'cybersecurity' means cybersecurity as defined in Article 2, point (1), of Regulation (EU) 2019/881". (European Parliament & Council of the European Union, 2022, art. 6) This regulation which is known as the Cybersecurity Act published in 2019, defines cybersecurity in Article 2, point (1) as: "the activities necessary to protect network and

information systems, the users of such systems, and other persons affected by cyber threats". (European Parliament & Council of the European Union, 2019, art. 2)

In contrast to different EU definitions, that are broader and protect networks and users, Merriam-Webster Dictionary definition is simplistic and focuses more on the technical side. It defines "cybersecurity" as "measures taken to protect a computer or computer system (as on the Internet) against unauthorized access or attack". (Merriam-Webster, n.d.)

Having outlined the definitions of cybersecurity, it is important to also define the activities that pose a major threat to maintaining cybersecurity. These are cyberattacks. The definition of a cyberattack in the context of IHL can be found in the Tallinn Manual 2.0. It defines a cyberattack as "a cyber operation, whether offensive or defensive, that is reasonably expected to cause injury or death to persons or damage or destruction to objects." (Schmitt, 2017a, p. 415) The non-legally binding Tallinn Manual 2.0 is a follow-up to the original Tallinn Manual, which was published in 2013. The first version covers the most serious cyber operations, those that violate the prohibition on the use of force, give rise to a situation in which states have the right to exercise the right of self-defense, or occur during an armed conflict. The Tallinn Manual 2.0, published in 2017, is more based on the framework of international law. Thus, while being non-binding, the Tallinn Manual 2.0 applies to cyber incidents between states that fall below the threshold of the use of force or armed conflict. (NATO Cooperative Cyber Defence Centre of Excellence [CCDCOE], n.d.)

Similarly to cybersecurity and cyberattacks, there is also no globally accepted definition for cyberwarfare. The term remains contested. Namely, cyberwar and cyberwarfare are often used synonymously, but there are also experts who believe that cyberwarfare requires violence. (Štrucl, 2022a, p. 114) This further highlights the amibuity of cyber-related terminology.

To have a deep understanding of the aforementioned terms, we also need to understand the environment where cybersecurity, cyberattack and cyberwarfare take place. This domain is cyberspace. It is a system where various objects are connected and accessible through a telecommunications network. These objects are connected by interfaces that allow remote control, data access, or participation in cyberspace activities. (ENISA, 2015, p. 30) Cyberspace is a double-edged sword. It presents itself as an asset, a tool for the information environment, but on the other hand it can be seen as both a source of threat and a subject of

threat. (Štrucl, 2022a, p. 105) For the attacker, it is the perfect domain to use their weapons at the speed of light since any borders, walls and oceans lose all meaning of longstanding protection. If the goal is to keep cyberspace safe and protected, it requires human intervention. Other domains, sea, land and air, have not been created by human unlike cyberspace has. Therefore, for cyberspace to keep existing, it must rely on a combination of public and private sector and their contribution and interference. (Smith, 2022)

In conclusion, there is no universally accepted definition for cybersecurity or any other relevant terms to this thesis. Institutions and experts have been offering slightly different interpretations that vary in scope and emphasis. This definitional ambiguity for the terms presents challenges for the consistent application of international law and poses complications for the efforts to regulate cyber activities at the global level.

1.3 Understanding Cyberattacks

Beyond various definitions to cyberattacks, it is necessary to understand how cyberattacks operate in practice, what roles they play and forms they might take. Cyberattacks, especially large-scale and state-sponsored, can potentially cause immense harm to various essential or important entities that people need to have access to daily. (Tran, 2018, p. 380) The term "cyberattack" is often used broadly, but it is not always used in the right context. The term is closely linked to the notion of "information warfare", which is broader than “cyberattack”, but represents its offensive aspect. In practice, information warfare activities involve various manipulations in information and communication technology (ICT) systems, which might lead to negative consequences. The main system is the Internet, which is easily accessible as a global information technology (IT) network and therefore the biggest victim of manipulations. Cyberattacks, being part of the concept of information warfare, can be divided into several categories depending on the technical methods of their perpetration, goals and results. (Terlikowski, 2007, p. 69)

One way to classify cyberattacks, for instance, is by the motivation behind them. The largest group of attacks is called cybercrime and mainly includes attacks, i.e. fraud, theft and other illegal activities committed via IT networks. A second category is also common, these are mainly committed by criminals who want to prove their technical abilities or are motivated by strong emotions. This involves creating malware or hacking into computers. The newest group is hacktivism, which is carried out by individuals or groups motivated by achieving political or ideological goals. Thus, they mainly attack governments or other vulnerable

organizations. The most serious subtype is cyberterrorism, which are politically motivated activities aimed at using ICT systems as weapons. The aim is to cause physical destruction or damage, for example by seriously disrupting critical infrastructure. (Terlikowski, 2007, pp. 69-70) This classification shows how cyberattacks can range from financially motivated to politically motivated crimes that all threaten people's safety and daily lives.

Beyond their motivation, cyberattacks tend to develop through a series of phases, even though they might seem to be instantaneous. These phases typically consist of five general steps, similar to how traditional crimes unfold. The first phase is reconnaissance where the attacker observes the target to gather necessary information like the hardware, software, and communication patterns used by the victim that helps to plan the attack in the most successful way. Second, there is penetration when the attacker gains access to the system. Until this step is taken, attackers can only disrupt services but not cause serious harm yet. Next there is expansion which means that once the attacker is inside the system, they look for ways, such as more valuable areas to access to expand the attack in order to cause more harm. Fourth, the attacker causes actual harm to the system or steals information. Lastly, the attacker covers any traces of their action to avoid getting detected. (Janczewski & Colarik, 2007, p. 15) This well structured process illustrates that cyberattacks are intentional and planned, rather than spontaneous endeavors.

Cyberattacks are carried out with the aim of targeting only a country's internet infrastructure, but we often hear about attacks that are carried out as part of a larger and more widespread attack. This means that cyberattacks often follow or accompany physical attacks, which shows the integration of cyber operations into conventional military conflicts, highlighting the hybrid nature of modern warfare. (Janczewski & Colarik, 2007, p. 14) A successful cyberattack requires real effort, not just dramatic disruption. It requires adequate planning, tool development, and intelligence. While kinetic weapon attacks can potentially cause destruction depending on their success, cyberattacks do not. For example, if a radar is hit by an armed attack, it will be reduced to rubble, but in the case of a cyberattack on a radar, it is not immediately apparent whether the radar has been seriously damaged or not. (Lewis, 2022, p 2) Therefore, the effects of cyberattacks tend to be less visible than those of physical attacks, while both can be equally destructive.

Cyber operations have their own special value, but it becomes particularly evident in the military domain. In modern warfare, cyberattacks are most successfully carried out in

conjunction with electronic warfare, disinformation campaigns, anti-satellite attacks, and precision-guided munitions. Cyberattacks aim to undermine an adversary's information infrastructure and intangible assets (such as data), communications, intelligence assets, and weapons systems. Cyber operations are also used to achieve political influence, primarily by disrupting the smooth functioning of finance, energy, transportation, and government services, thereby causing social, economic, and political harm at both the national and individual levels. (Lewis, 2022, p. 2) Thus, cyberattacks are serious activities that can harm whole societies, not just specific IT systems.

As will be explained in the following chapters, the main cyberattacks against Estonia and Ukraine have been political distributed denial-of-service (DDoS) attacks. DDoS attacks are always aimed at disrupting the normal functioning of websites for all their users. The attacks use computers that are infected with botnets or zombie army robots, or they can be tools installed onto people's computers without their knowledge. The easiest way to carry out a DDoS attack is to constantly reload and open a website in large numbers. (Nazario, 2018, pp. 1-2) By doing this, the fake requests exhaust a pool of Internet Protocol (IP) addresses and slow down the server's responsiveness. (Aslan et al., 2023, p. 27) This is usually done from several different locations, making it unmanageable for website managers to filter users and thus prevent malicious users from accessing it. (Nazario, 2018, pp. 1-2) DDoS attacks are considered one of the most destructive forms of cyberattacks as they directly harm the right of legitimate users to access systems. So far, no system has been able to be created that can completely stop DDoS attacks. (Aslan et al., 2023, p. 10)

In addition to cyberattacks, there are other types of cyber operations that usually do not cross the threshold of armed conflict or the use of force. One of these is cyber espionage. One such operation is cyberexploitation, which is commonly used in modern espionage. Although this method can be very invasive, it does not usually qualify as the use of force under international law. Espionage activities are generally not considered armed attacks unless they involve physical intrusion into a country's territory. Such an example would be intelligence gathering by a warship operating in a country's territorial waters. (Schmitt, 2011, p. 576)

As Christian-Marc Liflände once outlined: “Unlike troop buildups or other forms of military mobilisation that are infrequent and highly visible, cyber operations are the result of operational cycles that occur covertly and continuously through peacetime and wartime.” (Duguin & Pavlova, 2023, p. 6) This perspective highlights the difference of cyberattacks

from traditional military operations. They are not isolated disruptions but a part of a larger cycle that affects both peacetime and wartime, often without immediate detection.

1.4 Hybrid Warfare and Cyber Integration

Hybrid warfare is a strategic blend of conventional and irregular warfare methods. In a conflict like this, adversaries combine state-level military capabilities with irregular tactics, such as terrorism, insurgencies, and cyberwarfare. Hybrid warfare can be described by complexity, fusion, and simultaneity at operational and tactical levels, whereas in traditional or compound wars forces operate separately in different areas. In hybrid wars, both state and non-state actors could blend high-tech military systems, like anti-satellite weapons, with more irregular forms of warfare, such as cyberattacks targeting financial systems. (Hoffmann, 2009, pp. 36-37) Such a blending makes hybrid warfare far more unpredictable and challenging to respond to.

The ongoing war in Ukraine has shown directly how cyber capabilities are increasingly being used as a dangerous weapon in conventional warfare. This addition, however, makes the nature of war increasingly complex and acts as a force multiplier alongside conventional military operations. (Schulze & Kerttunen, 2023, p. 1) While there is a general global consensus that cyber activities during armed conflict can fall under military activity, there remains no unified agreement on the rules that should apply to cyber activities. (Hathaway & Klimburg, 2012, p. 18)

Despite its growing role, cyberwarfare has limitations, one of which is the disability to lead to territorial gains without physical combat and violence, which is one of the primary goals of most modern wars. ((Schulze & Kerttunen, 2023, p. 2) However, when integrating cyber operations to conventional wars they can play a crucial role in weakening an adversary's defenses or destabilizing societies in the lead-up to kinetic conflict.

In conclusion, the integration of cyber tools into hybrid warfare strategies demonstrates a transformation of the modern battlefield, where physical world can also start to feel the consequences of actions initiated in cyberspace. This shift challenges existing legal frameworks by blurring the line between peace and conflict.

1.5 Jus ad Bellum in the Context of Cyber Operations

While the principles of *jus ad bellum* regulate the use of force in international relations, their application to cyberspace poses significant challenges. One of the main difficulties is

identifying attackers in digital space. Unlike in the physical world, where state actors are easily identifiable, cyberattackers can conceal their identity through proxies, false flags, the anonymity of cyberspace, or other disguises, making it difficult to attribute attacks. This complicates the process of declaring war, as states often deny involvement in cyberattacks, even if they could be considered acts of war. (Inversini, 2020, p. 261)

This leads to another core element in the application of *jus ad bellum* to cyberspace, which is the right of a state to defend its territorial and political sovereignty. While political sovereignty can easily be threatened, it is difficult to determine when such intrusions justify self-defense. In cyberspace, attackers can destabilize a state by disrupting critical infrastructure or manipulating key systems. These attacks can undermine the stability of a state even without direct physical confrontation. Adapting the concept of territorial sovereignty to the digital world is difficult because cyberattacks often cross physical borders and the concept of territoriality becomes diffused which raises unresolved legal and practical challenges. (Inversini, 2020, p. 261)

Although *jus ad bellum* is grounded in Article 2(4) and Article 51 of the UN Charter, a more detailed analysis of their application to cyberspace will be addressed in a later subchapter.

1.6 Principle of Sovereignty

While the previous subchapter addressed political sovereignty in the light of *jus ad* bellum, the principle of sovereignty over cyber infrastructure also requires highlighting. Tallinn Manual 2.0 states this through Rule 1, which affirms: “The principle of State sovereignty applies in cyberspace.” (Schmitt, 2017a, p. 11) Sovereignty is a core principle of international law that gives states the right to control cyber infrastructure and related activities within their borders. While territoriality is central to sovereignty, there are situations in which states may extend their sovereign rights beyond their own territory to include cyber infrastructure and related activities outside their territorial jurisdiction, and to control people associated with those activities. (Schmitt, 2017a, p. 11) Additionally, just because a state's cyber infrastructure is connected to the global network i.e. cyberspace, it does not mean the country gives up its sovereignty over that infrastructure. The state still remains the right to disconnect its cyber infrastructure from the Internet, either fully or partially. However, this right is not absolute. It can be limited by international law, particularly by treaties or customary international law, including obligations related to human rights. In any case, the state must respect international legal commitments, especially

those protecting human rights. (Schmitt, 2017a, pp. 12-13) This demonstrates that cyberspace does not diminish the principle of sovereignty, it rather is extended into a new domain, while still falling within the scope of international law.

1.7 United Nations Framework

Since this thesis examines cyberattacks against Estonia and Ukraine, it is crucial to consider the United Nations (UN) framework, which regulates the use of force and safeguards state sovereignty. Estonia and Ukraine both being Member States of the UN, means that the UN Charter applies to both of them. Article 2(4) of the Charter states: "All Members shall refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any state, or in any other manner inconsistent with the Purposes of the United Nations." (United Nations, n.d.-a, Art 2(4)) As mentioned before, the principle of territoriality lies in sovereignty, and it holds up this principle. Sovereignty allows states to control the entire cyber infrastructure within their borders. As argued in the Tallinn Manual 2.0, sovereignty extends beyond the physical world to cyberspace, where a state retains control over its cyber activities even when connected to the global network. Therefore, a cyberattack that targets a state's cyber infrastructure or aims to violate the territorial integrity of a state is a direct violation of the principle of territoriality and therefore a violation of sovereignty. This is in line with Article 2(4), which prohibits activities that threaten or undermine the physical or virtual territorial boundaries of a state. Given that cyberattacks often involve activities that violate state borders in the digital realm, they effectively challenge the territorial integrity of states. Consequently, such attacks can be considered a violation of international law, as they are contrary to the Charter of the United Nations.

However, not every cyber operation that violates sovereignty or international law constitutes an "armed attack" under Article 51 of the UN Charter. Article 51 is about the right to self-defense through military action individually or collectively for a UN Member State who has been attacked. There have been discussions about whether a cyberattack could fall under an armed attack and therefore this specific article. In order to respond to an attack in self-defense and trigger Article 51, the attack must be armed. This raises a question whether a cyberattack is armed or not. (Ekstedt, Parkhouse, Clemente, 2012, pp. 169-170) An "armed attack" usually refers to the use of kinetic military force, which means it involves physical military action like bombing, shooting, or physical harm to humans or infrastructure or any other tangible object. This means that the critical element to an armed attack is whether the

attack causes harm or damage that is comparable to what an armed attack would cause, not just the method the attacks are carried out with. (Schmitt, 2011, p. 588) Cyber operations that cause physical harm to individuals or material objects are equated with attacks using armed force and therefore also constitute the use of force. For example, attacks targeting air traffic control systems directly endanger people and property.

However, according to the Tallinn Manual 2.0, the question of what type of damage constitutes an armed attack is much deeper than it seems. Namely, there is disagreement among experts regarding economic damage. Some experts are of the opinion that only cyberattacks that result in death, injury or physical destruction qualify as armed conflict. Others believe that the physical nature of the damage is not a weighty factor, but rather the extent of the consequences should be assessed. According to opinion of the latter, for instance, a stock market crash as a result of a cyberattack is a serious disruption that reaches the threshold of an armed attack even if there is no visible physical destruction. (Schmitt, 2017a, pp. 342-343) This means that the issue remains unsettled and it deepens the uncertainty about the application of Article 51 of the UN Charter to cyberattacks.

In the case of the situation that erupted in Estonia in 2007, there were no such consequences as physical harm to individuals or material objects. Therefore it cannot be equated with the use of force. (Schmitt, 2011, p. 573) For a cyberattack to be considered an armed attack, it needs to have consequences similar to those of traditional military attacks that cause physical harm such as death, injury or property damage. Therefore, cyberattacks that do not lead to these sorts of consequences can still be unlawful but do not qualify as an "armed attack" under international law and thus do not allow the state to use forceful self-defense with military force under Article 51 and international law. (Schmitt, 2011, p. 588)

This distinction is crucial for understanding legal responses to cyberattacks during both peacetime and wartime. In peacetime, only those cyber operations that qualify as an “armed attack” under Article 51 of the UN Charter are allowed to be responded with military force by a state affected. (Schmitt, 2011, p. 588) Attacks with lesser intrusions must be addressed through non-forceful means. (Ekstedt, Parkhouse, Clemente, 2012, pp. 169-170) In wartime, IHL applies to cyber operations that qualify as “attacks” under its framework. Therefore, the legal threshold between a prohibited use of force and an armed attack directly affects how and when are states allowed to respond to cyber operations following legal principles, both during peacetime and armed conflict.

War is considered justified only for national self-defense or humanitarian reasons. To invoke self-defense, a state must show that there has been an armed attack that threatens its sovereignty and independence, and that another state has committed the attack and is therefore responsible for it. Thus, the main challenges in applying the UN Charter to cyberattacks lies both in determining when attacks reach the threshold of an armed attack and identifying the responsible party for attribution. (Inversini, 2020, p. 261)

1.8 European Union Strategy

While the UN provides international framework for addressing sovereignty and the use of force, the European Union (EU) has also taken its approach towards the growing challenges of cyberspace. The existence of the internet has major important consequences for the EU's fundamental values of the rule of law, fundamental rights, freedom and democracy, among others. The high degree of openness and globalisation of cyberspace is constantly being exploited to achieve or disseminate political and ideological goals, which in turn exacerbates polarisation. This, however, poses a serious hybrid threat in the form of cyberattacks on infrastructure, economic processes and democratic institutions, with a high probability of physical, political and social damage. The EU, therefore, believes that it is essential to cultivate the development and diffusion of cybersecurity in order to, among other things, protect people's fundamental rights and freedoms, including the right to privacy and the protection of personal data, as well as freedom of expression and information. (European Commission, 2020)

One strategic step the EU has taken to tackle cyber threats is the enforcement of the EU Cybersecurity Strategy. The aim of this initiative is to protect citizens and businesses and work towards gaining as much benefit as possible from digital technology. An important aspect of this strategy is valuing human rights. (European Commission, n.d.) This illustrates how the EU treats cyber threats also as human rights challenges and not just security challenges. Another initiative of the EU is the Network and Information Security (NIS2) Directive about European cybersecurity. It states security requirements for operators of critical infrastructure and essential services, focusing on regulatory responses. (NIS2 Directive, n.d.) An additional key instrument is the EU’s Cyber Diplomacy Toolbox, which concentrates on joint diplomatic responses against malicious cyber operations. This, also, supports further promotion of security in the cyberspace. (The EU Cyber Diplomacy Toolbox, n.d.) In sum, the EU’s strategy goes beyong just focusing on the technical aspects

of cybersecurity as it also links the protection of human rights to its goals. By combining strategic, regulatory, and diplomatic measures, the EU is a key actor on standards in cyberspace.

1.9 NATO and Collective Defense

NATO has increasingly recognized cyberspace as a domain of security, promoting it as a free, stable and secure environment while acting in accordance with international law, including the UN Charter, IHL and IHRL, where applicable. (NATO, 2024)

Following the 2007 attacks on Estonian public and private institutions, the Allied Defence Ministers agreed that major changes were needed in the field of cyber defense, resulting in the first NATO Cyber Defence Policy in 2008. (NATO, 2024) Since then NATO has been taking steps to develop its approach to cyber threats.

A key legal foundation for NATO's response to cyber threats lies in Article 5 of the North Atlantic Treaty, which reflects the changing nature of conflicts in the digital age. Article 5 constitutes the principle of collective defense among Member States. It lays down that an armed attack against one or more NATO Member States is to be considered an attack against all Member States. This demonstrates the commitment of Member States to defend each other in times of need. Each Member State has the obligation to assist the attacked party, but has the right to decide for itself what measures it deems necessary in a specific situation. A measure like this could be the use of armed force, to restore and/or maintain security in the North Atlantic area. This central principle of NATO aims to deter potential aggressors and ensure the collective security of the Alliance. (NATO, 2023)

Although NATO's Article 5 has only been invoked once, after the September 11 terrorist attacks in the United States, its application to cyberattacks has been steadily acknowledged. For instance, in 2014 during the Wales Summit Declaration NATO affirmed that there is a possibility that a cyberattack could also trigger Article 5. However, there are no precise criteria by which to specifically assess the possibility of triggering Article 5. Due to the lack of clarity in the criteria, each attack must be assessed on a case-by-case analysis, taking into account the seriousness, scope and political motivation of the attack. This ambiguity acts as a deterrent that significantly discourages countries from attempting to invoke Article 5 and also as a challenge for legal clarity, which leaves states confused about the exact threshold for initiating

collective defense in the cyber domain. Cyberattacks have been a challenge for NATO for years, and Russia has been the main initiator of cyber activity and thus a threat to NATO. (Prucková, 2022)

Furthermore, in 2016, at the Warsaw Summit, the Allies reached a consensus and declared that cyberspace was a new domain, just like air, land and sea. Thus, it was confirmed that cyberspace would also become a core task for collective defense, an attack on which would trigger Article 5. (Prucková, 2022) Since the subject of this Master's thesis is cyberattacks against Estonia and Ukraine, it is important to mention that attacks against either country have not triggered the use of Article 5. In the case of Ukraine, the simple reason is that Ukraine is not a NATO Member State, but nevertheless received a lot of assistance from the alliance. In the case of Estonia, the reason for not triggering the article is that the seriousness of the attack did not exceed the threshold for the application of the article. Although the attacks against Estonia were severe, the overall situation did not reach a threshold where military collective defense would be necessary. (Ekstedt, Parkhouse, Clemente, 2012, p. 182) Despite that, the Estonian case marked a turning point by which the cyber dimension and its protection became an increasingly important goal. (Lindstrom & Luiijf, 2012, p. 52)

1.10 Attribution and State Responsibility under International Law

In international law, attribution is central to determining whether a state bears responsibility for conduct, including cyber operations. (Barrier & Subedi, 2020) Although the aim of this thesis is not to attribute cyberattacks to particular actors, it draws on widely held views about potential states that have committed cyberattacks. Understanding the legal framework of attribution is nonetheless important in assessing how international law responds to cyberattacks.

Attribution in cyberspace is widely considered one of the most complex challenges in international law. Without attribution, malicious actors could operate with impunity, causing harm without fear of consequences. Cyberattacks offer state actors a perfect opportunity to strike anonymously and avoid retribution. On the one hand, the architectural anonymity of the internet is one of its strengths, but on the other also makes it difficult to trace the source of the attacks. Although attribution is often viewed as a technical challenge, the real issue lies in determining legal responsibility. While technical attribution seeks absolute certainty through digital evidence, legal attribution focuses on assigning responsibility for a wrongful act to a state. (Tran, 2018, p. 381)

Although identifying the source of a cyberattack, such as the attacking machine or its IP address, has become easier and faster in recent years, the laws around cyberattack attribution are still unclear. One reason is that there are often delays in achieving attributions despite the fact that technology has improved immensly. Attackers make this harder by hiding their identities or making the attack look like it came from someone else. In addition, not being able to identify the source of an attack can lead to confusion and increase the risk of further conflict. (Banks, 2021, p. 1046)

The issue of attribution and responsibility in the context of cyber operations, specifically of cyberattacks in the case of the subjects of this thesis (Estonia and Ukraine), is integral to the application of international law. Tallinn Manual 2.0 Rule 14 states that a state is internationally responsible for cyber operations when two conditions have been met. First, it must constitute a breach of an international legal obligation applicable to that State. And second, it is attributable to the State under international law. (Schmitt, 2017a, p. 84) This also reflects Customary International Law stated in Articles on the Responsibility of States for Internationally Wrongful Acts (ARSIWA). Article 2 of ARSIWA states that for a State to bear international responsibility when two conditions must be fulfilled. These are the same conditions stated in Tallinn Manual 2.0: there must be a breach of an international obligation and the conduct must be attributable to the State under international law. (United Nations, 2001, art. 2) This means that the two legal instruments share the same approach, Tallinn Manual 2.0 in specific just adopts it in the cyber context.

Tallinn Manual 2.0 further clarifies specific circumstances in which attribution applies. The concept arises when cyber operations are either conducted by state organs (Rule 15) (Schmitt, 2017a, p. 87), entities empowered to exercise the elements of governmental authority (Rule 16) (Schmitt, 2017a, p. 93), or by non-state actors that act under the instructions, direction, or control of the state (Rule 17) (Schmitt, 2017a, p. 94). In such cases, cyberattacks can be directly attributed to the state. Furthermore, based on Rule 15 of the Tallinn Manual 2.0, the State is found responsible when its organs act *ultra vires* as in they act beyond the State's authority or goes against its orders. (Schmitt, 2017a, p. 89) According to the due diligence principle under Rule 6 of the Tallinn Manual 2.0, every State is expected to take reasonable steps to prevent cyber operations originating from its territory that cause significant harm to other States. The Manual does not affirm that failing to do so will automatically amount to responsibility but it might give raise to bearing responsibility.

(Schmitt, 2017a, p. 30) In practice, attribution under these rules is difficult, especially when states deny their involvement or take advantage of the anonymity of cyberspace, leaving the rules largely theoretical.

Although this chapter has outlined the key concepts, definitions and legal foundations related to cybersecurity and cyber conflicts, it is important to highlight that in international law there is a difference between cyberattacks during peacetime and armed conflict. This distinction also results in the application of different legal frameworks. In the following chapters, the author of the thesis examines how these frameworks are applied in practice, using cyberattacks against Estonia and Ukraine as examples.

2. CYBERATTACKS AGAINST ESTONIA IN 2007

2.1 Background: Estonia's Digital Landscape and Russian Relations

Estonia is an independent democratic country located in Northern Europe on the European Union's border. (Council of Europe, n.d.) Despite the small population and size of the country, Estonia is known for its high digital connectivity and cyber capabilites. When talking about Estonia, one can equate the state itself with a digital state. Developments in cyberspace carry out to real life and affect Estonia's daily affairs. (Estonian Information System Authority, 2023, p. 7) The development of cybernetics began in Estonia in the 1980s, laying the foundations for the region's public administration and economy to be best prepared to enter the digital age after the restoration of independence. Even before the turn of the century, Estonia stood out from other Eastern European countries for its digital services and high levels of internet connectivity and has been at the forefront ever since. (Bógdał-Brzezińska, 2023, p. 26)

By the mid-2000s, Estonia had achieved a high position in the digital society and internet integration, being at the forefront of this. Furthermore, Estonian society relied heavily on online services such as banking, communication and even voting in elections, but also on basic information sharing and entertainment. (Terlikowski, 2007, p. 71) In addition, by the same year 97% of all banking transactions were being conducted online. The spread of the Internet was deeply rooted in everyday life, with around 60% of the population using the Internet on a daily basis, which reflected Estonia's early and widespread adoption of digital infrastructure. (Ruus, 2008, p. 3) The Internet was involved in services related to school and university education, paying bills and filling in and submitting applications. Government work had also largely moved online to video-conferencing and other day-to-day communication via e-mail. Estonia was well ahead of other countries in giving its citizens the opportunity to vote online in national parliamentary elections. Estonians used the internet intensively on a daily basis, putting Estonia among the leaders in Europe. On the one hand, this demonstrated Estonia's rapid and high level of development in the IT field, but on the other hand it made the country very vulnerable to cyberattacks. (Terlikowski, 2007, p. 71)

2007 also marks an important point in the cyber capabilities development for Estonia. Namely, Estonia was one of the first states to experience the negative impact of and in cyberspace, as it was targeted by extensive cyberattacks orchestrated supposedly by Russia

in April of 2007. Due to this fact, Estonia was put in a position where it had to take necessary measures to protect its integrity, sovereignty and rights and freedoms of its people by developing and improving its cyber defense recognizing the importance of cybersecurity. This collision with Russia has led Estonia to develop one of the strongest and earliest cybersecurity strategies in the world. (Council of Europe, n.d.)

To understand Estonia's position in 2007, it is necessary to recall its long history with Russia. It goes back hundreds of years, before the existence of modern nation states. (Herzog, 2011, p. 50) Estonia gained independence from the Russian Empire in 1918, but lost it again to the Soviet Union in 1940, and regained independence in 1991. (Kohler, 2020, p. 4) In addition to natural migration, hundreds of thousands of ethnic Russians were settled in Estonia by the Kremlin after the Soviet annexation of the Baltic states in 1940 and throughout the Cold War. The idea behind the relocation of Russians was to Russify Estonian culture and integrate the nations in order to increase a sense of belonging. After the fall of the Soviet Union, Estonia set itself the goal of reducing the influence of Russians on Estonian culture. (Herzog, 2011, p. 50)

Estonia's and Russia's relations can be described as turbulent. The two countries share a border, Estonia's eastern border is connected to Russia. (Herzog, 2011, p. 50) Russian nationalism is concentrated mainly in the area bordering Russia, namely the North-Eastern Virumaa region and its largest city, Narva, where the majority of the population is ethnic Russians who speak only Russian. Having such a powerful neighbor as Russia, Estonia has been largely defined by it. The only ways to prove its sovereignty to Russia and reduce its influence have been through collective security arrangements. This is why Estonia joined both the North Atlantic Treaty Organization and the European Union in 2004. (Kohler, 2020, p. 4)

At the same time, Estonia was already positioning itself as a pioneer in cybersecurity development even before the 2007 attacks, which further shaped Estonian policy in this area. Estonia has long prioritized cyber resilience, e-governance and strong international alliances. The Ministry of Economic Affairs and Communications oversees national cybersecurity through the Cyber Security Council and the Information Systems Authority. Estonia's intelligence services are very capable, but suffer from a limited budget and staff. Estonia is actively involved in global cyber diplomacy through the UN, the EU and NATO, with close links to the US and its allies. While Estonia has some cyber intelligence and offensive cyber

capabilities, it relies heavily on more capable partners to conduct such operations. (International Institute for Strategic Studies, 2023, p. 6)

In the years leading up to the 2007 attacks, cyberattacks against public and private information systems had become more frequent, making cyberspace a major security threat. The 2007 attacks against Estonia marked a new era in international security, as for the first time a coordinated cyberattack took place at the state level. The attacks, which targeted critical information systems, rapidly elevated the importance of cybersecurity to a level comparable to traditional national defense. (Estonian Ministry of Defence, 2008, p. 7) As the first large-scale cyberattack against such a highly developed country, this example provides an important case study in understanding how international law responds to such operations, along with the later and more extensive example of Ukraine.

2.2 The Triggering Event: The Bronze Soldier Controversy

The cyberattacks against Estonia began on April 27, 2007, as a result of a political activity during which Estonian authorities removed the Bronze Soldier, a Soviet World War II war memorial in the form of a statue of a Red Army soldier, from the center of the capital city, Tallinn, to a military cemetary the day before the first attacks hit Estonian cyberroom. To Estonians, the statue was and still is an oppressive reminder of the Soviet Union's occupation from 1940-1991, and to local Russians, it is a symbol of strength and praise. (Greene, 2010) At that moment, about 20% of Estonia's population were Russians (Terlikowski, 2007, p. 71), which means that the response from ethnic Russians was loud and aggressive as they rioted and looted in the capital of Estonia. (Greene, 2010)

In the last few years before the statue was moved, it had become a focal point for tensions between pro-Kremlin and Estonian nationalist movements. In order to alleviate the situation and to accommodate the views of pro-Estonian citizens, the Estonian government decided to move the monument to the Tallinn Military Cemetery. Work to move the monument began on 26th of April, 2007. On the same day, mainly peaceful demonstrators gathered at the previous location of the monument, but by the evening the crowd had grew more aggressive. This led to violent clashes with the police which lasted for a few hours. Later, the rioters turned away and proceeded to loot and vandalise nearby shops and other establishments. (Ottis, 2008, p. 1) This triggered a series of widespread and violent riots in Tallinn that lasted for four days, an event known as the Bronze Night. This name is derived from the bronze monument whose removal sparked the conflict. (Rajavee, 2017)

The controversy quickly spread beyond Estonia's borders, sparking anger among Russian citizens as well. During protests in Moscow, the demonstrators harassed the local Estonian ambassador which led to the ambassadors's bodyguards to use a mace-like spray to protect her. The protest in Russia lasted for almost a week, during which rampant demonstrators surrounded the Estonian embassy and consulate. The protest posed such a threat that Estonia evacuated some of its diplomats and their families from Russia. The Russian government condemned Estonia's decision to remove the statue, claiming it was an insult to the memory of Soviet soldiers and the Russian-speaking community in Estonia. (Finn, 2007) The authorities in Russia expressed deep indignation at Estonia's actions and publicly blamed the Estonian government of violating human rights, promoting fascism and lying about history. (Terlikowski, 2007, p. 71) The Russian authorities even strongly advised Andrus Ansip, who was the Prime Minister of Estonia at the time, to arrange for the monument to be moved to its former location and to resign from office and apologise publicly to the Russians. The Russian media presented the moving of the monument as a major and serious political problem, which in turn fuelled hostility and increased conflict. (Terlikowski, 2007, p. 71)

While in Estonia, the police was trying its best to keep the situation under control and calm down the looters, the government had to deal with unexpected cyberattacks that started on 27th of April and targeted Estonia's online information systems. (Ottis, 2008, p. 2) These cyberattacks will be described in a following subchapter.

2.3 Nature, Execution, and Targets of the Cyberattacks

The attacks on Estonia were the first politically motivated, large-scale cyberattacks on an entire nation and it is often called Cyber War I. (Ruus, 2008, p. 1) The situation globally marked a turning point in cybersecurity and international law, raising questions about how to balance digital sovereignty with evolving hybrid threats, and blurred the lines between peacetime disruptions and armed conflict.

Prior to the first attacks, posts were circulated in Russian-language outlets to incite people to attack various Estonian institutions and organizations. Institutions that were called to be attacked online in Russian public forums included the Ministry of Foreign Affairs, the Ministry of Culture, the Ministry of Defense, the Ministry of the Environment, the Patent Office, Tallinn University, University of Tartu, Estonian Parliament, Estonian Radio, and various companies. (Berendson, 2007)

The series of cyberattacks were aimed to destabilize Estonia's highly advanced IT networks. (Terlikowski, 2007, p. 71) Estonia became a target mainly for DDoS attacks (defined earlier under chapter 1.3) of varying levels of sophistication (Kohler, 2020, p. 5) and the attacks lasted 22 days in total. Although the types of attacks were well known and not overly complex, they were nevertheless disproportionately large and widespread for a small country like Estonia. Even then Estonia was already highly networked, so attacks against the availability of public digital services had a serious impact on the day-to-day operations of ordinary citizens, officials and businesses. The attacks therefore posed a threat to national security. (Ottis, 2008, p. 2) Others have found that the attacks had only a relatively mild direct impact on Estonian society. (Schmidt, 2013, p. 22) Journalist Kertu Ruus noted that the rhythm of life of Estonians did not change much despite the attacks. (Ruus, 2008, p. 3) The impact of the attacks was rather short-lived, which is why it is described more as a cyber riot than a military attack. The most serious aspect of the attacks is the Estonian government's inability to communicate truthful information to its citizens. (Willett, 2022, p. 8; Waterman, 2007) The series of attacks was volatile and unstable in terms of intensity. It consisted of both moments of intense activity, when DDoS attacks were mainly carried out in massive waves, and periods of relative calmness, when the attacks were rather simple and schematic. (Terlikowski, 2007, p. 74) Nonetheless, the cyberattacks proved to the world that they can be used as a tool in international conflicts, undermining the political, economic and social security of the other side. The attacks also highlighted Russia's foreign policy strategy of influencing neighbouring countries. (Schmidt, 2013, p. 22)

The special software used for the attacks was called "botnets" i.e., networks of computers that served illegal purposes by turning infected computers into zombie-like machines, meaning the computers had no control over themselves, in various countries, such as Vietnam and Brazil. Since the use of such techniques and the infection of computers required knowledge, funding, and planning and coordination by larger or smaller groups, the Estonian government concluded that the events were being carried out by Russian authorities. (Terlikowski, 2007, pp. 74-75)

The media also became a key target. One of Estonia's main news publications, Postimees Online, came under attack, as it was hit by a massive barrage of comment spam from abroad, attacking then-Prime Minister Andrus Ansip with abusive comments in Russian and aggressively calling for his resignation. In addition, Postimees Online was hit by denial-of-

service (DoS) attacks detected from abroad on Estonian and Russian-language portals, which sent masses of fake requests to Postimees' network addresses, clogging up the network connection and making it difficult for regular users to access the news. (Berendson, 2007)

Due to the attacks, some organizations' online and email services were disrupted; they were only partially functional. For instance, the email servers of journalists who wanted to report on the incident were flooded with spam, and government officials continued to experience difficulties reading their emails and accessing their banks for weeks after the attacks. (BBC News Online, 2007) MThe attacks affected the availability and quality of online services Estonians used on a daily basis. Some services were forced to only allow access to their servers from Estonia, blocking access to anyone outside the country's borders to mitigate the risk of being attacked. This left Estonia isolated from the rest of the world. (Ashraf, 2023; BBC News Online, 2007)

Malicious traffic on online Estonian sites often contained clear references to political motives and included direct references to a Russian-language background. An illustrative example is a phrase such as "ANSIP_PIDOR=FASCIST", which was directed at a government website. Mr Ansip was the Prime Minister of Estonia at the time. Many different variants were used, often containing expletives and Russian expressions. (Ottis, 2008, p. 2)

The most serious disruptions, however, were aimed against Estonia's financial sector. During these 22 days, ATMs and internet banks were intermittently down, news coverage was disrupted and government officials were unable to communicate. (Willett, 2022, p. 8) The most serious attack was the one against two Estonian banks, Hansapank and SEB Eesti Ühispank, which severely disrupted e-banking between May 9 and 15. (Kohler, 2020, p. 5) One Estonian bank reported a loss of $1 million due to the temporary suspension of its e-services. (Terlikowski, 2007, p. 75) Although the economic damage caused by the attacks was relatively modest, the incident nevertheless demonstrated how cyber operations can disrupt infrastructure at a national level. The incident raises questions about the adequacy of existing international legal frameworks.

2.4 Attribution Challenges and Political Implications

While this thesis does not aim to establish any one state's ultimate responsibility for the 2007 cyberattacks, the issue of attribution cannot be completely dismissed. Russia's possible involvement must be seen as part of the broader political and operational context in which

the attacks took place. Even though the attacks have not been fully attributed to Russia and no individual or group has claimed responsibility, experts have pointed to circumstantial evidence that nevertheless points to Russian involvement in the attacks.

First, the attacks were committed starting from the day after the removal of the Bronze Soldier monument which angered Russians both in Estonia and Russia. Second, the instructions for attacks were disseminated in Russian-language forums in Russian. Third, there was a lack of cooperation coming from Russia. During and after the attacks, the Estonian government sought assistance from Russian authorities to investigate the attacks, but the response was vague and generic, which raised suspicions about the Russian government's involvement or tacit approval of the attacks. Fourth, high-ranking Russian officials made statements that could be interpreted as encouragement for cyber activities against Estonia, creating an environment conducive to the spread of cyberattacks. (Ottis, 2008, pp. 2-5) The actions of the Russian media and authorities created a hostile image campaign against Estonia, which clearly influenced the decisions of individuals and groups involved in the confict to participate in the riots in any form. (Terlikowski, 2007, p. 74)

The author of this thesis does not claim that the attacks were committed by Russia nor is this the objective of the thesis to prove the Russian interference. Taking this into consideration, it is evident that the cyberattacks were linked with the overall political tensions between Estonia and Russia and part of the conflict between the two states. (Ottis, 2008, p. 1)

Scholars have also analyzed the series of attacks systemically. For instance, Estonian computer scientist Rain Ottis conducted an analysis of the 2007 cyberattacks against Estonia considering three different hypotheses as a plausible explanation for the cyberattacks that took place against Estonian information systems between 27th of April and 18th of May 2007. These were:

1. the attacks were a Russian information operation against Estonia;
2. the attacks were a false flag operation to frame Russia as the attacker;
3. the attacks were a spontaneous grass root level response to the policy of the Estonian government. (Ottis, 2008, pp. 4-5)

He came to a conclusion that the only plausible hypothesis would be the first one as the attacks were politically motivated, aligning with the hostile rhetoric from Russian officials and media regarding the relocation of the Bronze Soldier statue. Additionally, the fact that

Russian-language forums openly discussed and facilitated the attacks, providing easy-to-follow instructions, points to a coordinated effort. The third element that suggests Russia's potential role in orchestrating the series of events is the Russian government's lack of cooperation in investigations and failure to curb the attacks implied implicit support, allowing attackers to operate without consequences. The second and third hypotheses were crossed out by Mr. Ottis as they did not find enough backing. (Ottis, 2008, pp. 4-5)

However, it has to be said that the attacks cannot be fully attributed to Russia alone. On 9th of May, the day of the most sophisticated attacks, IT networks from all over the world, not just Russia, were used. Most of the IT networks used in the attacks were used without the knowledge of their owners because their computers were deliberately infected by third parties with special software. In addition, some of the IT networks were leased so that they could be used for attacks. (Terlikowski, 2007, p. 74)

Russia, however, has denied any involvement in the attacks and therefore rejected responsibility. It has warned Estonia against making further accusations without solid evidence. Russian authorities have argued that the IP addresses that the Estonian team tracked in connection with the attacks may have also been infected with botnets that turn them into "zombie-like" computers. It is therefore not certain that these IP addresses were controlled by Russians at the time of the attacks. Even though there are several clear indications that Russia was involved in the attacks, these have not proven to be sufficient to indict the Russian government. (Ruus, 2008, p. 4)

It has been stated that the attacks were carried out by pro-Russian individuals and groups. (NATO Strategic Communications Centre of Excellence, n.d., p. 53) Even though multiple people were behind the attacks, only one arrest has been made. The arrest was made by the Estonian government in connection with cyberattacks in January 2008, when the government managed to capture one of the attackers, a Russian-born student living in Estonia, Dmitri Galushkevich. It turned out that Galushkevich had used his laptop to participate in a DoS attack against the website of an Estonian political party (the Reform Party), successfully taking it offline for ten days. Galushkevich pleaded guilty to the offense and also admitted that he had participated in the attacks to protest the removal of the Bronze Soldier. The young man was fined 17,500 kroons (former Estonian currency), which is about 1,635 US dollars. (Sieg, 2009)

The entire cyberattack campaign was of a mass anti-Estonian nature, designed to undermine Estonian businesses and state institutions, whose perpetrators had the equipment, knowledge and motivation to achieve such goals, and were motivated by a desire to intervene in the Russian-Estonian conflict. As Russia's involvement has not been confirmed by substantial evidence, it still cannot be ruled out that the initiative to launch the attacks came from the Russian authorities, or even that state officials were actively involved, but there is insufficient evidence to support this hypothesis either. (Terlikowski, 2007, p. 75) Additionally, other government officials, such as Estonia's current Minister of Defense Hanno Pevkur, has publicly stated that the 2007 cyberattacks were committed by Russia. (FB Analytics, 2023)

The incident in 2007 has not been the only time Estonia was targeted by a large-scale series of coordinated cyberattacks by Russia. Namely, Russia interfered with Estonia's cyberspace in 2022 as well. Killnet, a Russian hacker group, confessed to having carried out the cyberattacks against Estonia. The group took responsibility for blocking access to a couple hundred online webpages and systems, such as state and private Estonian institutions. The reasoning behind the attacks was similar as the one in 2007, Estonia had removed another Soviet-era monument, a Soviet Tu-34 tank from public display in a city bordering Russia, Narva, which has an ethnic Russian majority. (Deutsche Welle, 2022) While this thesis does not examine the 2022 attacks in depth, it highlights their similarity in motivation and timing which underscores the persistent geopolitical and symbolic nature of cyber conflicts between Estonia and Russia.

2.5 Estonia's Response and Reforms

Estonia's response to the cyberattacks reflected a broad understanding that the objective of the attacks was to undermine the country's digital infrastructure. The provocative attacks highlighted the need for robust defense mechanisms and the potential rising concern on cyberwarfare in the fast-developing world. (Deutsche Welle, 2022) Attacks on Estonian government agencies, banks, media and telecom companies demonstrated the vulnerability of society's information systems and the need for stronger protection. Although cybersecurity had been recognised in Estonia before these attacks, the measures taken were not always sufficient. Falling victim to attacks represented a new timeline in Estonia's cybersecurity development, during which effective protection was raised to a higher priority by ensuring the security of the state's cyberspace. This involved reducing the vulnerability of cyberspace,

preventing cyberattacks and restoring the functioning of information systems as quickly as possible in the event of attacks. (Estonian Ministry of Defence, 2008, p. 7) Although as noted in subchapter 2.3, the attacks did not paralyze Estonia's digital systems in the long term, their symbolic and political weight made it a focal turning point in Estonia's cybersecurity policy.

Despite the type, scale and dynamics of the cyberattacks in 2007, the critical information and communication systems attacked in Estonia were defensible. At the time, the systems could be characterised as patchy in terms of their technical and information security level, but due to the effective and good cooperation of information security specialists, they proved to be quite resilient to attacks. There were, however, a considerable number of systems that were disrupted to a greater or lesser extent during and as a result of attacks. (Estonian Ministry of Defence, 2008, p. 14)

In the immediate aftermath of the attacks, Estonia set new projects and initiatives, legislative and regulatory changes, and strengthened cooperation. Estonia launched the first Estonian Cyber Security Strategy published by the Ministry of Defence in 2008, which set out strategic objectives to ensure cybersecurity and areas for action to strengthen cybersecurity. These areas for action were development and implementation of security measures, cybersecurity capacity building, improvement of the regulatory environment, international cooperation, outreach and awareness raising. (Estonian Ministry of Defence, 2008, pp. 4-6) It is one of the first horizontal cyber strategies in the world. (Republic of Estonia, Ministry of Economic Affairs and Communications, 2022, p. 7) In addition, in 2007 Estonia launched a public-private partnership project "Computer Security 2009", which aimed to increase information security awareness in Estonia and improve security across society. (Estonian Ministry of Defence, 2008, p. 16) The attacks against Estonia made this country, and others, consider cybersecurity as an important part of national security. (Republic of Estonia, Ministry of Economic Affairs and Communications, 2022, p. 7)

Following the attacks, changes were also made to Estonian legislation regarding cybersecurity needs. A legal analysis carried out in 2007 showed that the offence provisions in the Estonian Penal Code (Riigi Teataja, 2002) did not cover cybersecurity needs in terms of sanctions and procedures. The Code was supplemented to include different types of cyberattacks and to increase sanctions for offences where sanctions are insufficient to prevent the offence or do not allow for an investigation. In addition, the presumption of

interference with computer data or hindrance of functioning of computer systems as well as threatening with commission of such acts was added to an offence of acts of terrorism as a necessary element for one to be held accountable for the crime. (Estonian Ministry of Defence, 2008, p. 19)

Beyond national reforms, Estonia also pursued international cooperation. Estonia was expected to make a greater contribution than usual at the international level and in some cases to take the lead in processes, precisely because of the experience gained during the attacks, which other countries lacked. Therefore, Estonia actively engaged in cybersecurity initiatives both within international organizations and through bilateral cooperation. For example, Estonia was one of the initiators of the NATO Cyber Defence Policy adopted in 2008. In addition, Estonia has been active in cybersecurity and IT initiatives of the United Nations (UN) and its specialised agencies. Following the attacks, Estonia joined the Organisation for Economic Cooperation and Development (OECD) in 2010, providing an institutional opportunity to exchange experiences within this international organization. (Estonian Ministry of Defence, 2008, p. 22) However, most important international project for Estonia was the establishment of the NATO Cooperative Cyber Defence Centre of Excellence (NATO CCDCOE) in Tallinn in 2008, through which Estonia has direct communication with NATO cyber defense structures, including the relevant research and development institutions, to optimize cooperation and strengthen cybersecurity. (Estonian Ministry of Defence, 2008, p. 17)

Today, Estonia has received much praise and a strong reputation as one of the most digitalized societies in the world, especially in terms of public digital infrastructure and e-identity. On the other hand, this makes Estonia more vulnerable to cyberattacks, given the country's high dependence on digital services. As a result of the attacks, Estonia became the first European country to adopt a comprehensive cyber policy in the form of a national cybersecurity strategy and the creation of new institutions, such as the Defense League's cyber unit. (Kohler, 2020, p. 4) In conclusion, the attacks paved a way for Estonia to become a pioneer in national and international cybersecurity governance.

2.6 International Reactions and Strategic Significance

The attacks on Estonia immediately attracted international attention and intervention. Namely, both the EU and NATO were involved from the beginning of the crisis, and they were early critics of Russia’s aggressive rhetoric. Strong and transparent support from the

EU and NATO was also a key part of Estonia's political success and resistance. (Terlikowski, 2007, p. 72)

As a response, NATO sent its top cyberterrorism experts to assist Estonia in strengthening its defenses. NATO officials expressed serious concern over the attacks, emphasizing the need to address the implications of cyberwarfare. At the time, Estonian officials were concerned that NATO did not clearly define cyberattacks as military action, i.e. the provisions of Article 5 of the North Atlantic Treaty did not apply to cyberattacks, which meant that Estonia was not treated as a state under attack that would have triggered collective defense. (Traynor, 2007) NATO Secretary General at the time, Jaap de Hoop Scheffer, commented on the situation as a security issue for NATO as a whole. (Mite, 2007) Despite the high public attention NATO paid to the issue, the Alliance did not take any procedural steps against Russia. At that point, initiating any proceedings would have been risky and potentially perceived as an attack on Russia, which would have exacerbated relations between the great power and the Alliance. (Terlikowski, 2007, p. 76)

The seriousness of the problem is reflected by the fact that from the beginning of the cyber operations, both the EU and NATO were involved by providing assistance to Estonia. Both organizations were unanimous in criticising the Kremlin's aggressive rhetoric, fuelling Russian hostility, which developed into attacks on the Estonian embassy, which the authorities failed to stop. The strong support of the two organizations also ensured Estonia's political success in this conflict. Highlighting the problem by the EU and NATO also raised awareness among the general public and cyber professionals. Notably, information and communication technology experts from all over Europe contributed their knowledge to the verification of the timing of attacks. (Terlikowski, 2007, p. 72)

Although Estonia was able to cope with the attacks quite well, the start of the series of attacks was unexpected and the IT network was not sufficient to remain immune to Russian attacks. Initially, it was mainly possible to increase the capacity of servers and block access to Estonian portals from foreign countries, but that was largely the end of the matter. As the attacks were the first of their kind, they also provoked an international reaction. To counter and recover from the attacks, close cooperation between Estonia and international organizations began. (Herzog 2011, p. 54) A tightly connected network of IT experts and international support came to help as Computer Emergency Response Teams (CERTs) aided Estonia from Finland, Germany, Slovenia and elsewhere to mitigate the attacks. (Ruus, 2008,

p. 2) Security measures adopted in coordination with the teams allowed the attacks to be temporarily controlled. (Terlikowski, 2007, p. 72) In addition, the EU's European Network and Information Security Agency (ENISA) provided additional assistance by providing technical expertise on the evolving situation. A large amount of intelligence was also shared between Western countries. (Herzog, 2011, p. 54)

The attacks also had longer-term consequences. In addition to the funding of the NATO CCDCOE in Tallinn, the first authoritative handbook on the application of international law to cyber operations Tallinn Manual (Schmitt, 2013) was produced. The attacks demonstrated to Russia which against a NATO state might not trigger the application of Article 5. (Willett, 2022, p. 9)

In summary, the 2007 cyberattacks against Estonia highlighted the vulnerabilities of Estonia's cyberspace and Russia's willingness to exploit it for political purposes. The incident deepened the understanding of the need for reforms at both the national and international levels, and provided clarity on how international law regulates cyberattacks.

3. CYBERATTACKS AGAINST UKRAINE (2022-2024)

3.1 Ukraine-Russia Conflict and Cyber Dimension

While Ukraine has been the target of ongoing cyber operations since 2014, as briefly outlined later in the chapter, this chapter focuses specifically on the period that began in February 2022, when Russia launched a full-scale invasion of Ukraine and some months prior to the beginning of war. This ongoing event marks a significant escalation in the scale and sophistication of cyberattacks, with cyberattacks being actively used alongside traditional warfare.

Relations between Russia and Ukraine have been difficult for a long time, the root cause being the imperial past. (Kappeler, 2014, p. 108) Ukraine's relations with Russia have been strained by several key historical factors. Namely, in 1954 the Crimean peninsula was transferred from Russia to Ukraine within the Soviet Union, but many Russians still considered the area it theirs, which later led to the 2014 conflict during which Russia annexed the peninsula. Another point of tension is the Russian Black Sea Fleet base in Sevastopol on the Crimean peninsula, which Ukraine leased to Russia until 2042. The base is part of Ukraine, but Russians, who see it as an important symbol of nationalism, do not accept it as officially part of Ukraine. In addition, there is a large Russian-speaking population, especially in eastern and southern Ukraine, and almost half of Ukrainians consider Russian their first language, which makes Russia believe that Ukraine is still part of a great power and part of its sphere of influence. However, this has made their relationship unequal and complicated. (Kappeler, 2014, pp. 108-109) Russia's annexation of Crimea in 2014 was prompted by Ukraine's attempts to forge closer ties with the EU. Under pressure from Putin, Ukrainian President Yanukovych postponed an EU trade agreement, which led to widespread protests (Euromaidan) in 2013. After Yanukovych fled to Russia in February 2014 amid chaos in Ukraine, where over a hundred people were shot by snipers, Putin seized the opportunity to take military control of the strategically important Crimea. (Lutsevych & Wallace, 2021)

Similarly to Estonia, Ukraine was also part of the Soviet Union which has further complicated the relations between the two states. Ukraine, with a population of 46 million, was the largest country to break free from Soviet rule and had a strategically advantageous location between Russia and the West. (Rutland, 2015, p. 123) In 2014, after two decades of

growing tensions after gaining independence, it finally exploded when Russia annexed Crimea and Ukraine became a testing ground for disillusionment and uncertainty. (Rutland, 2015, p. 122) The conflict between Russia and Ukraine that has been ongoing since 2014 must be seen in the context of the broader historical confrontation between Russia and the West. This confrontation has become particularly aggressive after the collapse of the Soviet Union. Russia continues to view the post-Cold War international order with deep suspicion. The 2014 conflict, as well as the current war, reflect Russia's perceptions: first, it increasingly perceives external threats, while being certain that it has regained the necessary strength to reassert itself regionally and globally. This threat is perceived mainly in terms of NATO expansion. For Russia, the expansion of the alliance is an existential threat, especially for the countries on its western border, including Ukraine. As a result, Ukraine has become the main focus of Russia's strategic and geopolitical ambitions. (Giles, 2015, p. 19)

Tensions escalated significantly with Russia's full-scale military invasion of Ukraine in 2022 when on the night of February 24, 2022, Russian President Vladimir Putin made a statement that he had started a war against Ukraine, calling it a special military operation. (Guchua, Zedelashvili, & Giorgadze, 2022, p. 29) The war between Ukraine and Russia is the biggest one Europe has seen since 1945. Russia massed large numbers of troops on the Ukrainian border as early as January 2022, demanding guarantees from NATO and the US that Ukraine would not join NATO. Unable to obtain Russian consent, Russia invaded Ukraine with the intention of proving that Ukraine clearly falls within Russia's sphere of influence. As Ukraine has become more closely aligned with the West in recent years, Moscow sees this as a major threat to its interests and security. (Guchua, Zedelashvili, & Giorgadze, 2022, p. 30)

Since the beginning of the full-scale invasion, Ukraine has been the victim of Russian cyberattacks in addition to physical attacks. (Tavakkoli et al. 2025, p. 1) The Russian invasion was originally planned to be carried out quickly and effectively, to achieve its goals before potential sanctions or other international support for Ukraine could affect the outcome of the invasion. However, the opposite has happened on the cyber front, where Russia's attacks have lacked strategic impact. The tactics used and the attacks carried out have proven to be largely unsuccessful and ineffective. (Black, 2023, p. 6) Russia has launched a series of disruptive and destructive attacks against Ukrainian computer networks. These have included DDoS attacks and the deployment of wiper malware. The attacks have been

detected in a wide range of sectors, from government to energy. (Canadian Centre for Cyber Security, 2022, p. 2)

The conflict between Ukraine and Russia is the first major one of its kind to involve large-scale cyber operations, including a number of cyberattacks, alongside kinetic strikes. Russia has employed a variety of tactics, but Ukraine's better-than-expected defenses appear to be one of the defining features of this invasion and a key reason why Russia's cyber efforts have had limited impact. (Lewis, 2022, p. 1) It is part of a broader strategy rooted in the Soviet era and its patterns of aggression. Russia's use of cyber and information warfare is a key element of its hybrid warfare approach, which provides a greater opportunity for wider success. (Guchua, Zedelashvili, & Giorgadze, 2022, p. 31) This apporach of hybrid warfare has been tested before by Russia, namely in Georgia in 2008 and in Crimea in 2014, but on a smaller scale. (Barichella, 2022, p. 9) Hybrid warfare combines targeted cyberattacks with kinetic military strikes on the territory of the adversary. (Barichella, 2022, p. 1) Ukraine's strong understanding of information security and cybersecurity stems from the Soviet era and also from the experience of persistent hostile cyber and information operations conducted by Russia since 1991. (Giles, 2023, p. 4) Russia has treated the countries that once made up the Soviet Union as its experimental subjects to test its cyber capabilities using non-state actors and proxies, and has so far conducted cyber operations primarily in support of hybrid operations and information operations. (Štrucl, 2022b, p. 110)

For years, Russia has been known to the general public as a state that makes extensive use of cyber tactics. In fact, for more than 15 years Russia has developed and deployed offensive cyber capabilities against its perceived adversaries to control its own information space and undermine that of its adversaries. (Willett, 2022, p. 7) In the past, these tactics were used without direct military aggression. However, this changed with the invasion of Ukraine, where Russia combined cyber operations with conventional weapons and is still fighting using physical force. This change, which has altered the understanding of international law, human rights, and cybersecurity, has highlighted new features of hybrid warfare, mainly in cyberspace. (Štrucl, 2022b, p. 104) Thus, the Russia-Ukraine conflict illustrates how cyber operations are now integrated with traditional warfare methods, thereby raising questions about the application of international law.

3.2 Background: Russia's Cyber Operations Against Ukraine Pre-2022

Before the months leading up to Russia's full-scale invasion in 2022, Moscow had been ramping up its cyberattacks against, while also massing its forces along the border with the aim of destabilizing its adversary. Examples date back to early to mid-2021, when Russia conducted hacking attempts on Ukrainian security websites and computer systems relied on by top government agencies. The frequency of cyberattacks increased even further in early 2022, just before the invasion. (Barichella, 2022, p. 7) Ukraine was then subjected to cyberattacks that foreshadowed the coming invasion. These similarly included primarily DDoS attacks, but also website defacements and cyberattacks from government and private computers aimed at deleting data. (Blinken, 2022) Preparing the battlefield before the invasion also involved gathering intelligence to optimize the success of future attacks and to identify targets, with Russian network reconnaissance increasing in late 2021, just before the start of the war. (Schulze & Kerttunen, 2023, p. 4) These are genuine examples of Russia's playbook. (Blinken, 2022)

Russia's main tactics prior to invading Ukraine concluded standard attack methods such as phishing, exploiting weak passwords, and secretly entering systems. Ukraine responded with preparations for strenghtening its cyber capabilities. They improved visibility into their networks, secured remote connections critical information infrastructure, supplemented passwords with multi-factor authentication, limited access to only those who really needed it, and made sure to scan the system for potential threats. Furthermore, as Ukraine reflected its potential to fall victim to cyber threats, they had already adopted a national cybersecurity strategy in 2016. This became especially relevant by 2021, when Russia began more extensive data collection on Ukraine's cyber domain. (Black, 2023, p. 12) In addition, high-level policymakers have paid attention to improving cybersecurity, and Ukraine has relied heavily on past experience. Namely, over the years, Ukraine has become familiar with how Russia typically operates in cyber and information space. This allowed Ukraine to make quick and smart decisions and stay one step ahead of its adversary. However, to maintain this advantage, Ukraine has needed solid defensive fundamentals. (Black, 2023, p. 3)

One of the most significant attacks pre-invasion occurred on January 14, 2022. Ukraine was hit by a massive cyberattack, that targeted the websites of several government departments, including the Ministry of Foreign Affairs and the Ministry of Education rendering them temporarily inaccessible and unusable. The attackers left a threatening message on the

Ministry of Foreign Affairs' website, telling Ukrainians that all their personal data had been made public and warned them to expect worse in the future. The message included the Ukrainian flag and map, which had been crossed out indicating the denial of Ukraine's existence. It was suspected that Russian hackers were behind the attacks but no ground breaking evidence was found. (Harding, 2022) This attack was carried out using wiper malware called WhisperGate. The malware was designed to look like ransomware, offering victims the opportunity to decrypt their data for a fee, when in reality the malware wiped the system of data. (Fendorf & Miller, 2022)

Only a month after Whispergate, and just days before the invasion, Ukraine experienced another cyber offensive. This attack occurred on February 15th, reflecting the already rising geopolitical tensions. Ukrainian government websites, including those of the Ministry of Defense, the Ukrainian Armed Forces, and several major banks, such as PrivatBank and Oschadbank, were targeted by DDoS attacks. The attacks were launched in three separate waves, peaking at 150 Gbps, which made it a highly sophisticated cyber assault as a whole. The DDoS attacks had a significant impact on the availability of essential websites and services. (Karpenko, 2022) These attacks illustrate how Russia made preparations well before the invasion began, attempting to weaken Ukraine's cyber preparedness and create fertile ground for the upcoming full-scale invasion.

3.3 The Escalation: Cyberattacks During the 2022 Full-Scale Invasion

As the invasion began, Russia was expected to launch extensive cyber operations that would severly disable Ukraine’s critical infrastructure, such as telecommunications, banking, water supply, and energy supply. In reality, cyber operations did emerge as the war started but their scale and impact was far more limited than anticipated. Cyber operations did not prove as capable as the cyber dimension of a modern war could potentially be. (Willett, 2022, p. 7)

Main target of the cyberattacks between 2022 and 2024 has been critical infrastructure. The organizations and governments that have fallen victim to the attacks have therefore had a strong economic and operational impact, as in today's world all major services depend on digital systems and ICT. (Duguin & Pavlova, 2023, p. 9) In the early weeks of the Russian invasion, Microsoft conducted a threat analysis to determine whether there was a temporal correlation between cyberattacks and physical attacks. The analysis was supported by a clear temporal overlap, demonstrating that Russian military and cyber operations were focused on the same targets, whether specific sectors or geographic areas. (Microsoft, 2022, p. 10) Such

coordination means that cyberattacks were likely used to complement or enhance the impact of targeted military attacks, which directly points to a close connection between cyber and kinetic operations. On the other hand, it has been found that there has been no correlation between the timings of cyber and conventional attacks, Russia was either incapable of doing that or simply decided not to do it. Planning them for the same time would make cyberattacks more useful and successful by commanding networks and weakening the enemy's forces over time. (Lewis, 2022, p. 3) The different conclusions about temporal correlation suggest that while there is some evidence of coordination between cyber and kinetic attacks, it has not been consistent enough to establish a clear pattern.

As the invasion had officially launched on February 24, 2022, Ukraine was hit by a cyberattack on Viasat, which disrupted broadband satellite internet access. The attack disrupted modems that share information with Viasat Inc.'s KA-SAT satellite network. The satellite network provides Internet access to tens of thousands of people in Ukraine, which was disrupted by the attacks. (CyberPeace Institute, 2022) The US government confirmed its assessment that the cyberattacks on commercial satellite communications networks were carried out by Russia with the aim of disrupting Ukraine's ability to control and govern its country during the Russian invasion. (Blinken, 2022) The attack, which affected telecommunications systems, not only threatened government and military facilities, but also affected the civilian population and civilian facilities in Ukraine and elsewhere, as the use of telecommunications is an everyday reality for everyone. Thousands of people experienced internet outages and problems with energy sector systems. In some cases, internet access was lost for more than two weeks. The attack on Viasat also had a significant effect on satellite internet service providers in Germany, France and other European countries. (CyberPeace Institute, 2022) An analysis by SentinelLabs conducted in March 2022 attributed the cyberattack to the Russian military intelligence agency (GRU). The EU and the Five Eyes countries, which include the United States, United Kingdom, Australia, New Zealand, and Canada, also blamed Russia for the attack. The indictments cited violations of international norms by Russia in cyberspace. They primarily concerned the impact on civilians of critical infrastructure. This approach marked a significant advance in the application of international law in cyberspace. (CyberPeace Institute, 2022)

The attack on Viasat was technically successful, as it disrupted access to telecommunications systems for businesses and civilians, but the operational impact was rather small. Since the

aim of the attack can be considered to be disrupting the country's operations on the first day of the invasion, it cannot be considered successful, as satellite communications were of secondary importance to the Ukrainian military and more of an reduncancy option. (Schulze & Kerttunen, 2023, p. 5)

In addition, Ukraine's energy sector fell victim to Russian attacks. In particular, Russia used a malware called Industroyer2, which is designed to attack industrial control systems. (e-Estonia, 2023) Industroyer2 is malware designed to affect the industrial control systems of the Ukrainian power grid. The effect of this malware would have been similar to the one in 2016 that knocked out the Kiev power grid for a few hours. As of April 2023, it was the only publicly known malware to attack Ukraine that could potentially have been designed to cause physical impact in Ukraine. Industroyer2 was able to be deactivated before it was launched without causing any damage. The consequences of such malware can be largely negative, but due to the presence of a timer, its probability of success is limited, as the malware can be successfully interrupted if detected. This malware demonstrates the potential of cyber operations to cause physical damage, but also their limitations. On the other hand, conventional warfare tactics such as bombings were able to disrupt more than 40 percent of the Ukrainian power grid. This directly indicates the greater success of using conventional means than cyber operations. (Schulze & Kerttunen, 2023, p. 6)

Ukraine also has fallen victim to a handful of wiper attacks. One of such was named CaddyWiper. This wiper malware was detected March 14th, 2022 and targeted Ukrainian organizations. Unlike ransomware that seeks financial gain, wiper malware is designed to permanently delete data, or wipe the system clean. This makes data recovery difficult or impossible. CaddyWiper specifically deleted user data, but intentionally avoided affecting domain controllers to maintain attackers' access to desired networks. (Osborne, 2022) Such wiper attacks reflect Russia's preference for creating short-term disruption rather than achieving long-term and more strategic benefits from the attacks.

Russia's cyber operations are not limited to just military or energy targets. Ukraine has also suffered cyberattacks on its humanitarian aid coordination efforts. On January 28, 2024, Russian-linked entities launched a cyberattack on the information systems of the Coordination Headquarters for the Treatment of Prisoners of War. It was a DDoS attack and targeted Ukraine's humanitarian aid and critical services infrastructure. The attack resulted in the hackers blocking access to certain web resources, as the Coordination Headquarters

had details of the prisoner exchange and the downing of a Russian IL-76 aircraft. Although the Coordination Headquarters became a target, it was able to continue its operations without serious disruption. (Ukrinform, 2024) Furthermore, Ukrainian think tanks, other humanitarian organizations, and IT companies have been hit by the cyberattacks. (Smith, 2022) This has had a negative effect on the distribution of medicine, food and relief supplies in Ukraine. The impact of the attacks has ranged from blocking access to basic services to data theft and disinformation, including causing harm through deepfake technology. (Przetacznik & Tarpova, 2022, p. 2)

Overall, Russia's cyberattacks during the invasion were initially are characterized by an impulsive ambition of large-scale disruption, but the failure to do so led Russia back to more limited tactics, such as cyber operations that support DDoS attacks, data theft, military and psychological propaganda. (Kolodii, 2024, p. 281) These tactics fit into Russia's hybrid strategy of combining military and non-military tools, including cyber tools, to pursue national interests to achieve its goals, while economizing its use of force. (Chivvis, 2017, p. 2)

3.4 Ukraine's Response and Reforms

Russian cyberattacks have forced Ukraine to further accelerate its cybersecurity, especially its legal frameworks. Due to the experience so far, Ukraine's ability to proactively repel and mitigate the consequences of cyberattacks is faster and more effective. (Kolodii, 2024, p. 284) For instance, in April 2023, The Cabinet of Ministers of Ukraine adopted a new resolution establishing a national procedure for responding to cyberincidents and cyberattacks as a response to the growing cyberattacks due to the ongoing war with Russia. The response mechanism was developed by the State Service for Special Communications and Information Protection and it outlines the identification, defense, prevention recovery, and evaluation stages of the attacks. It also introduces criteria for assessing the criticality of cyberattacks. (EU4Digital, 2023)

Ukraine's response to the growing cyber threat from Russia has shifted from a defensive stance to a proactive and offensive one. Ukraine has adopted a "defend forward" strategy inspired by the US doctrine, which aims to target adversary cyber infrastructure to undermine its operational capabilities and thereby prevent attacks against itself. With this goal in mind, Ukrainian cyber units have begun conducting offensive cyber operations against Russian entities. These include a scientific research center, state tax service, civil aviation agency,

and Russia's largest private bank. Targeted attacks allow Ukraine to gather intelligence, which in turn helps to uncover Russian plans to attack critical infrastructure both in Ukraine and abroad, prevent planned cyberattacks, and support military attacks against Russia. Ukraine's reforms and responses to cyberattacks reflect a growing understanding that resilience alone is not enough to protect against ongoing cyberattacks. The preventive actions developed by Ukraine have found an important place in countering hybrid warfare. (Antoniuk, 2024)

Another groundbreaking but unconvetional response from Ukraine to the cyberattacks has been the formation of the IT army. The volunteer-driven initiative was created on the first day of the full-scale invasion, initiated by Deputy Prime Minister, Minister of Digital Transformation of Ukraine. (Kvartsiana, 2023, p. 18) The army is coordinated with no proven connection to Ukraine's government but has been proven to be successful at disrupting Russia's financial infrastructure, state services, and propaganda media. (Kvartsiana, 2023, pp. 18-19) It has mobilized members from all over the world and at its peak, its Telegram channel had over 300,000 users. The channel functioned as a coordination hub for DDoS attacks and other disruptive activities to undermine Russia's cyber capabilites. (Kvartsiana, 2023, p. 18) The group's status is difficult to determine, it is neither entirely civilian nor military, which in turn creates legal ambiguity from the perspective of international humanitarian law and international human rights law. Its hybrid and grassroots nature creates difficulties in establishing the attribution of crimes committed by it. (Kvartsiana, 2023, p. 19) Ultimately, Ukraine's responses and reforms have demonstrated proactive and innovative strategies, making the country a key actor in shaping defense for cyberattacks during armed conflict.

3.5 International Reactions and Strategic Significance

International reactions to cyberattacks against Ukraine show how cyber operations are viewed as strategic events that can have implications beyond alliances. For instance, although Russia's goal was to push through its demand that Ukraine not join NATO, the war and cyberattacks against Ukraine have actually made the latter's relationship with NATO closer. The same happened with the attack on Estonia, which strengthened the relationship between Estonia and NATO, especially in the area of security. ((Guchua, Zedelashvili, & Giorgadze, 2022, p. 33) In the case of Ukraine, the cyberattacks prompted NATO to take additional steps to strengthen alliance-wide cybersecurity. Namely, at the NATO summit in

Madrid in June 2022, the alliance announced that it would begin creating a virtual rapid response capability. This set the direction for using NATO to gather and organize the cyber capabilities of Member States. Similarly, EU countries increased their capabilities to remotely support Ukraine by strengthening their already existing cyber rapid-response teams. (Black, 2023, p. 4)

A year before the war, Ukraine applied for membership in the NATO Cooperative Cyber Defence Centre of Excellence, but NATO rejected it. However, in March 2022, NATO reversed the earlier decision and accepted Ukraine as a contributing participant in the NATO Cooperative Cyber Defence Centre of Excellence, a status granted to non-NATO countries. (Smalley, 2024)

In response to the cyberattacks, Microsoft played an active role in supporting Ukraine's cyber defense. The company did this primarily by sharing real-time threat intelligence with Ukrainian authorities through secure channels established before the war. The company provided critical information about vulnerabilities in government systems using external threat analysis tools. Microsoft also works with U.S. government, NATO, and EU cyber officials to share relevant intelligence. In addition, Microsoft has recognized from the outset the efforts of Ukrainian defenders and CERT-UA to maintain cyber resilience during the conflict. (Microsoft, 2022, p. 16)

Not only has Ukraine received support from major technology companies such as the aforementioned Microsoft, as well as Amazon, Google, and SpaceX, (Kvartsiana, 2023, p. 21) but it has been also helped by western countries. For instance, the United Kingdom played its part of supporting Ukraine, by providing £6.35m to help with incident response and information sharing. (Sabbagh, 2023) In conclusion, these reactions and assistance underscore the growing importance of cyberspace and the fight against the threats it poses, increasing international cooperation.

The cyberattacks described in this chapter were part of a broader campaign against Ukraine, which constituted widespread violations of international law and human rights, as also publicly confirmed by independent non-governmental organizations. (Lewis, 2022, p. 7) The cyberattacks described in this and the previous chapter not only posed significant challenges and threats to national security, information systems and public services, but also raised serious and relevant questions about how international law responds to situations where

cyberattacks are carried out during and as part of armed conflict. The legal issues related to them are discussed in detail in the following chapter.

4. BETWEEN PEACE AND WAR: INTERNATIONAL LEGAL FRAMEWORKS GOVERNING CYBERATTACKS

The rise of cyberattacks as a tool of geopolitical conflict has introduced new challenges for international law, particularly in terms of application for peacetime and during armed conflict. This chapter uses the cyberattacks against Estonia and Ukraine as case studies to examine how existing international law frameworks respond to cyberattacks in different contexts. While both incidents are significant in the context of cyberwarfare, the legal frameworks applied to these attacks differ.

This analysis is primarily important for understanding how international legal frameworks, both those applicable during peacetime and those relevant in situations of armed conflict, respond to cyberattacks,. The chapter evaluates the adequacy and limitations of international law, in particular IHRL and IHL, in addressing the legal challenges posed by cyber operations. The chapter first focuses on the cyberattacks targeting Estonia, which occurred in a peacetime context, and then turns to the cyberattacks against Ukraine, which are currently taking place during an armed conflict. In both cases, the analysis compares the relevant legal frameworks and their effectiveness in ensuring protection against such threats. A comparative assessment of the two cases is also made to highlight the differences and similarities in legal responses and the broader implications for the evolution of international law for cyberattacks.

Regardless of membership in alliances or transnational coalitions, every state must observe and adhere to the principles of international humanitarian law. This is true both in the physical world and in cyberspace. Since IHL applies during war, cyberattacks in 2007 against Estonia cannot be analyzed in this light. This is because they did not occur during an armed conflict, therefore IHL does not provide a framework for analysis in this case. Instead, in this chapter, the author assesses the responses in the light of other legal frameworks including IHRL, restrictive and diplomatic measures under the UN Charter, and the analysis provided by the Tallinn Manual 2.0 since it's also applicable for cyber operations during peacetime. (International Committee of the Red Cross [ICRC], n.d.-a) In contrast, the cyberattacks against Ukraine, which took place and are still ongoing during an armed conflict, are assessed mainly through the lens of IHL and complementary guiding documents.

4.1 Legal Frameworks Applicable in Peacetime

Malicious cyber operations carried out in peacetime raise complex questions about the scope and interpretation of existing international law. The legal principles most frequently challenged include sovereignty, due diligence and non-intervention. (Duguin & Pavlova, 2023, p. 14) All of these require further clarification in the context of cyberspace. In addition, cyber operations also have an impact on human rights and fundamental freedoms, although they are less frequently invoked. In this chapter, the author examines what legal frameworks exist in such situations, how international law responds to such operations, and what measures targeted states can use to defend themselves, and how they are interpreted and applied when attacks fall below the threshold of armed conflict, with a focus on Estonia as a case study.

4.1.1 International Human Rights Law in Cyberspace

Human rights usually refer in a legal context to those rights found in the Universal Declaration of Human Rights (UDHR) and the International Covenant on Civil and Political Rights (ICCPR), both of which were adopted by the UN. The former includes, among others, the rights to life, liberty and privacy, the right to be free from torture, the right to freedom of expression, the right to education and the right to seek asylum, the rights to social security, health and adequate housing. (United Nations General Assembly, 1948) The latter covers, for instance, rights and freedoms such as right to life, freedom of thought, conscience, and religion, freedom of expression, right to participate in public affairs, right to privacy. (United Nations General Assembly, 1966)

The rise of the Internet has led to a common view that it has become a new platform for the expression of fundamental human rights. This is why the UN Special Rapporteur on Freedom of Opinion and Expression and the European, Latin American and African Rapporteurs on Freedom of Expression signed a joint declaration in 2011, affirming that freedom of expression also applies online. The following July, the UN Human Rights Council further affirmed that the human rights covered by the aforementioned declarations must be protected both online and offline. (Rossini & Green, 2015, p. 15)

According to the UN, “human rights are rights inherent to all human beings, regardless of race, sex, nationality, ethnicity, language, religion, or any other status. Human rights include

the right to life and liberty, freedom from slavery and torture, freedom of opinion and expression, the right to work and education, and many more. Everyone is entitled to these rights, without discrimination." (United Nations, n.d.-b)

IHRL is created for governments and for the benefit of people. Governments must follow the set of rules international human rights law lays down in order to protect and promote human rights. These rules either impose duties on states to act (e.g., to protect freedoms) or to abstain from harmful behavior (e.g., discrimination or torture). (United Nations, n.d.-b)

Although the concept of human rights predates the creation of the UN, the organization has nevertheless played a central role in shaping the modern framework of IHRL. This is mainly through the adoption of key documents such as the UDHR and the development of binding treaties and monitoring mechanisms. This means that the UN created a sort of "universal rulebook" that all countries can agree with internationally and all people can rely on to have their fundamental rights protected. The UN recognizes a wide range of rights, which are civil, political, economic, social, and cultural. (United Nations, n.d.-b)

However, as the world becomes increasingly digital and cyberwarfare capabilities are becoming more sophisticated (Brown, 2020), the rights enshrined in the UN and their protection are facing new and complex challenges. This is particularly the case in cyberspace, in the context of this Master's thesis. Cyberattacks, whether committed by state or non-state actors, can directly or indirectly violate many of these fundamental rights, just like any other attack. Consequently, it is important that IHRL adapts to the new reality, where every human right, including civil, political and even social rights, can be violated.

Human rights are considered fundamental requirements of global justice. These rights are based on human dignity and aim to create conditions in society that respect the inherent worth of every person. When a state fails to take the necessary measures to protect the human rights of its citizens or, conversely, actively violates them through its actions, agents outside that society can intervene to alleviate the situation of human rights abuses. This also reflects the previously mentioned universality of human rights, which in turn points to the moral responsibility of the international community to ensure social conditions that allow people to live a decent life both within their own country and outside it. (Beitz, 2003, p. 44)

States face legal uncertainity as there is no single, legally binding instrument that responds to cyberattacks during peacetime. States do agree that international law applies to cyber

operations across borders, yet there is still a lot of disagreement about how it applies in practice. This in turn makes it hard for states to respond consistently to cyber threats. (Schmitt, 2017b, p. 242)

A cyberattack committed during peacetime can violate multiple basic human rights, such as privacy, freedom of expression, and access to information. As a small country, Estonia is at the forefront of emphasizing the preservation and protection of human rights and other principles under the value- and rules-based international order, including in cyberspace. (Pernik, 2021, p. 14) This made the 2007 cyberattacks especially alarming, as they demonstrated how even states strongly committed to international norms and upholding human rights can become targets of cyber operations that disrupt core democratic values. These attacks, while having been non-lethal, had significant implications for the exercise of fundamental rights, particularly freedom of expression and access to information. No conclusive evidence suggests that the cyberattacks led to systematic violations of human rights. Nevertheless, the theoretical framework allows us to evaluate them as potential interferences with rights that are protected both online and offline.

Freedom of expression, which is guaranteed in Article 19 of the UDHR, is a fundamental right of individuals to hold, receive and impart information and ideas. Everyone has the right to do so, without interference or restriction by external factors, in public or private, in a manner and on a subject of their choice. In its essence, freedom of expression includes both spoken words and any other form of expression, such as artistic and symbolic expressions, the press and other sources of expression. It is an important pillar of democracy, fostering a plurality of opinions on a wide range of important issues, allowing people to express their beliefs, challenge authority and participate in public debate. It promotes the advancement of society as a whole, despite the existence of potentially opposing points of view, because it nevertheless encourages the proliferation of public information and thus the development of the individual personality. However, this right is not absolute and may be subject to limitations, for example if the expressions incite violence, hate speech or threaten national security. (Article 19, n.d.) This right is also enshrined in Article 19 of the ICCPR. Furthermore, freedom of expression includes the right to access information, which is defined in Article 19(2) as the right to “seek, receive and impart information and ideas of all kinds ...”. The UN Human Rights Committee has affirmed in General Comment No. 34 that the right to freedom of expression under Article 19 ICCPR includes the freedom to seek and

receive information, particularly from public sources. (UN Human Rights Committee, 2011, p. 4) Therefore, cyberattacks that block access to any sort of governmental website, online news agency or any other critical communications infrastructure may undermine citizens' ability to exercise this fundamental right.

As highlighted in the chapter focusing on the Estonian case, the attacks disrupted access to important online platforms, including national news outlets, government websites and social media forums. By overwhelming the servers of media organizations such as Postimees, the attacks undermined the ability of journalists to disseminate information and the ability of citizens to access current events and information on how to act during cyberattacks and protests in the capital. In this way, the attacks restricted the free flow of information and disrupted the functioning of democracy. From a human rights perspective, this can be considered a violation of the right to freedom of expression, which constitutes both the right to disseminate information and the right to receive it. Even if freedom of expression was considered to have been violated, the interference was not sufficient to constitute a violation under IHRL.

Alongside freedom of expression, the 2007 attacks against Estonia also raise concerns about another fundamental right: the right to privacy. This right is enshrined in Article 12 of the UDHR and emphasizes human dignity and individual autonomy in terms of privacy. The purpose of this right is to ensure protection against unauthorized access to the private sphere or personal affairs. The right protects the family, home, correspondence and reputation from undue interference. While the concept of "privacy" is generally accepted, its definition is still questionable, as there is no consensus on it. It is believed that privacy encompasses several areas, such as physical integrity, mental integrity and the sphere of intimate relationships. On the other hand, it is believed that privacy is only included in private space and does not extend beyond it. This means that one cannot talk about the right to privacy in a public place. (Woods, 2019, p. 422) The right to privacy is also protected under Article 17 of the ICCPR, which closely mirrors Article 12 of the UDHR and gives the protection binding legal force unlike the UDHR which is not legally binding. The right to privacy also applies in the digital space. According to General Comment No. 16 on Article 17 of the ICCPR, which follows the wording of Article 12 of the UDHR, "surveillance, whether electronic or otherwise, interceptions of telephonic, telegraphic and other forms of communication, wire-tapping and recording of conversations should be prohibited." (United

Nations Human Rights Committee, 1988, para. 8) Furthermore, it states “The gathering and holding of personal information on computers, data banks and other devices, whether by public authorities or private individuals or bodies, must be regulated by law”. (United Nations Human Rights Committee, 1988, para. 10)

Due to the effects of the aforementioned cyberattacks, the right to privacy may have been violated to a certain extent for Estonian citizens. It is important to reiterate that although the attacks were mainly DDoS attacks and did not appear to involve the theft of personal data that would affect the privacy of citizens, their impact on the right to privacy cannot be completely underestimated. Given that Estonia was already highly digitalized in 2007 and that public and private sector institutions relied largely on electronic systems to store and process personal data, this episode of attacks also raised concerns about data security. If any of the systems or organizations targeted by the attack had been compromised in a way that would have exposed, accessed or interfered with the sensitive information of its users, this could constitute a violation of the right to privacy.

Despite the potential human rights implications, assessing whether the 2007 cyberattacks on Estonia amounted to actual violations of international human rights law remains complex. Since the attacks did not cause physical harm or result in deaths, and did not permanently disable infrastructure or lead to documented theft of personal data, they were not treated as clear violations of specific human rights, and the question of state responsibility under human rights law was therefore not pursued. Furthermore, there was the issue of attribution which might have discouraged any further human rights evaluation. IHRL technically applied as the attacks did not qualify as as a use of force or armed attack but nonetheless they did not trigger a response under IHRL. (Fidler, 2014, p. 316) These two issues remain. IHRL gathers attention and is applied when the weapons used are lethal. (Fidler, 2014, p. 304) As explained before, cyberattacks are usually accompanied by non-lethal weapons that do not cause any kinetic or physiological harm, it is a computer code. This makes it challenging to establish clear violations of rights such as the right to life or health. As a result, many cyberattacks do not fall inside the scope of human rights protections as they do not trigger tangible harm to individuals' life or health. Second, challenges related to attribution and jurisdiction further limit the application of IHRL. As cyberattacks are mostly carried out by anonymous actors from across borders, it would be difficult to identify them and therefore going forward with legal remedies. (Fidler, 2014, p. 306) This highlights a

challenge when leaning on IHRL for a response to peacetime cyberattacks: cyberattacks that cause damage and seriously disrupt citizens' daily lives, but not to the extent that their human rights are violated, raise the question of how to apply existing legal frameworks and whether they are sufficient to ensure the exercise of people's fundamental rights. Namely, victim states often do not refer to IHRL when they have to respond to cyberattacks. Even though cyberattacks might affect human rights to some extent depending on the situation in question, IHRL is far more often applied in surveillance contexts than in attack contexts. (Sander, 2019, p. 373) Therefore, there is a normative gap. This highlights the need to further develop or clarify how IHRL applies in cyberspace, particularly in situations where cyberattacks disrupt digital public services that are essential for the enjoyment of human rights. States rarely use IHRL frameworks to respond or assess legality even when cyberattacks could have potentially affected human rights. This state silence reflects their doubts about the adequacy and adaptability of the international legal framework to cyberspace. (Sander, 2019, p. 369) The lack of detailed interpretative guidance and consistent state practice makes it difficult to determine whether a peacetime cyberattack constitutes a human rights violation. Therefore, while peacetime cyberattacks implicate rights protected by international human rights frameworks such as the UDHR and ICCPR, they are not sufficiently reliable and enforceable in state practice. This reflects both normative uncertainty and geopolitical hesitation that suggests further clarification is necessary in order to ensure the protection of human rights during peacetime cyber operations.

4.1.2 The UN Charter and Restrictive Measures

Among IHRL, the UN Charter also remains relevant for regulating cases of peacetime state behaviour, including in cyberspace, such as the 2007 cyberattacks against Estonia. The UN Charter was not adopted with the aim of addressing or protecting cyberspace but as time has went on and technology has become a significant part of modern world, the UN has taken steps to adapt to the growing trend. Even though the UN Charter does not mention cyberspace, it is applicable to attacks committed in cyberspace. Namely, the UN Group of Governmental Experts (GGE) have affirmed in 2013, “international law, and in particular the Charter of the United Nations, is applicable and is essential to maintaining peace and stability and promoting an open, secure, stable, accessible and peaceful ICT environment.” (United Nations General Assembly, 2013, para. 19) Therefore, the UN Charter principles are

applied to cyberspace. This reflects how the UN recognizes the possibility of cyber challenges being as big of a threat as any other traditional form of conflict.

Additionally, while the UN Charter does not specifically mention cyberattacks or any other cyber operation, its principles such as use of force and the right to self-defense need to be highlighted when discussing cyberattacks in the context of international law. As explained in subchapter 1.7, the UN Charter prohibits the use of force in international relations under Article 2(4), yet it allows the use of self-defense in cases of an "armed attack" under Article 51. However, as discussed earlier, not all cyber operations meet the threshold of an armed attack as they do not cause the level of harm attacks committed with kinetic weapons do. Therefore, since incidents such as the 2007 cyberattacks against Estonia did not cause physical harm or destruction, they did not qualify as armed attacks. As a result, applying Article 51 was not legally allowed for Estonia.

For attacks that do not involve armed force, states must turn to non-forceful measures available under international law as a response. For situations like these, the UN has proposed alternative non-forceful solutions enshrined in Article 41 of the UN Charter which states the Security Council's authority to apply sanctions. (Boon, 2014, p. 2) This article offers the option of using economic or diplomatic measures which can be imposed by the Security Council to maintain or restore peace. These measures are called sanctions and they can be imposed on any state, group or individual. (United Nations Security Council, n.d.) Article 41 covers cyberwarfare, which also includes DDoS attacks (Herman, 2021), which were used as a primary measure against Estonia's digital infrastructure. The sanctions imposed by Article 41 are binding and temporary. (Boon, 2014, pp. 3-4)

Although the Security Council has not invoked Article 41 for cyberattacks, it would be a valuable measure for targeted states to rely on. When a state falls victim to cyberattacks that do not meet the threshold of an armed attack and consequently do not cause physical or physiological harm to its citizens, using armed force to respond to the attacks would be disproportionate. Therefore, using sanctions to cut or disturb economic relations and of rail, sea, air, postal, telegraphic, radio, and other means of communication, and to apply diplomatic pressure represents a proportionate and legally permissible response, especially considering it is happening during peacetime. This measure would allow the targeted state to seek accountability and justice through the Security Council without the use of force. This

would keep the state's actions within the framework of international law applicable in peacetime.

With the case of Estonia, it would bring up a challenge due to the veto power of the permanent members of the Security Council. As explained in subchapter 2.4, the main issue with seeking justice had to do with attribution. Even though Russia's involvement has not been confirmed by substantial evidence, it is still widely believed that Russia orchestrated the first ever major cyberattacks. As Russia is one of the permanent members of the Security Council, it has veto power. When a resolution is brought up to the Security Council, each permanent member has the ability to block the adoption of this resolution unilaterally. (Better World Campaign, 2025) Since it was Russia that was pointed the finger at after the 2007 cyberattacks against Estonia, it would be too optimistic to believe that Russia would not use its veto power to trigger Article 41 against itself.

The limited use of Article 41 in response to the growing trend of cyberattacks reveals a gap between legal possibility and political reality. This reflects a need for either reform within the UN system, particularly the decision making of the Security Council, or the strengthening of other lawful response mechanisms at the regional or multilateral level so targeted states can pursue accountability through peaceful and legal measures.

4.1.3 Tallinn Manual and Customary Law Principles

Another perspective on how international law responds to peacetime cyberattacks is Tallinn Manual, specifically the latest version of it – Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations. This legally non-binding study provides a significantly comprehensive collection of interpretations on how international law principles apply to behavior in cyberspace. As mentioned in subchapter 1.2, Tallinn Manual 2.0 applies to cyber incidents between states that fall below the threshold of the use of force or armed conflict. Since the 2007 cyberattacks against Estonia did not prove to reach the threshold of an armed conflict nor was it proven force was used, Tallinn Manual 2.0 could be used for it as guidance.

One central idea of Tallinn Manual 2.0 is sovereignty, which has been discussed in subchapter 1.6. As stated in Rule 1 of the study, state sovereignty applies fully in the cyber domain. This rule is a legal foundation used to assess whether a cyber operation violates

international law, especially if the attacks interfere with a country's cyber infrastructure or territorial integrity. (Schmitt, 2017a, p. 11)

Tallinn Manual 2.0 addresses the principle of non-intervention in Rule 66 which prohibits intervention including by cyber means, in the internal or external affairs of another state. (Schmitt, 2017a, p. 312) However, not all interventions are prohibited with the rule. As the world and therefore states with eachother have become more digitally connected, it is inevitable that states intervene with other states' internal or external affairs. The rule prohibits only coercive intervention. (Schmitt, 2017a, p. 312) Coercion in this case means taking away another state's freedom of choice, or creating a situation where the targeted country is forced to act against their free choice. (Schmitt, 2017a, p. 317)

Tallinn Manual 2.0 also covers the principle of due diligence in Rule 6. The rule states "A State must exercise due diligence in not allowing its territory, or territory or cyber infrastructure under its governmental control, to be used for cyber operations that affect the rights of, and produce serious adverse consequences for, other States." (Schmitt, 2017a, p. 30) States must control the activities on the territory they enjoy their sovereignty on. (Schmitt, 2017a, p. 30) This principle recognizes that not all cyberattacks come from the state itself. Some could be originated from within the state's territory as in they might not have direct state involvement. In such cases, the state has an obligation to take necessary measures to stop it, if knowing about the cyberattacks. For the rule to apply, there must be at least three parties: first, the state that has become the victim of a cyber operation, second, the state from whose territory the cyber operation is being carried out, and third, the party carrying out the cyber operation. (Schmitt, 2017a, p. 32) The rule also applies in cases where the party carrying out the cyber operation is acting remotely from a third country. Thus, in cases where the party carrying out the cyber operation is located in country A and carries out a cyber attack against country B using cyber infrastructure located in country C, the principle of due diligence applies to country C. If the latter knows that harmful attacks are being carried out using cyber infrastructure under its sovereignty and control and fails to act against the attacks, it has breached the duty of due diligence. (Schmitt, 2017a, p. 32)

A parallel can be drawn here with the 2007 Estonian case, where, as highlighted in subchapter 2.4, attacks were traced to IP addresses located in Russia, but there was no connection to the Russian government. This suggests that at least some of the attacks were carried out using Russian cyber infrastructure, even if the party carrying out the attacks may

not have been located in Russia. In such a case, Estonia could have relied on Rule 6, which states that Russia had an obligation to stop the attacks by having control over its territory and cyber infrastructure, if it knew that the attacks were being carried out. As Russia did not fulfil this obligation, it can be said to have breached the principle of due diligence.

Tallinn Manual 2.0 also covers principles of attribution and responsibility. As explained in subchapter 1.10, under Rule 14 of the Tallinn Manual 2.0, which also reflects the principles set out in Article 2 of ARSIWA, a state bears international responsibility when two conditions are met: first, the conduct in question must constitute a breach of an international legal obligation, and second, the act must be attributable to the state under international law. In the 2007 Estonia case, these requirements were not met under the framework set out in the Tallinn Manual 2.0. As mentioned earlier, Rule 15 (Attribution of cyber operations by State organs) arises when acts are carried out by state organs, and therefore can be directly attributed to the state. Nevertheless, in the 2007 Estonia case, there was not enough evidence to link the cyberattacks to Russian government or other official state entities. Therefore, Rule 15 cannot be applied here. In reality, as mentioned in subchapter 2.4, the attacks were believed to be carried out by individuals and groups which leads to Rule 17 (Attribution of cyber operations by non-State actors) since they are non-state actors. According to this rule, a state that is responsible for cyberattacks if they are carried out by non-state actors under the instructions, direction, or control of the state in question. There were several factors that pointed to a possible Russian attribution for the attacks, such as the political motivation for the relocation of the Bronze Soldier, Russia's lack of cooperation with Estonia, and the provision of Russian-language instructions on Russian-language platforms to coordinate the attacks. However, these indications were not sufficient to overcome the threshold of attribution to Russia. Thus, even if the first prerequisite of Rule 17 were met, it would still not apply because the attacks could not be attributed to Russia.

Tallinn Manual 2.0 outlines countermeasures under Rules 20-25. Based on Rule 20, countermeasures can be used in response to another state's violation of an international legal obligation. These countermeasures can be in nature cyber or not cyber. A state that acquires the right to use countermeasures may use them only to compel the responsible state to continue compliance with its international legal obligations. (Schmitt, 2017a, p. 112) The prerequisite for using countermeasures is the attribution of the operation to a state, which follows from Rules 15 and 17. (Schmitt, 2017a, p. 113) Since the presumption of attribution

was not met in the case of Estonia, the legal basis for using countermeasures was lacking even if the cyberattacks could have potentially violated the principle of due diligence and sovereignty.

Although Tallinn Manual 2.0 provides answers to questions about how international law responds to cyberattacks committed in peacetime, it raises limitations in the Estonian case. As a result of interpreting the Manual, it could be argued that Russia violated the duty of care and Estonian sovereignty, but Estonia would not be able to rely on it due to the problem of attribution, even if there is quite concrete evidence of Russia's involvement. This highlights a major shortcoming in the application of international law to ensure accountability for cyberattacks. Attribution issues aside, the Tallinn Manual 2.0 is a good basis for interpreting international law in cyber operations, despite its non-binding nature.

4.1.4 Normative Gaps and Legal Uncertainty

The 2007 cyberattacks against Estonia are a striking example of peacetime cyber operations that create legal uncertainty. Despite widespread political suspicions about Russian involvement, neither Russia nor any other state was held legally responsible. However, a young Estonian citizen of Russian nationality mentioned earlier was detained in connection with one specific cyber operation. Despite this, no formal legal mechanism was launched to deal with the attacks under international law. This shows that the lack of a cyber-specific treaty or enforcement body allowed the attacks to go unpunished. The Estonian case highlights the broader challenge of peacetime cyberattacks. While general principles such as sovereignty apply, but their application to real incidents remain controversial and unenforceable. The Estonian case is thus a vivid illustration of how states attacked in peacetime have limited legal remedies beyond political statements or technical responses.

Furthermore, the Estonian case highlighted the limitations of existing collective security frameworks. NATO and the EU both acknowledged the seriousness of the incident and highlighted the need to raise awareness of cyber threats, but did not implement collective defense mechanisms or demand legal accountability for the attacks. NATO sent cyber experts to Estonia to respond forcefully to the attacks, but that was all. The response was limited to technical and political support. Further legal steps were also hampered by the uncertainty over whether a cyberattack constitutes a use of force or an armed attack under the UN Charter. This situation prompted the creation of the Tallinn Manual, but it also does not contain binding obligations and legal penalties.

No treaty exists which specifically regulates cyberattacks during peacetime. There is no equivalent to a Geneva Convention regulating purely cyberspace operations or a UN Treaty focusing on cyberattacks during peacetime. This means that no treaty uniformly defines what constitutes a cyberattack, explains what responses are lawful and, and sets binding rules for state conduct in cyberspace during peacetime. Currently existing legal frameworks are fragmented as in only some aspects of cyber operations are addressed but no comprehensive treaty has been adopted by all UN Member States or even by a regional bloc such as the EU.

4.2 Legal Frameworks Applicable During Armed Conflict

Besides IHRL, which applies continuously regardless of whether an armed conflict occurs or not, IHL becomes particularly relevant in times of armed conflict, as in case of Ukraine. (Duguin & Pavlova, 2023, p. 14)

4.2.1 International Humanitarian Law and Cyberattacks

During armed conflicts, cyberattacks are used to exert greater influence in support of kinetic operations. The use of cyber operations makes it possible to disrupt the functioning of the attacked state and achieve military objectives without using traditional means of warfare and without harming civilians and civilian infrastructure. On the other hand, cyberattacks can damage essential services used by civilians, which can severely disrupt their daily lives. In such situations, civilians are protected by IHL. (ICRC, 2021, pp. 483-484)

IHL applies once an armed conflict starts and kinetic weapons are being used. However, once IHL has come into play, it regulates not only traditional methods of warfare but also methods that are carried out in the cyber domain. Although cyber technology is relatively new and evolving, the use of cyber assets in armed conflicts is governed by existing legal norms, specifically IHL. (ICRC, 2011, p. 38) In addition, the International Committee of the Red Cross (ICRC) has affirmed that IHL applies regardless of the means and methods of warfare used during cyber operations. (ICRC, 2021, p. 484) Thus, the rules IHL in force during armed conflict apply to the use of DDoS attacks, which are the main form of cyberattacks in Estonia and Ukraine, as examples of which are given in this thesis, as well as other cyber operations. In times of armed conflict, international law generally provides protection against the potential human damage of cyber operations, and the aim IHL is to reduce suffering, thereby protecting civilians and civilian infrastructure in particular. (Duguin & Pavlova, 2023, p. 14)

IHL is governed by treaties, such as four Geneva Conventions of 1949 and Additional Protocols. (ICRC, 2004) In addition, its rules can be found in customary international law, which derives from the general practice of states, adhered to out of a sense of legal obligation. (British Red Cross, n.d.) IHL concludes some principle rules, first of which is distinction. This principle requires that parties to an armed conflict always distinguish between civilians and combatants. Only the latter may be targeted, while attacks against the former are prohibited. The next principle is proportionality. According to this principle, attacks that are expected to cause harm (in the form of injury or death) to civilians and civilian objects must not cause excessive harm in relation to the concrete military advantage anticipated. In addition, there is the principle of humanity, which prohibits the infliction of suffering, injury or destruction that is unnecessary for the achievement of legitimate military objectives. Finally, there is the principle of military necessity. According to this, only the extent and type of force may be used that is necessary to achieve a legitimate objective, but which is not prohibited by international humanitarian law. (British Red Cross, n.d.)

Compared to the cyberattacks against Estonia in 2007, the armed conflict between Russia and Ukraine that began in early 2022 is a clear example of how cyber operations have been used in conjunction with kinetic attacks. This, however, automatically activates IHL and has raised concerns about the legality of war. Both Russia and Ukraine are parties to the Geneva Conventions and Additional Protocol I, which means that IHL fully applies to their conduct during the conflict, including in cyberspace.

The principle of distinction comes into play in the case of Ukraine in cases where cyberattacks have been aimed at disrupting dual-use (i.e. used for both military and civilian purposes) or purely civilian infrastructure. The attack on the Viasat KA-SAT satellite network at the beginning of the full-scale invasion described in subchapter 3.3 is a prime example of this. The attack in question cut off internet access for tens of thousands of civilians across Ukraine and also in other parts of Europe. While the aim of the attack may have been to damage Ukrainian military communications, the widespread negative impact of the dual-use infrastructure on non-military users and services suggests a failure to comply with the principle of distinction in that it would only affect military objectives and not civilian objectives. Similar concerns raise regarding cyberattacks carried out against government websites, financial institutions and the Ministry of Education, which had no

apparent military objective but appeared to be primarily aimed at sowing confusion or disrupting public administration.

The principle of proportionality becomes important in the aforementioned deployment of the WhisperGate and CaddyWiper malware. Their purpose was to delete data from Ukrainian systems. The strategic goal of using the malware may have been to undermine the functionality of the government, but at the same time these operations affected civilian institutions and essential services. There was no clear military advantage and they caused excessive damage compared to the military objectives. Even if the deployment of the Industroyer2 malware against the Ukrainian power grid had been successful, it would likely have caused widespread civilian damage. This would in turn be disproportionate to any expected tactical benefit. The level of disproportionality would be especially high given the potential disruption of hospitals, heating and water supply systems in the event of a successful attack, which would likely cause even more harm to civilians. Thus, such cyberattacks can be considered disproportionate to the achievement of the desired military objective.

The principle of military necessity is called into question in the case of Russian tactics by cyber operations, some aspects of which lacked the objective of achieving military results, but rather aimed at sowing psychological disturbance and uncertainty. The consistency with the principle of military necessity is questioned, for example, by WhisperGate. This malware not only deleted data, but also contained a crossed-out Ukrainian flag, implying the non-existence of Ukraine. This could indicate the attackers' desire to deny Ukrainian sovereignty. This operation, carried out just before the invasion, had no apparent military necessity, but seems to be an act of intimidation.

The humanitarian principle is highlighted by the attacks that disrupted the functioning of systems for the distribution of medicine, food and relief, emergency response or the coordination of humanitarian assistance. Disrupting or completely impeding such essential operations seriously affects Ukraine's ability to protect its civilian population and respond to humanitarian needs. The attacks that have led to these results cause unnecessary suffering and hardship to the civilian population, which is contrary to international humanitarian law.

Despite the formal applicability of the principles of IHL to cyberattacks committed during armed conflict, the anonymity that characterizes cyberspace poses significant challenges,

primarily in the form of attribution. (ICRC, 2011, p. 37) The complexity of attribution directly hinders the enforcement of the principles outlined above. The application of IHL to a cyberattack depends on whether the perpetrator of the attack who is a party in the conflict can be identified at all. Since this is a rather complicated process and often impossible, it hinders the application of IHL and the achievement of justice for the victimized state, company or individual through this branch of law. (ICRC, 2011, p. 37) This creates a legal gap in how international law, specifically IHL, responds to cyberattacks and highlights a weakness in IHL's effectiveness when applied to modern warfare involving cyberattacks.

The cyberattacks carried out during the armed conflict between Russia and Ukraine highlight both the relevance and the limits of applying traditional IHL principles to cyber operations. In the case of IHL, similarly as with the frameworks applicable during peacetime (IHRL, the UN Charter, and the Tallinn Manual 2.0), the issue of attribution is a key concern. This affirms an urgent need for their further clarification in cyberspace.

4.2.2 Complementary Role of International Human Rights Law During Armed Conflict

The next legal framework relevant cyberattacks during armed conflict is IHRL. As explained above, IHRL applies continuously, both in war and peace, and protects fundamental rights and freedoms. However, in a situation where there is an armed conflict and IHL applies during that period, it is necessary to carefully assess how IHRL operates simultaneously next to IHL. According to the principle of *lex specialis*, in a situation where both general rules and specific rules exist, the specific rules may prevail. Thus, in the case of an armed conflict, IHL, which is specifically designed to respond to only armed conflicts, would apply, while IHRL still remains relevant. (ICRC, n.d.-b) The principle of *lex* specialis is one of the most used principles when dealing with conflicting norms of general and specific norms to a situation. (Banaszewska, 2015) There is also another approach, which empahasizes the complementary nature of the two branches. According to this approach IHL and IHRL are not contradicting, but rather reinforcing each other and potentionally harmonious. (Droege, 2007, p. 337) It is said that *lex specialis* is to be applied in situations where there is conflict between IHL and IHRL, but the complementary approach is more useful when one norm from IHRL complements the other one in IHL. (Droege, 2007, p. 340) Therefore, IHL and IHRL can be in relationship of *lex specialis* or complement each other, while both sharing some common aims, such as protecting lives and health of persons. (ICRC, 2011, p. 14)

The aim of this subchapter is not to repeat the human rights content already analysed, as was done in subchapter 4.1.1, but rather to highlight the complementary role of IHRL during armed conflict, particularly in the context of cyberattacks. Furthermore, how it continues to provide legal protection in situations where international humanitarian law may be silent or inadequate.

International Court of Justice (ICJ) affirmed in its Advisory Opinion about Legality of The Threat or Use of Nuclear Weapons in 1996 that IHRL and IHL can coexist during armed conflicts even when *lex specialis* applies. The opinion states that the right to life stemming from Article 6 of the ICCPR is non-derogable even during armed conflict even if the legal framework is applicable only during peacetime. The opinion therefore affirms that IHRL is not completely deposed during armed conflict, it continues to apply but its content is interpreted in the light of IHL. (International Court of Justice, 1996, para. 25) The importance of IHRL emerges in situations where cyber operations fall below the threshold of kinetic attacks. Since many operations in cyberspace during armed conflict do not directly cause physical harm or injury, IHRL retains its relevance as a legal tool to address the broader impact of such activities on the rights of individuals.

Although cyberspace is often considered a borderless domain, it is in fact subject to fragmented national controls, while lacking a coordinated legal order. Such a regulatory vacuum seems to justify cyberattacks that violate human rights such as privacy, freedom of expression and access to essential services. (Novas-Peña, 2024) In the absence of physical harm from attacks, the protections under IHL are not triggered. In such cases, IHRL becomes the primary framework, as IHL alone is not sufficient. IHRL takes on a primary role in addressing violations even in times of armed conflict when the attacks do not reach the threshold of an attack under IHL, establishing binding legal obligations and state responsibility in situations.

There are several illustrative examples in the context of Russian cyberattacks against Ukraine that demonstrate the continuing importance of international human rights in times of armed conflict. In the case of the WhisperGate malware, government institutions were targeted and data was deleted and corrupted. While this may not have been an “attack” in the sense of IHL, if no physical harm was caused, it could potentially have violated fundamental rights protected by IHRL, such as access to public information and the functioning of public services. As noted in subchapter 1.7, an “attack” under IHL is

traditionally defined as an act of violence that causes injury or death to persons or the physical destruction of objects. Thus, if the WhisperGate malware merely disrupted civilian infrastructure, such as power grids, communications systems, or medical databases, without causing any physical harm, an attack would fall outside this definition, but IHRL would still apply. Also in the Viasat KA-SAT satellite network case, the attack could have prevented civilians from communicating, coordinating evacuations or accessing emergency services, indirectly impacting the right to life.

The interaction between IHRL and IHL also raises important questions regarding who is bound by these branches of law. Namely, IHL binds all parties involved, including both states and non-state actors. IHRL, however, is designed to traditionally bind only states, specifically their relations with their own people. (ICRC, 2003, p. 1) This creates a legal gap in cases where IHRL could be invoked in principle, but the cyberattacks are carried out by non-state actors, such as private hacker groups. As argued by the recent practice and scholarship, IHRL can, however, be used to attribute responsibility to non-state actors but in cases only be used to attribute responsibility directly to these non-state actors in cases where they exercise government-like functions or have control over territory and/or population, in which they still might carry IHRL responsibilities. (ICRC, 2011, pp. 14-15; Office of the United Nations High Commissioner for Human Rights, 2021) This distinction is relevant in the context of the Ukrainian cyberattacks, where there are indications of the involvement of Russian non-state actors. Non-state groups, such as the hacker group Killnet, which can be linked to Russia's interests, can themselves be bound by IHRL if they independently exercise government-like functions. In contrast, if those acts can be attributed to Russia, for instance, if they are acting on behalf of Russia, then it is Russia, not the hackers, who bear responsibility for human rights obligations under IHRL if any human rights are violated. In such situations, the complementary role of IHRL would be directed at the state, and IHL will continue to apply directly to all parties to the conflict, including non-state actors.

Furthermore, whereas IHL is applicable extraterritorially since it regulates armed conflict, including international armed conflicts, IHRL was developed to govern how states exercise their power over individuals within their own territory. (Gill et al., 2017, p. 76) Later, however, as international law has evolved, it has been accepted that states must exercise IHRL obligations extraterritorially when they exercise effective control over individuals or areas, whether lawfully or not. Therefore, a state has IHRL duties toward people outside the

state itself. This interpretation of the interplay between extraterritoriality and IHRL is now accepted by all. (Gill et al., 2017, pp. 79-80) However, not all cyberattacks result in IHRL obligations for a state. IHRL applies only when the cyberattack involves a genuine interference with human rights or a form of control, mere disruption does not suffice. (Besson, 2023, p. 278) In the context of Russia's cyberattacks against Ukraine, some attacks came from across Ukraine's borders as explained in subchapter 3.3. This means that Russian cyberattacks originating from its own territory could give rise to human rights obligations for Russia if they directly affect the human rights or show a form of control over Ukrainian individuals.

In conclusion, IHRL continues to play an important complementary role in times of armed conflict. This is particularly the case in cases where cyberattacks fall outside the scope of IHL but still potentially violate fundamental rights.

4.3 Current Gaps and Future Paths

Despite the existence of IHL and IHRL, there are still significant gaps in their frameworks and their implementation. This subchapter highlights them and proposes future paths to fill the gaps. As mentioned throughout this thesis, IHL and IHRL are both branches of law that apply, respectively, during armed conflict or both during armed conflict and peacetime. They are binding and states must abide by the rules set out in each law regime. However, there are challenges to adapt and apply these legal regimes to the challenges created by cyberspace.

For IHL, the main gap in applying the framework to cyberattacks is the understanding of what constitutes an "attack" and how to apply the existing "attack" definition to attacks taking place in cyberspace. IHL was designed long before cyberspace, as we know it to be today, existed. As an attack brings upon physical damage, death and/or injury, it is challenging to measure these consequences for a cyberattack as it takes place in the cyber domain that is physically not tangible. If it is uncertain whether a cyberattack falls under IHL's definition of an "attack", the application of the principles of IHL set out in subchapter 4.2.1 will also be an obstacle, depriving victims of disruptive but non-physical cyberattacks of the legal protection that IHL should in practice guarantee.

In relation to the physical component, there is also ambiguity about the threshold for armed conflict. Whereas in traditional armed conflict the parties use armed violence, in a cyberattack the operations often consist of disrupting or completely disabling digital

systems, but without causing physical harm or casualties. Thus, even cyberattacks and their perpetrators that cause harm, but not at a sufficiently traditional level, may escape the consequences of crossing the threshold for armed conflict.

Confusion also arises in the distinction between military and civilian, which is a core principle in IHL, as attacks on civilian infrastructure are not permitted. The problem arises mainly in the case of dual-use infrastructure, where it is difficult to distinguish whether attacks on them are permitted, as it serves both civilian and military principles. If the cyber system of a power grid, which supplies both civilians and military facilities, is attacked, it is not possible to make a clear decision as to whether the attack was permissible under IHL. This is because the civilian aspect also becomes apparent, which makes it difficult to separate lawful targets from unlawful ones. This legal framework clearly prohibits attacks on civilian infrastructure and causing excessive harm to civilians, but the blurring of boundaries between civilian and military cyber systems in the new domain, the indirect impact of malware, and the evolving nature of digital warfare have also raised significant enforcement challenges. This clearly highlights the serious need for further legal clarity and consensus on the application of IHL in cyberspace.

In relation to the application of IHRL, a shortcoming in applying it to cyberattacks is the question of attribution. As in the case of Estonia, attributing cyberattacks to Russia proved impossible, even though it is widely believed that Russia was the orchestrator of the first major series of cyberattacks. This meant that Estonia was unable to defend itself through the courts and place responsibility on Russia with real, serious means. Since IHRL places obligations on states to protect the fundamental rights and freedoms of their own citizens, these obligations also extend to their conduct towards individuals in other states. Ignoring them by launching cyberattacks that violate the rights of foreign populations, also carries legal consequences. However, if the state that committed the cyberattacks cannot be identified, i.e. attribution is impossible, the damage caused by the violation of human rights cannot be compensated. This greatly undermines the effectiveness of IHRL in cyberspace, as fundamental rights such as privacy, freedom of expression and access to information can be seriously affected, but without the possibility of holding anyone accountable, the functions of IHRL also remain purely theoretical.

In this context, attribution remains a challenge for IHL as well. In addition to the fact that IHL only applies during armed conflict, it is important to note that it only binds states and non-state actors involved in armed conflict. (ICRC, 2022, p. 2) If a cyberattack cannot be linked to any party to an armed conflict, for instance, if the attack is committed by self-proclaimed hackers (non-state actors), they would be considered civilian hackers under IHL and therefore their legal status under IHL is “civilians”. If they directly participate in cyberattacks that cause hostilities, they face losing protection against direct attacks. (ICRC, 2024) Nevertheless, attribution remains complex. The high level of anonymity in cyberspace often makes it impossible to determine who committed the attack. This also makes it more difficult to apply the attribution standards set out in ARSIWA and reflected in the Tallinn Manual 2.0, which require that cyberattacks are carried out under the direction or control of the state for attribution and state liability. In the case of self-proclaimed hackers, this standard is particularly difficult to meet, as there might not be any evidence of the state being involved. The involvement of third countries can also be an aggravating factor, which happened in peacetime during the example of Estonia described in subchapter 2.3, but clearly illustrates the redirection to third countries. Namely, malicious traffic was detected with botnets that operated through servers in third countries, such as Vietnam and Brazil. This conceals their true origin, which makes attribution difficult to detect the state actually committing the crime. As a result, responsible parties can evade liability because they cannot be identified, which in turn emphasizes the dependence of IHL on attribution and does not allow for the final resolution of violations.

The application of the *lex specialis* principle between IHL and IHRL is also a concern. As discussed in subchapter 4.2.2, one approach states that in times of armed conflict, IHL is the *lex specialis* and it applies over IHRL. That is because IHL is specifically designed to regulate armed conflict. This creates a grey area as to the extent to which IHRL has a role to play in such times. Cyberattacks may violate human rights, such as the right to privacy, freedom of expression and the right to information, and thus fall under IHRL, but if they do not amount to an "attack" and do not cause physical harm, IHL will not be triggered. Thus, the applicable framework is IHRL. However, if there is a situation of armed conflict, some argue that IHL, as the *lex specialis* prevails over IHRL. (Pertile & Vitucci, 2015) Others argue that in most cases the complementary approach must be taken, but it can be limited by

lex specialis principle where norms conflict. (Droege, 2007, p. 355) This illustrates how the interplay between two frameworks has not reached a consensus yet.

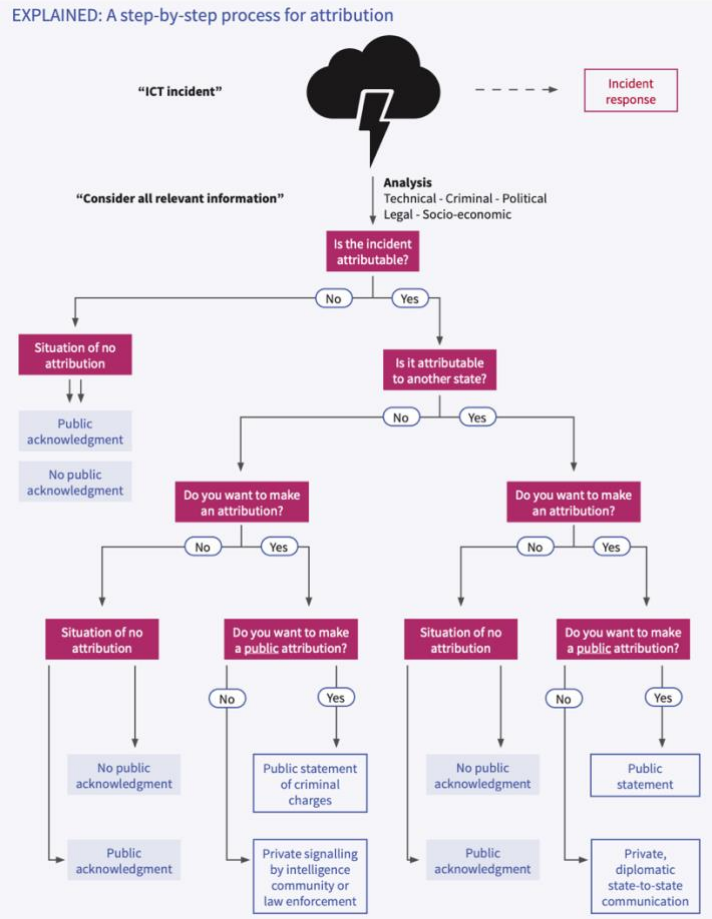
Another common gap between IHRL and IHL, but from slightly different angles, is the availability of sanctions as an enforcement mechanism. Namely, when a cyberattack occurs in peacetime and does not reach the level of an armed attack, but nevertheless violates fundamental rights such as privacy, freedom of expression or access to information, the framework of the UN Charter, specifically Article 41 and the resulting restrictive measures, i.e. sanctions, under the presidency of the Security Council, is not applied. In such cases, less effective restrictions are invoked. In contrast, under IHL, the Security Council has the theoretical right to impose sanctions under Article 41 of the UN Charter in response to cyber operations related to armed conflict. While this possibility exists, it is undermined by the Security Council's veto power. In practice, the political dynamics of the Security Council prevent action against powerful states. This is demonstrated by the war between Ukraine and Russia, during which Russia launches cyberattacks against Ukraine, but since Russia is a permanent member of the Security Council and has veto power, it protects the superpower from sanctions despite its participation in cyber operations. So in theory, the victim state may have the opportunity to achieve peace if restrictive measures are imposed against the aggressor at the international level, but in practice, a large gap appears due to political reality.

Despite the existing shortcomings in the IHL and IHRL regimes, the UN has nevertheless taken steps to regulate cyberspace and cyberattacks at the state level. Such an initiative are the UN norms of responsible state behaviour in cyberspace (Hogeveen, 2022) which contains 11 rules. These rules include interstate cooperation on security, considering all relevant information, preventing misuse of ICTs in a state's territory, cooperating to stop crime and terrorism, respecting human rights and privacy, not damaging critical infrastructure, protecting critical infrastructure, responding to requests for assistance, ensuring supply chain security, reporting ICT vulnerabilities and not harming emergency response teams. The purpose of these norms is to regulate interstate actions that have the potential to severely disrupt the security of both citizens and cyber systems. (Hogeveen, 2022, p. 14) They are concluding the work of the UN GGE and the Open-Ended Working Froup (OEWG). (Hogeveen, 2022, p. 15) These norms have been accepted by all states through consensus in the UN General Assembly resolution 70/237 in 2015. (Hogeveen, 2022, p. 8)

The main limitation these norms have is that they are non-binding, which means that states can follow them but they are not obliged to do so. This is a major disadvantage for these norms, as they lack the status of a single set of rules that all countries would follow equally and in the same way. This means that states cannot be held accountable and imposed with obligations that must be strictly followed. This initative therefore shows that states are agreeing on a need to regulate malicious activity in cyberspace as they recognize the gaps but have yet to agree on legal commitments that binds all parties.

Attribution as one of the gaps argued earlier, is covered in the UN initiative. Norm (b) of the UN norms of responsible state behaviour in cyberspace states that "In case of ICT incidents, States should consider all relevant information, including the larger context of the event, the challenges of attribution in the ICT environment and the nature and extent of the consequences". (Hogeveen, 2022, p. 13) This norm promotes transparency and cooperation between countries, mainly through information sharing. The framework recognizes that attribution is extremely difficult. (Hogeveen, 2022, p. 32) However, it requires techniques, skills, and resources that not every government may have in sufficient quantities. (Hogeveen, 2022, p. 33) Despite the fact that the norm does not concern law enforcement, it urges countries to thoroughly analyze the impacts of a cyberattack.

The UN has proposed a scheme of step-by-step process for attribution (as shown below). It advocates the state to analyze not only the technical side of a cyberattack, but also the criminal, political and legal, and to take into account all the information there is about the specific cyberattack. On the one hand, attribution under the scheme is clear and systematic, it takes into account the possibilities of informing the public about attribution and developing diplomatic communication. On the other hand, sanctions and accountability are absent among the consequences. Moreover, since the norm is non-binding, states are not even obliged to make a public statement and confirmation, which under the scheme is in many cases a response. Thus, attribution, if possible, is dependent on the political interest and willingness of states to take this step against the perpetrator of the attack. In concept, this particular UN initiative norm is trust-building and has a noble purpose, but it does not fill the attribution gap.



The UN scheme for norm (b)

Another gap argued in the UN norms is about due diligence under norm (c). This norm states "States should not knowingly allow their territory to be used for internationally wrongful acts using ICTs." (Hogeveen, 2022, p. 13) According to this norm, a state has an obligation to take the necessary measures to stop malicious activity carried out through its territory if it is aware of or has been informed in good faith of such activity. (Hogeveen, 2022, p. 36) The UN recognizes with this norm that attacks are directed through third countries, which can be linked once again with the Estonian case, where botnet activity was traced back states such as Vietnam and Brazil. If these states had known or should have known that their network was being used for attacks, they would have been required to take reasonable steps to stop the attack under UN norms. If such resources were lacking, they would have been expected to seek help from other states or from the private sector. (Hogeveen, 2022, p. 36) The strength of this norm is that it creates a situation where, in addition to the victim state, the state which's territory was used for the internationally wrongful act also contributes to identifying the source of the cyberattack. This could increase the likelihood of detection. The

norm could theoretically reduce the involvement of third countries in carrying out cyberattacks, but due to its non-binding nature, countries are not obligated to do so in this case either, and failure to do so will not entail legal consequences.

The UN initiative also covers human rights in norm (e) which states “States, in ensuring the secure use of ICTs, should respect Human Rights Council resolutions 20/8 and 26/13 on the promotion, protection and enjoyment of human rights on the Internet, as well as General Assembly resolutions 68/167 and 69/166 on the right to privacy in the digital age, to guarantee full respect for human rights, including the right to freedom of expression.” (Hogeveen, 2022, p. 13) The importance of this norm lies in the recognition that human rights can be violated in cyberspace and need to be protected in the same way as in the physical world. It links cybersecurity to the protection of fundamental rights such as privacy, freedom of expression and access to information, all of which can be violated by cyberattacks and which was done to some extent in the cases of both Estonia and Ukraine. The norm emphasizes that human rights must not be left out of cyber policy. The weakness of the norm lies once again in its non-binding nature and lack of enforcement mechanisms. It restates already existing obligations and does not create any new legal duties to protect human rights globally. Although the UN norms are global, the initiative provides examples of implementation from the Association of the Southeast Asian Nations (ASEAN) region. However, these good practices may not be equally applicable in other regions, and therefore there is no unified enforcement mechanism.

Another weakness the UN initative aims to acknowledge is the threshold gap in IHL. Norm (f) affirms “A State should not conduct or knowingly support ICT activity contrary to its obligations under international law that intentionally damages critical infrastructure or otherwise impairs the use and operation of critical infrastructure to provide services to the public”. (Hogeveen, 2022, p. 13) The norm technically requires countries to take adequate measures to protect their critical infrastructure. (Hogeveen, 2022, p. 50) IHL already prohibits attacks on civilian infrastructure, but it only applies when the situation meets the threshold of an armed attack and the operation in question is an "attack" and consequently causes physical or physiological harm to its citizens. Since some attacks do not exceed this threshold, IHL does not apply either. Norm (f) attempts to cover this grey area in situations where a cyber attack does not exceed the threshold during an armed conflict or in cases where there is no armed conflict. In both the Estonian and Ukrainian cases, cyberattacks

have occurred against critical infrastructure that is essential to the functioning of everyday civilian life. The norm reaffirms the prohibition on attacking infrastructure, and even more so now in cyberspace. The biggest weakness of this standard is its non-binding nature.

As the previous analysis demonstrates, the norms created by the UN are comprehensive in scope and could, in theory, address many of the problems arising from cyberspace and cyberattacks. The norms acknowledge the seriousness of these concerns and the need for protection, serving as a valuable foundation for further steps. They reaffirm the protection mechanisms already formulated through IHL and IHRL, but now in the cyber domain. However, the application of the norms is hindered by their non-binding nature, which also does not allow for a unified global approach to significant vulnerabilities.

Therefore, in the author's opinion, one solution to fill the currently existing gaps would be the creation of a new binding framework that would cover challenges such as attribution, civil protection and accountability, while clarifying the areas that the UN norms leave ambiguous. Such a treaty would clarify more specifically enforcement mechanisms and explanations for how different norms would apply to different cyber operations. This set of rules would be global and binding, so states would not be able to ignore the obligations arising from it, otherwise they could face meaningful consequences. However, coming to a consensus about such a treaty would probably be challenging due to the different approaches of states to cyberspace and the political interests related to the matter. If these obstacles could be overcome, a new treaty could reshape the legal environment of cyberspace. A more realistic alternative, however, would be to supplement the existing UN norms and make them binding. As the norms have already been accepted by all states, it would not require a new time-consuming journey to reach consensus. Instead, the UN could step-by-step start to focus on making the existing norms binding. Both options would create an opportunity to reduce current legal gaps and provide protection for victims of cyberattacks. However, both require political readiness and a willingness on the part of states to make cyberspace a more regulated domain. The current legal ambiguity allows for avoidance of full responsibility and attribution.

CONCLUSION

This thesis examined how international law responds to cyberattacks both in peacetime and in armed conflicts. The case studies used were the 2007 cyberattacks against Estonia and the cyberattacks accompanying Russia's invasion of Ukraine in 2022–2024. A comparative approach was used to analyze the strengths and weaknesses of existing international legal frameworks that are applied to cyberspace. Through this, it was assessed whether currently existing international law, mainly branches of law such as IHL and IHRL, provide sufficient protection for victims and accountability for attackers in a rapidly evolving landscape.

Cyberspace has become a new domain that is exploited to disrupt the orderly functioning of states. This is achieved by creating chaos in the functioning of critical infrastructure and seriously affecting the daily lives of civilians. Cyberattacks have the potential to undermine economic stability and public services, as well as interfere with fundamental human rights, such as access to information, privacy and freedom of expression, when critical systems are attacked. Although the strategic importance of cyberspace is growing over time, there is no specific universally binding framework to fully regulate it. This creates a favorable situation for states and non-state actors, where the anonymity and complexity of attribution in cyberspace make it possible to evade responsibility and sanctions. This increases the courage and audacity of actors to launch larger-caliber and more disruptive attacks. Without a binding framework, cyberspace and its specificities allow for further uncertainty and confusion.

The main and first research question set out to examine how international law responds to cyberattacks in times of peace and armed conflict, as illustrated by the cases of Estonia and Ukraine. The analysis found that in peacetime, as illustrated by the Estonian case, the legal aspects of cyberattacks are covered by the legal provisions enshrined in the UN Charter, IHRL, Tallinn Manual 2.0 and the principle of sovereignty. IHRL is a branch of law that applies continuously, i.e. it regulates human rights issues both in peacetime and during armed conflict. Both IHRL and the UN Charter are considered to have a binding nature, i.e. it is hard law. Tallinn Manual 2.0, on the other hand, is soft law, i.e. states are not obliged to follow it, it has rather a recommendatory weight, as it contains expert commentary and is of a guiding nature. IHL applies to the example of armed conflict illustrated by the Ukrainian case, as it is designed to regulate attacks and other hostilities committed during armed conflicts, protecting civilians and those not taking part in the conflict. During armed conflict, IHRL also applies, insofar as it applies at any time, regardless of whether there is a war or

not. Based on the lex specialis principle, IHL is considered to often prevail over IHRL, since according to the principle, the framework that is specifically designed to answer the legal questions that arise in the context of a specific situation always applies. However, others argue that in such a situation the complementary approach would be better applied. Under this, IHRL continues to apply alongside IHL and fills the gaps where needed. When IHL and IHRL seem to conflict, there is no consensus which framework should prevail. However, IHRL does not lose its influence during armed conflict, as the ICJ itself acknowledged in its Advisory Opinion on Legality of The Threat or Use of Nuclear Weapons in 1996. Namely, IHRL applies at all times. In situations where cyberattacks do not exceed the threshold of an armed conflict because it does not cause physical or psychological harm, IHL is not triggered and only IHRL is applied. The relationship between the two is nevertheless still debated. IHL offers structured principles such as distinction, proportionality, humanity and military necessity, which are used to assess the legality of attacks. However, the relative novelty of the proliferation of cyberattacks, the dual-purpose nature of much civilian infrastructure, and the lack of clarity as to whether specific cyberattacks qualify as "attacks" under international humanitarian law create significant ambiguity. Thus, the current international legal framework responds to cyberattacks by expanding existing norms governing kinetic attacks, but lacks a precise, unified and global understanding of the issues surrounding cyberattacks, increasing the likelihood that civilians will be left unprotected. This analysis also answers the first sub-question, which international law frameworks regulate cyberattacks in peacetime and during armed conflict.

The second research question asked how the Estonian and Ukrainian case studies were addressed under international law. The Estonian case raised the limitations that emerge in cyberattacks in peacetime. Namely, the attacks fell below the threshold of "armed attack" in the UN Charter. This denied Estonia the right to use military self-defense, as Article 51 did not apply. Although the response was mainly political and deeply condemned the attacks, presumably carried out by Russia, it nevertheless contributed to the drafting of the Tallinn Manual. Estonia received support from both the EU and NATO, and the alliances acknowledged the seriousness of the attacks. There is a widespread public perception that the attacks were carried out by Russia, but no real legal action was taken against the superpower, as the central challenge was attribution.

In the case of Ukraine, cyberattacks occurred in parallel with kinetic attacks when Russia's full-scale invasion of Ukraine began in February 2022. Thus, IHL applied, but even then there was doubt whether, for example, the Viasat hack or Industroyer 2 were cyber operations that qualified as "attacks" under IHL. Russia has also not been sanctioned for the cyberattacks that took place between 2022 and 2024, even though there is a widespread view that Russia is behind the attacks. Nevertheless, the US, UK and EU's public attribution of the Viasat attack to Russia was a significant political step. This too lacked a legal aspect, meaning no accountability measures were taken, but it nevertheless strengthened opposition to Russia's actions and the perception of Russian involvement. The situation also prompted other political responses, such as with NATO and EU providing cyber assistance to Ukraine to strenghten their cyber capabilities. The examples of both Estonia and Ukraine illustrate how cyberattacks can cause harm and disrupt both civilians and infrastructure, but there is no necessary framework to reverse the damage and hold the perpetrators accountable.

The third research question of the study addressed the shortcomings and challenges of international law responses. The main obstacle is attribution. The examples of both Estonia and Ukraine show that even if there is a widespread understanding that Russia is the perpetrator of cyberattacks, technical and legal attribution mechanisms pose serious difficulties. This in turn does not allow for holding the perpetrator accountable and restoring justice to the victims. In addition, the issue of the threshold of an attack poses difficulties. Many cyberattacks do not qualify as an "attack" under IHL, which is why IHL and the mechanisms arising from it are not triggered. Also, not every violation of sovereignty exceeds the threshold for the use of force, which is why Article 51 of the UN Charter does not trigger. The dual-purpose nature of many infrastructures, i.e. infrastructure that is used for both civilian and military purposes, also poses a challenge. This creates a gap as to whether such infrastructure is protected by the prohibition on attacking civilian infrastructure or not. Among other things, there is also a gap in enforcement, which arises from the lack of international accountability mechanisms. Even if legal norms exist, they are not automatically enforced. Without enforcement mechanisms, states can only publicly shame attackers, impose sanctions, or strengthen their cyber systems.

Moreover, although Article 41 of the UN Charter gives the Security Council the power to impose restrictive measures, or sanctions, such as complete or partial interruption of economic relations or the severance of diplomatic relations, the norm has little power if the

accused state is a permanent member of the Security Council with veto power. This is the case, for instance, with Russia. This makes the functioning of an international and binding process even more complicated. Turning to the rules of IHL, attacks against military targets are permitted, provided they comply with the principles of distinction, proportionality, humanity and military necessity. Attacks against civilians or civilian objects, on the other hand, are prohibited. The absence of enforcement mechanisms, as well as the aforementioned challenges of attribution, dual-use infrastructure and the threshold of an "attack", therefore all make the lives and rights of civilians more vulnerable.

One of the most significant steps to date in creating unified rules for cyberspace is the development of UN norms on the responsible behavior of states in cyberspace. As the analysis revealed, the 11 existing norms cover many of the current shortcomings. These include, for instance, cooperation in attribution, due diligence, respect for human rights in cyberspace, and the prohibition of attacks on critical infrastructure. These norms have been agreed by all states, which also indicates the recognition of states that there is a need to regulate cyberspace. Despite the common consensus on the creation of such a set of norms, these norms are still non-binding, which creates an important limitation. Due to their voluntary nature, states are not obliged to comply with them, nor do they impose sanctions due to the lack of an enforcement mechanism. Although the norms cover the issue of attribution, the sanctions following attribution are inadequate. According to the scheme of the attribution process, states can submit a public acknowledgement or develop diplomatic communication after public attribution, but there are no automatic sanctions and accountability measures. Attribution is less a binding legal mechanism than a political tool that states can choose not to use. Whether a state attributes a cyberattack to someone depends on the state's political willingness and interest. Since the norm does not specify penalties, it remains a diplomatic value that does not contribute to the prevention of future attacks. The norm is a strong basis for regulating malicious activities in cyberspace, but it needs clarification and binding to carry regulatory force.

The way forward could be either supplementing the existing UN norms on the responsible behavior of states in cyberspace and making them binding, or creating a new globally unified and binding treaty. The advantage of the first option would be that the norms have already been accepted by states, and thus it would be possible to avoid the time spent on creating a new treaty. However, the different political interests of states in cyberspace and its regulation

with binding norms may prove to be an obstacle. The main difficulty in creating a new treaty may be the lack of time, since cyberattacks are constantly evolving by their nature and can create more and more chaos. However, it could include explanations from the very beginning of its creation for all ambiguities, what the enforcement mechanisms are, what the threshold for the use of force in cyberspace is, and provide a more precise definition of what constitutes an attack. Regardless of whether existing rules are supplemented or a new treaty is created, international law must strike a balance between the security of states and the protection of civilians. By achieving this, there will be less room for malicious actors to exploit cyberspace.

The case studies also highlight the dimension of human rights violations from the perspective of the civilian population. In Estonia, in 2007, Estonian government institutions, banks, media and telecom companies were targeted, disrupting citizens' freedom of expression, access to information and privacy. In Ukraine, attacks were directed at critical infrastructure and humanitarian organizations in 2022-2024, which have had a negative impact on medical, food, and relief distribution systems. This in turn affected citizens' right to life, security and humanitarian assistance. In the case of Ukraine, the principle of extraterritoriality also arises in relation to human rights, which is still unresolved in the question of whether Russia has obligations under IHRL towards Ukrainians if the attacks originate from outside Russian territory. Both cases show that cyberattacks can affect the everyday life of the civilian population and their fundamental rights. This highlights the need to strengthen IHRL protection mechanisms to protect civilians both in peace and in times of armed conflict.

Analyzing Estonia and Ukraine, it is possible to conclude that cyberattacks clearly highlight the shortcomings of international law and the need for major changes and additions. Overcoming the attribution barrier, clarifying sovereignty in cyberspace, and strengthening enforcement mechanisms are important steps to transform cyberspace into a domain where law and order prevail.

REFERENCES

1. Antoniuk, D. (2024, February 8). *Ukraine's cyberattacks on Russia aiding ground operations, top Kyiv cyber official says.* The Record. https://therecord.media/ukraine-cyberattacks-aiding-ground-war-russia
2. Article 19. (n.d.). *What is freedom of expression?* Article 19. https://www.article19.org/what-is-freedom-of-expression/
3. Ashraf, C. (2023, August 22). *A preliminary engagement with the spatiality of power in cyberwar*. GeoJournal, 88(5555–5573). https://doi.org/10.1007/s10708-023-10929-z
4. Aslan, Ö., Aktuğ, S. S., Ozkan-Okay, M., Yilmaz, A. A., & Akin, E. (2023, March 11). A Comprehensive Review of Cyber Security Vulnerabilities, Threats, Attacks, and Solutions. *Electronics*, 12(6), 1333. https://doi.org/10.3390/electronics12061333
5. Banaszewska, D. M. (2015, November). *Lex Specialis.* Oxford Public International Law. https://opil.ouplaw.com/display/10.1093/law:epil/9780199231690/law-9780199231690-e2171?p=emailA4tEUQOECiZCE&d=/10.1093/law:epil/9780199231690/law-9780199231690-e2171
6. Banks, W. (2021). *Cyber Attribution and State Responsibility. International Law Studies, 97*, 1039–1068. https://digital-commons.usnwc.edu/cgi/viewcontent.cgi?article=2980&context=ils
7. Barichella, A. (2022, September). *Cyberattacks in Russia's hybrid war against Ukraine and its ramifications for Europe* (Policy Paper No. 281). Jacques Delors Institute. https://institutdelors.eu/wp-content/uploads/dlm_uploads/2022/09/PP281_The-cybersecurity-dimension-of-the-war-in-Ukraine_Barichella_EN.pdf
8. Barrier, A., & Subedi, A. (2020). Book review: *Attribution in International Law and Arbitration* by Carlo de Stefano. ITA in Review, 2(2). https://itainreview.org/articles/2020/vol2/issue2/attribution-book-review.html
9. BBC News Online. (2007, May 17). Estonia hit by 'Moscow cyber war'. *BBC News Online*. http://news.bbc.co.uk/2/mobile/europe/6665145.stm
10. Beitz, C. (2003). What Human Rights Mean. *Daedalus, 132*(1), 36-46. https://www.jstor.org/stable/20027821
11. Berendson, R. (2007, May 3). *Küberrünnakute taga seisavad profid* [Professionals behind the cyber attacks]. Postimees. https://www.postimees.ee/1656489/kuberrunnakute-taga-seisavad-profid

12. Besson, S. (2023, August 15). Extraterritoriality in international human rights law: back to the jurisdictional drawing board. In A. Parrish & C. Ryngaert (Eds.), *Research Handbook on Extraterritoriality in International Law* (pp. 269–291). Edward Elgar Publishing. https://folia.unifr.ch/unifr/documents/326075
13. Better World Campaign. (2025, February 9). *UN, explained: The history of the United Nations Security Council veto.* Better World Campaign. https://betterworldcampaign.org/peace-and-security-issues/un-explained-the-history-of-the-united-nations-security-council-veto
14. Black, D. (2023, March). *Russia's War in Ukraine: Examining the Success of Ukrainian Cyber Defences*. The International Institute for Strategic Studies. https://www.iiss.org/research-paper/2023/03/russias-war-in-ukraine-examining-the-success-of-ukrainian-cyber-defences/
15. Blinken, A. J. (2022, May 10). *Attribution of Russia's Malicious Cyber Activity Against Ukraine.* U.S. Department of State. https://2021-2025.state.gov/attribution-of-russias-malicious-cyber-activity-against-ukraine/
16. Bógdał-Brzezińska, A. (2023). Effectiveness of Russia's cyberaggression against Ukraine in 2022/2023. *Przegląd Geopolityczny, 44*, 25-40. https://przeglad.org/wp-content/uploads/2023/06/XLIV-02-BogdalBrzezinska.pdf
17. Boon, K. E. (2014). *The legal framework of Security Council sanctions* [Report]. International Peace Institute. Terminating Security Council Sanctions. http://www.jstor.com/stable/resrep09626.5
18. British Red Cross. (n.d.). *International humanitarian law*. British Red Cross. https://www.redcross.org.uk/about-us/what-we-do/protecting-people-in-armed-conflict/international-humanitarian-law
19. Brown, D. (2020, May 26). *It's Time to Treat Cybersecurity as a Human Rights Issue*. https://www.hrw.org/news/2020/05/26/its-time-treat-cybersecurity-human-rights-issue
20. Canadian Centre for Cyber Security. (2022). *CYBER THREAT BULLETIN: Cyber Threat Activity Related to the Russian Invasion of Ukraine*. Communications Security Establishment. https://www.cyber.gc.ca/sites/default/files/cyber-threat-activity-associated-russian-invasion-ukraine-e.pdf
21. Chivvis, C. S. (2017, March 2). *Understanding Russian "Hybrid Warfare" and What Can be Done About It.* The RAND Corporation.

https://www.rand.org/content/dam/rand/pubs/testimonies/CT400/CT468/RAND_CT468.pdf

22. Council of Europe. (n.d.). *Estonia*. Octopus Cybercrime Community. https://www.coe.int/en/web/octopus/-/estonia
23. CyberPeace Institute. (June, 2022). *Case Study: Viasat.* CyberPeace Institute. https://cyberconflicts.cyberpeaceinstitute.org/law-and-policy/cases/viasat
24. Deutsche Welle. (2022, August 18). *Estonia hit by cyberattacks after Soviet memorial removal*. Deutsche Welle. https://www.dw.com/en/estonia-hit-by-cyberattacks-after-soviet-memorial-removal/a-62849029
25. Droege, C. (2007, December 15). *The Interplay between International Humanitarian Law and International Human Rights Law in Situations of Armed Conflict* (Research Paper No. 14-07). The Hebrew University of Jerusalem Faculty of Law. https://www.icrc.org/sites/default/files/document_new/file_list/interplay-article-droege_0.pdf
26. Duguin, S., & Pavlova, P. (2023, September). *The role of cyber in the Russian war against Ukraine: Its impact and the consequences for the future of armed conflict.* Directorate-General for External Policies of the Union, European Parliament. https://www.europarl.europa.eu/RegData/etudes/BRIE/2023/702594/EXPO_BRI(2023)702594_EN.pdf
27. e-Estonia. (2023, March 27). *Estonia saw a record number of cyber attacks in 2022*. e-Estonia. https://e-estonia.com/in-2022-estonia-had-the-highest-number-of-cyber-attacks/
28. Ekstedt, V., Parkhouse, T., & Clemente, D. (2012). Commitments, Mechanisms & Governance. In Klimburg, A. (Ed.), *National Cyber Security Framework Manual* (pp. 146-190). NATO Cooperative Cyber Defence Centre of Excellence. https://ccdcoe.org/publications/national-cyber-security-framework-manual
29. Estonian Information System Authority. (2023). *Cyber Security in Estonia 2023*. Estonian Information System Authority. https://www.ria.ee/sites/default/files/documents/2023-02/Cyber-Security-in-Estonia-2023.pdf
30. Estonian Ministry of Defence. (2008). *Küberjulgeoleku strateegia 2008–2013* [Cybersecurity strategy 2008–2013]. Estonian Ministry of Defence. https://energiatalgud.ee/sites/default/files/images_sala/e/ea/Kaitseministeerium._Küberjulgeoleku_strateegia_2008_-_2013._Tallinn_2008.pdf

31. Estonian Ministry of Defence. (2017). *National Security Concept 2017*. Estonian Ministry of Defence. https://www.kaitseministeerium.ee/sites/default/files/elfinder/article_files/national_security_concept_2017_0.pdf
32. EU4Digital. (2023, May 18). *Strengthening cybersecurity: Ukraine's government approves response mechanism.* EU4Digital. https://eufordigital.eu/strengthening-cybersecurity-ukraines-government-approves-response-mechanism/
33. European Commission, & High Representative of the Union for Foreign Affairs and Security Policy. (2013). Cybersecurity strategy of the European Union: An open, safe and secure cyberspace (JOIN(2013) 1 final). https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=join:JOIN_2013_071
34. European Commission. (2020, December 12). JOINT COMMUNICATION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL. *The EU's Cybersecurity Strategy for the Digital Decade* (JOIN/2020/18 final). https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52020JC0018
35. European Commission. (n.d.). *EU Cybersecurity Strategy.* European Commission. https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-strategy
36. European Parliament & Council of the European Union. (2019). *Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communication technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act).* EUR-Lex. https://eur-lex.europa.eu/eli/reg/2019/881/oj/eng
37. European Parliament & Council of the European Union. (2022, December 27). *Directive (EU) 2022/2555 of the European Parliament and of the Council of 27 December 2022 on measures for a high common level of cybersecurity across the Union (NIS2 Directive).* EUR-Lex. https://eur-lex.europa.eu/eli/dir/2022/2555/2022-12-27/eng
38. European Union Agency for Network and Information Security (ENISA). (2015, December). *Definition of Cybersecurity: Gaps and overlaps in standardisation* (v1.0). https://www.enisa.europa.eu/sites/default/files/publications/Cybersecurity_Definition_Gaps_v1_0.pdf
39. Fendorf, K., & Miller, J. (2022, March 1). *Tracking Cyber Operations and Actors in the Russia-Ukraine War.* Council on Foreign Relations. https://www.cfr.org/blog/tracking-cyber-operations-and-actors-russia-ukraine-war

40. Fidler, D. P. (2014). Cyberattacks and international human rights law. In Casey-Maslen, S. (Ed.), *Weapons under International Human Rights Law* (pp. 299–333). Cambridge University Press. https://doi.org/10.1017/CBO9781139227148.014

41. Finn, P. (2007, May 3). *Protesters in Moscow Harass Estonian Envoy Over Statue*. *The Washington Post*. https://www.washingtonpost.com/archive/national/2007/05/03/protesters-in-moscow-harass-estonian-envoy-over-statue/680ebc03-58c4-4218-ae70-b745ec4350e1/

42. FP Analytics. (2023, August 31). *Lessons from Estonia's whole-of-society approach to cyber defense*. Digital Front Lines. https://digitalfrontlines.io/2023/08/31/lessons-from-estonias-whole-of-society-approach-to-cyber-defense/

43. Giles, K. (2015). Russia and Its Neighbours: Old Attitudes, New Capabilities. In K. Geers (Ed.), *Cyber War in Perspective: Russian Aggression Against Ukraine* (pp. 19-28). NATO Cooperative Cyber Defence Centre of Excellence. https://ccdcoe.org/uploads/2018/10/CyberWarinPerspective_full_book.pdf

44. Giles, K. (2023, December). *Russian Cyber and Information Warfare in Practice: Lessons Observed from the War on Ukraine*. Chatham House. https://www.chathamhouse.org/sites/default/files/2023-12/2023-12-14-russian-cyber-info-warfare-giles.pdf

45. Gill, T. D., Fleck, D., Boothby, W. H., & Vanheusden, A. (Eds.). (2017). The Applicability of International Human Rights Law in Peace Operations (pp. 76–90). In *Leuven Manual on the International Law Applicable to Peace Operations*. Cambridge University Press. https://www.cambridge.org/core/books/leuven-manual-on-the-international-law-applicable-to-peace-operations/applicability-of-international-human-rights-law-in-peace-operations/3AA48430DF735519DB29E9B242A4BB7A

46. Greene, D. (2010, August 23). *Russian minority struggles in post-Soviet Estonia*. NPR. https://www.npr.org/2010/08/23/129333023/russian-minority-struggles-in-post-soviet-estonia

47. Guchua, A., Zedelashvili, T., & Giorgadze, G. (2022, June 20). Geopolitics of the Russia-Ukraine War and Russian Cyber Attacks on Ukraine-Georgia and Expected Threats. *Ukrainian Policymaker, 10*, 27-36. https://doi.org/10.29202/up/10/4

48. Harding, L. (2022, January 14). *Ukraine hit by 'massive' cyber-attack on government websites*. The Guardian. https://www.theguardian.com/world/2022/jan/14/ukraine-massive-cyber-attack-government-websites-suspected-russian-hackers

49. Hathaway, M. E., & Klimburg, A. (2012). Preliminary Considerations: On National Cyber Security. In Klimburg, A. (Ed.), *National Cyber Security Framework Manual* (pp. 1-43). NATO Cooperative Cyber Defence Centre of Excellence. https://ccdcoe.org/publications/national-cyber-security-framework-manual
50. Herman, S. (2021, January 29). Cybersecurity and the U.N. Charter: A Square Peg in a Round Hole. *Colorado Technology Law Journal, 19*(1). https://ctlj.colorado.edu/?p=701
51. Herzog, S. (2011). Revisiting the Estonian cyber attacks: Digital threats and multinational responses. *Journal of Strategic Security, 4*(2), 49-60. https://doi.org/10.5038/1944-0472.4.2.3
52. Hoffman, F. G. (2009). Hybrid Warfare and Challenges. *Joint Forces Quarterly*, *52*, 34-39. http://www.intelros.ru/pdf/jfq_52/9.pdf
53. Hogeveen, B. (2022, March). *The UN norms of responsible state behaviour in cyberspace: Guidance on implementation for Member States of ASEAN*. Australian Strategic Policy Institute. https://documents.unoda.org/wp-content/uploads/2022/03/The-UN-norms-of-responsible-state-behaviour-in-cyberspace.pdf
54. International Committee of the Red Cross. (2003, January). International Humanitarian Law and International Human Rights Law: Similarities and differences. ICRC Advisory Service. https://www.icrc.org/sites/default/files/document/file_list/ihl-and-ihrl.pdf
55. International Committee of the Red Cross. (2004, July). *What is IHL?* International Committee of the Red Cross. https://www.icrc.org/sites/default/files/external/doc/en/assets/files/other/what_is_ihl.pdf
56. International Committee of the Red Cross. (2011, October). *International Humanitarian Law and the challenges of contemporary armed conflicts* (Report for the 31st International Conference of the Red Cross and Red Crescent, 31IC/11/5.1.2). International Committee of the Red Cross. https://www.icrc.org/sites/default/files/external/doc/en/assets/files/red-cross-crescent-movement/31st-international-conference/31-int-conference-ihl-challenges-report-11-5-1-2-en.pdf
57. International Committee of the Red Cross. (2021). International humanitarian law and cyber operations during armed conflicts (Position paper submitted to the UN OEWG and GGE). *International Review of the Red Cross, 102(*913), 481–492. https://international-

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

58. International Committee of the Red Cross. (2022, March). *What is International Humanitarian Law? Advisory Service on International Humanitarian Law.* International Committee of the Red Cross. https://www.icrc.org/sites/default/files/document/file_list/what_is_ihl.pdf
59. International Committee of the Red Cross. (2024, August 2). *Eight rules for "civilian hackers" during war, and four obligations for states to restrain them.* International Committee of the Red Cross. https://www.icrc.org/en/article/8-rules-civilian-hackers-during-war-and-4-obligations-states-restrain-them
60. International Committee of the Red Cross. (n.d.-a). *Human rights law.* International Committee of the Red Cross. https://www.icrc.org/en/law-and-policy/human-rights-law
61. International Committee of the Red Cross. (n.d.-b). *Lex specialis.* International Committee of the Red Cross. https://casebook.icrc.org/a_to_z/glossary/lex-specialis
62. International Court of Justice. (1996, July 8). *Legality of the Threat or Use of Nuclear Weapons* (Advisory Opinion, I.C.J. Reports 1996). https://iilj.org/wp-content/uploads/2016/08/Legality-of-the-Threat-or-Use-of-Nuclear-Weapons-1996.pdf
63. International Institute for Strategic Studies. (2023, September 7). *Cyber Capabilities and National Power: Volume 2.* International Institute for Strategic Studies. https://www.iiss.org/globalassets/media-library---content--migration/files/research-papers/2023/09/cyber-capabilities-and-national-power-vol-2/cyber-capabilities-and-national-power_volume-2.pdf
64. Inversini, R. (2020). Cyber Peace: And How It Can Be Achieved. In Christen, M., Gordijn, B., & Loi, M. (Eds.). (2020). *The Ethics of Cybersecurity* (Vol. 21, pp. 259-276). The International Library of Ethics, Law and Technology. Springer Nature. https://link.springer.com/book/10.1007/978-3-030-29053-5
65. Janczewski, L. J., & Colarik, A. M. (2007). Introduction to cyber warfare and cyber terrorism. In L. J. Janczewski & A. M. Colarik (Eds.), *Cyber Warfare and Cyber Terrorism* (pp. 8-30). IGI Global. https://www.andrewcolarik.com/docs/IntroductiontoCyberWarfareandCyberTerrorism.pdf

66. Kappeler, A. (2014, July 1). Ukraine and Russia: Legacies of the Imperial Past and Competing Memories. *Journal of Eurasian Studies, 5,* 107–115. https://doi.org/10.1016/j.euras.2014.05.005
67. Karpenko, O. (2022, February 16). *Що відомо про DDoS-атаку на держсайти та банки: пік до 150 Гбіт/с, ймовірно з РФ.* AIN.UA. https://ain.ua/2022/02/16/shho-vidomo-pro-ddos-ataku-15-lut/
68. Kohler, K. (2020, September). *Estonia's National Cybersecurity and Cyberdefense Posture. Policy and Organizations.* Center for Security Studies (CSS), ETH Zürich. https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/Cyber-Reports-2020-09-Estonia.pdf
69. Kohler, K. (2020, September). *Estonia's National Cybersecurity and Cyberdefense Posture. Policy and Organizations*. Center for Security Studies (CSS), ETH Zürich. https://css.ethz.ch/en/publications/risk-and-resilience-reports.html
70. Kolodii, R. (2024, April 3). The pedagogy of Cyber-WAR: Explaining Ukraine's resilience against Russian Cyber-aggression. *Defense & Security Analysis, 40*(2), 270–291. https://doi.org/10.1080/14751798.2024.2326313
71. Kvartsiana, K. (2023, December). *Ukraine's Cyber Defense: Lessons in Resilience.* German Marshall Fund of the United States. https://www.gmfus.org/sites/default/files/2023-12/Kvartsiana%20-%20Ukraine%20Cyber%20-%20Report.pdf
72. Lewis, J. A. (2022, June). *Cyber War and Ukraine* (CSIS Report). Center for Strategic and International Studies
73. Lindstrom, G., & Luiijf, E. (2012). Political Aims & Policy Methods. In Klimburg, A. (Ed.), *National Cyber Security Framework Manual* (pp. 44-66). NATO Cooperative Cyber Defence Centre of Excellence. https://ccdcoe.org/publications/national-cyber-security-framework-manual
74. Lutsevych, O., & Wallace, J. (2021, November 24). *Ukraine–Russia relations.* Chatham House. https://www.chathamhouse.org/2021/11/ukraine-russia-relations
75. Merriam-Webster. (n.d.). *Cybersecurity.* In *Merriam-Webster.com dictionary*. Merriam-Webster. https://www.merriam-webster.com/dictionary/cybersecurity
76. Microsoft. (2022, April 27). *Special report: Ukraine. An overview of Russia's cyberattack activity in Ukraine.* Digital Security Unit. https://www.microsoft.com/en-us/security/security-insider/threat-landscape/special-report-ukraine

77. Mite, V. (2007, May 30). *Estonia: Attacks seen as first case of 'cyberwar'*. Radio Free Europe/Radio Liberty. https://www.rferl.org/a/1076805.html
78. Mueller, G. B., Jensen, B., Valeriano, B., Maness, R. C., & Macias, J. M. (2023, July 13). *Cyber Operations during the Russo-Ukrainian War: From Strange Patterns to Alternative Futures.* Center for Strategic and International Studies.
79. Nazario, J. (2018). *Politically Motivated Denial of Service Attacks*. NATO Cooperative Cyber Defence Centre of Excellence. https://ccdcoe.org/uploads/2018/10/12_NAZARIO-Politically-Motivated-DDoS.pdf
80. NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE). (n.d.). *The Tallinn Manual.* NATO Cooperative Cyber Defence Centre of Excellence. https://ccdcoe.org/research/tallinn-manual/
81. NATO Strategic Communications Centre of Excellence. (n.d.). *2007 cyber attacks on Estonia.* NATO Strategic Communications Centre of Excellence. https://stratcomcoe.org/cuploads/pfiles/cyber_attacks_estonia.pdf#:~:text=In%20April%20and%20May%202007%2C%20Estonia%20became,by%20a%20Distributed%20Denial%20of%20Service%20(DDoS)
82. NIS 2 Directive. (n.d.). The NIS 2 Directive. Updates, Compliance. https://www.nis-2-directive.com
83. NIS2 Directive. (n.d.) *What is The NIS2 Directive?* NIS2 Directive. https://nis2directive.eu/what-is-nis2/
84. North Atlantic Treaty Organization (NATO). (2024, July 30). *Cyber defense*. NATO. https://www.nato.int/cps/uk/natohq/topics_78170.htm?selectedLocale=en
85. North Atlantic Treaty Organization. (2023, July 4). Collective defence and Article 5. NATO. https://www.nato.int/cps/bu/natohq/topics_110496.htm
86. Novas-Peña, A. (2024, September 19). *Lack of International Cyberspace Regulation Threatens Human Rights and International Security*. Human Rights Research Center. https://www.humanrightsresearch.org/post/lack-of-international-cyberspace-regulation-threatens-human-rights-and-international-security
87. Office of the United Nations High Commissioner for Human Rights. (2021, February 25). *Joint Statement by independent United Nations human rights experts* on human rights responsibilities of armed non-State actors*. Office of the United Nations High Commissioner for Human Rights. https://www.ohchr.org/en/press-

releases/2021/02/joint-statement-independent-united-nations-human-rights-experts-human-rights

88. Osborne, C. (2022, March 15). *CaddyWiper: More destructive wiper malware strikes Ukraine.* ZDNet. https://www.zdnet.com/article/caddywiper-more-destructive-wiper-malware-strikes-ukrainian-targets/
89. Ottis, R. (2008). *Analysis of the 2007 Cyber Attacks Against Estonia from the Information Warfare Perspective.* NATO Cooperative Cyber Defence Centre of Excellence. https://www.ccdcoe.org/uploads/2018/10/Ottis2008_AnalysisOf2007FromTheInformationWarfarePerspective.pdf
90. Pernik, P. (2021, October). *Cyber deterrence: A case study on Estonia's policies and practice* (Hybrid CoE Paper 8). European Centre of Excellence for Countering Hybrid Threats. https://www.hybridcoe.fi/wp-content/uploads/2021/10/20211012_Hybrid_CoE_Paper_8_Cyber_deterrence_WEB.pdf
91. Pertile, M. & Vitucci, C. (2015, May 12). *On the relationship between IHL and IHRL 'where it matters' once more: Assessing the position of the European Court of Human Rights after Hassan and Jaloud*. Questions of International Law. https://www.qil-qdi.org/on-the-relationship-between-ihl-and-ihrl-where-it-matters-once-more-assessing-the-position-of-the-european-court-of-human-rights-after-hassan-and-jaloud/
92. Przetacznik, J., & Tarpova, S. (2022, June). *Russia's war on Ukraine: Timeline of cyber-attacks.* European Parliamentary Research Service. https://www.europarl.europa.eu/RegData/etudes/BRIE/2022/733549/EPRS_BRI(2022)733549_EN.pdf
93. Prucková, M. (2022). *Cyber attacks and Article 5 – a note on a blurry but consistent position of NATO.* NATO Cooperative Cyber Defence Centre of Excellence. https://ccdcoe.org/library/publications/cyber-attacks-and-article-5-a-note-on-a-blurry-but-consistent-position-of-nato/
94. Rajavee, A. (2017, April 26). *AK 26.–27. aprillil 2007: Linn mässab | Pronksiöö.* Eesti Rahvusringhääling. https://www.err.ee/592086/ak-26-27-aprillil-2007-linn-massab
95. Republic of Estonia, Ministry of Economic Affairs and Communications. (2022). *Cybersecurity Strategy of Estonia 2022.* Ministry of Economic Affairs and Communications. https://www.mkm.ee/media/703/download
96. Riigi Teataja. (2002, September 1). *Penal Code* [Estonian]. *Riigi Teataja*. https://www.riigiteataja.ee/en/eli/529122024005/consolide

97. Rossini, C., & Green, N. (2015). Cybersecurity and Human Rights. GCCS 2015 - Webinar Series Training Summaries. https://www.gp-digital.org/wp-content/uploads/2015/06/GCCS2015-Webinar-Series-Introductory-Text.pdf
98. Rutland, P. (2015). An Unnecessary War: The Geopolitical Roots of the Ukraine Crisis. In A. Pikulicka-Wilczewska & R. Sakwa (Eds.), *Ukraine and Russia: People, Politics, Propaganda and Perspectives* (pp. 122-133). E-International Relations. https://rideauinstitute.ca/wp-content/uploads/2022/02/Ukraine-and-Russia-E-IR-2016.pdf
99. Ruus, K. (2008). *Cyber War I: Estonia Attacked from Russia. European Affairs, 9(*1-2). http://www.cs.yale.edu/homes/jf/RuusCyberWarEstonia.pdf
100. Sabbagh, D. (2023, January 19). *Cyber-attacks have tripled in past year, says Ukraine's cybersecurity agency.* The Guardian. https://www.theguardian.com/world/2023/jan/19/cyber-attacks-have-tripled-in-past-year-says-ukraine-cybersecurity-agency
101. Sander, B. (2019). *The Sound of Silence: International Law and the Governance of Peacetime Cyber Operations.* NATO Cooperative Cyber Defence Centre of Excellence. https://ccdcoe.org/uploads/2019/06/Art_20_The-Sound-of-Silence.pdf
102. Schmidt, A. (2013, January). The Estonian Cyberattacks. In J. Healey (Ed.), *The fierce domain: Conflicts in cyberspace 1986–2012.* Atlantic Council. https://www.researchgate.net/publication/264418820_The_Estonian_Cyberattacks
103. Schmitt, M. N. (2011). Cyber Operations and the Jus Ad Bellum Revisited. *Villanova Law Review, 56*(3), 569–606. https://digitalcommons.law.villanova.edu/cgi/viewcontent.cgi?article=1019&context=vlr
104. Schmitt, M. N. (2017a). *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations.* Cambridge University Press. https://ilmc.univie.ac.at/fileadmin/user_upload/p_ilmc/Bilder/Bewerbung/Case_2/Michael_N._Schmitt_-_Tallinn_Manual_2.0_on_the_International_Law_Applicable_to_Cyber_Operations-Cambridge_University_Press__2017_.pdf
105. Schmitt, M. N. (2017b). Peacetime Cyber Responses and Wartime Cyber Operations Under International Law: An Analytical Vade Mecum. Harvard National Security Journal,

8(2), 239–282. https://harvardnsj.org/wp-content/uploads/2017/02/Schmitt-NSJ-Vol-8.pdf

106. Schmitt, M. N. (Ed.). (2013). *Tallinn Manual on the International Law Applicable to Cyber Warfare*. Cambridge University Press. https://csef.ru/media/articles/3990/3990.pdf

107. Schulze, M., & Kerttunen, M. (2023). *Cyber operations in Russia's war against Ukraine: Uses, limitations, and lessons learned so far*. SWP Comment, 23/2023. Stiftung Wissenschaft und Politik. https://doi.org/10.18449/2023C23

108. Sieg, M. (2009, April 4). *Denial-of-Service: The Estonian Cyberwar and its Implications for U.S. National Security.* The International Affairs Review. https://www.iar-gwu.org/blog/2009/04/04/denial-of-service-the-estonian-cyberwar-and-its-implications-for-u-s-national-security

109. Smalley, S. (2022, March 4). *Ukraine, looking to fortify itself against Russian attacks, admitted to NATO cyber center.* CyberScoop. https://cyberscoop.com/ukraine-admitted-nato-ccdcoe/

110. Smith, B. (2022, June 22). *Defending Ukraine: Early lessons from the cyber war. Microsoft.* https://blogs.microsoft.com/on-the-issues/2022/06/22/defending-ukraine-early-lessons-from-the-cyber-war/

111. Štrucl, D. (2022a, June). Russian Aggression on Ukraine: Cyber Operations and the Influence of Cyberspace on Modern Warfare. *Contemporary Military Challenges, 99*(SVI.11), 103–119. https://doi.org/10.33179/BSV.99.SVI.11.CMC.24.2.6

112. Štrucl, D. (2022b, March 25). Russian aggression on Ukraine: Cyber operations and the influence of cyberspace on modern warfare. *Contemporary Military Challenges 2022(2)*, 103-123. https://doi.org/10.33179/bsv.99.svi.11.cmc.24.2.6

113. Tavakkoli, N., Çetin, O., Ekmekcioglu, E., & Savaş, E. (2025, January 16). From frontlines to online: examining target preferences in the Russia–Ukraine conflict. *International Journal of Information Security, 24,* Article 64. https://doi.org/10.1007/s10207-025-00981-w

114. Terlikowski, M. (2007). Cyberattacks on Estonia: Implications for international and Polish security. *The Polish Quarterly of International Affairs, 16*(3), 68-87. https://www.ceeol.com/search/article-detail?id=134771

115. The EU Cyber Diplomacy Toolbox. (n.d.). *The Cyber Diplomacy Toolbox*. The Cyber Diplomacy Toolbox. https://www.cyber-diplomacy-toolbox.com

116. Tran, D. (2018). *The Law of Attribution: Rules for Attributing the Source of a Cyber-Attack.* Yale Law School. https://openyls.law.yale.edu/bitstream/handle/20.500.13051/7830/DelbertTranTheLawofAttrib.pdf?sequence=2&isAllowed=y

117. Traynor, I. (2007, May 17). *Russia accused of unleashing cyberwar to disable Estonia*. *The Guardian*. https://www.theguardian.com/world/2007/may/17/topstories3.russia

118. Ukrinform. (2024, January 29). *Coordination HQ hit by cyberattack.* Ukrinform. https://www.ukrinform.net/amp/rubric-ato/3819543-coordination-hq-hit-by-cyberattack.html

119. UN Human Rights Committee. (1988, April 8). *CCPR General Comment No. 16: Article 17 (Right to Privacy), The Right to Respect of Privacy, Family, Home and Correspondence, and Protection of Honour and Reputation* [General comment]. https://www.refworld.org/legal/general/hrc/1988/en/27539

120. UN Human Rights Committee. (2011, September 12). *General comment No. 34, Article 19: Freedoms of opinion and expression* (CCPR/C/GC/34) [General comment]. https://www.refworld.org/legal/general/hrc/2011/en/83764

121. United Nations General Assembly. (1948). *Universal Declaration of Human Rights*. (Resolution 217 A (III)). https://www.un.org/en/about-us/universal-declaration-of-human-rights

122. United Nations General Assembly. (1966). *International Covenant on Civil and Political Rights* (Resolution 2200A (XXI)). https://www.ohchr.org/en/instruments-mechanisms/instruments/international-covenant-civil-and-political-rights

123. United Nations General Assembly. (2013, June 24). *Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security* (UN Doc. A/68/98). United Nations General Assembly. https://docs.un.org/en/A/68/98

124. United Nations Security Council. (n.d.). *Actions with Respect to Threats to the Peace, Breaches of the Peace, and Acts of Aggression. Article 41 – Measures not involving the use of armed force*. United Nations Security Council. https://main.un.org/securitycouncil/en/content/repertoire/actions

125. United Nations. (2001). *Responsibility of States for Internationally Wrongful Acts.* United Nations https://legal.un.org/ilc/texts/instruments/english/draft_articles/9_6_2001.pdf

126. United Nations. (n.d.-a). *United Nations Charter, Chapter I: Purposes and Principles.* United Nations. https://www.un.org/en/about-us/un-charter/chapter-1

127. United Nations. (n.d.-b). *Human rights.* United Nations. https://www.un.org/en/global-issues/human-rights

128. Waterman, S. (2007, June 11). Analysis: Who cyber smacked Estonia? *United Press International.* https://www.upi.com/Defense-News/2007/06/11/Analysis-Who-cyber-smacked-Estonia/26831181580439/

129. Willett, M. (2022). The Cyber Dimension of the Russia–Ukraine War. *Survival, 64*(5), 7-26. https://doi.org/10.1080/00396338.2022.2126193

130. Woods, L. (2019, August 20). Digital privacy and Article 12 of the Universal Declaration of Human Rights. *The Political Quarterly, 90*(3), 422-429. https://onlinelibrary.wiley.com/doi/10.1111/1467-923X.12740