Digital Battlegrounds: Evaluating the Impact of Cyber Warfare on International Humanitarian Law in the Russian-Ukraine War

Aaron Broekstra

Peace and Conflict Studies
Bachelor
12 ECTS
Spring/2024
Supervisor: Katrine Gotfredsen
Word Count: 12032

Abstract

This study investigates the legal and ethical challenges posed by cyber warfare in the ongoing Russian-Ukraine war. Cyber warfare represents a transition from traditional conflict dynamics, impacting civilian populations and national security without direct physical confrontations. The significance of this research is the inadequacy of current legal norms that govern the rapidly evolving techniques of cyber-attacks which challenge established norms of International Humanitarian Law. Hence, the research question explores how cyber warfare challenges existing legal and ethical norms for civilian protection, and what the broader implications are for the regulation of modern conflicts. Through a qualitative case study approach, the thesis analyses three cases of Russian cyber-attacks on Ukrainian civilian infrastructure: the 2015 attack on the Ukrainian power grid, the 2023 cyber-attack on Kyivstar, and the 2022 Asylum Ambuscade. In the simplified legal framework by Hoffman and Rumsey, these cases were analysed using the Tallinn Manual, and Mary Kaldor's New Wars theory to highlight the challenges and violations of IHL. The findings conclude that the IHL framework is insufficient for the unique challenges of cyber warfare. Moreover, the study addresses for the revaluation and updating of international legal norms to keep up with the constant development of cyber warfare. In all, this thesis showcases the need for enhanced legal standards that can safeguard civilian populations and maintain international security, contributing to the fields of international law and conflict resolution.

Keywords: *Cyber Warfare; International Humanitarian Law (IHL); Cyber Attacks; Russian – Ukraine War; Civilian Protection; Tallinn Manual; New Wars Theory*

Number of words: 12032

List of Abbreviations

CEO	Chief Executive Officer
CFR	Council of Foreign Relations
CISA	Cybersecurity & Infrastructure Security Agency
CISA	Cybersecurity & Infrastructure Security Agency
CSIS	Center for Strategic and International Studies
E-ISAC	Institute and The Electricity Information Sharing and Analysis Center
GRU	Russia's Main Intelligence Directorate
HRC	Human Rights Council
IBA	International Bar Association
ICRC	International Committee of the Red Cross
IHL	International Humanitarian Law
NGO	Non-Governmental Organisation
SANS	SysAdmin, Audit, Network, and Security
SBU	Security Service Agency of Ukraine
SIPRI	Stockholm International Peace Research Institute
UN	United Nations
US	United States

Table of Contents

1. Introduction

A new form of warfare is on the rise which is reshaping the landscape of international conflict. As the former Estonian President Toomas Hendrik Ilves stated during the 69th UN General Assembly, “In the modern world, cyber warfare will be the primary way that countries assert their dominance and resolve their conflicts. This digital battleground is where future wars will be won and lost” (Ilves, 2014). Cyber warfare challenges the established traditional norms of warfare and International Humanitarian Law (IHL). IHL, “can be defined as the branch of international law limiting the use of violence in armed conflicts by: sparing those who do not or no longer directly participate in hostilities.” (Carnegie Endowment for International Peace, 2024). This thesis will look into the Russian-Ukraine war, which has not only in terms of direct violence but also stands as the most extensive instance of cyber warfare in history (Sheldon, 2024), addressing the consequences of digital combat.

The thesis will investigate three cases of Russian cyber-attacks on civilians and analyse their legality and ethicality during the Russian-Ukraine war. By using IHL and the Tallinn Manual - which is a guide and reference when connecting legal norms to cyber-attacks (Schmitt, 2017) - as a fundamental framework, the thesis will analyse and evaluate the three Russian cyber-attacks. The thesis will focus on fundamental principles in IHL, which will help identify the legal and ethical norms within the cases: distinction and proportionality, dual-use infrastructure, and espionage and information warfare. In addition to IHL and the Tallinn Manual, the thesis will use Kaldor’s new wars theory (2012) to help build a better understanding of what the development of cyber warfare means for IHL. Kaldor’s theory will also be used to help justify when IHL is applicable and to examine what means and methods can be used during war (Miller, 1964: 282 & Henriksen, 2017: 261). In all, these methods and theories will allow me to better understand the legal and ethical norms of the three cases.

1.1 Research Problem, Cases, and Peace and Conflict Studies Relevance

The evolving development of cyberwarfare creates constant challenges to the frameworks of IHL and the Tallinn manual. Hence, the research problem this thesis explores is

based on the adequacy of existing IHL norms and the guidelines provided by the Tallinn manual in regulating and complex nature of cyber-attacks that affect civilians in areas of conflict. There have been public calls for a change in the legislation of UN charters and IHL, but due to numerous factors including consensus requirements and sovereignty concerns, particularly in international laws governing warfare, this is difficult to change (Thürer, 2010). Furthermore, the three cases this thesis will investigate are instances that highlight the challenges to, and adequacy, of existing IHL norms in regulating the complexity of cyber warfare impacting civilians. The first case I will examine is the 2015 cyber-attack on the Ukrainian power grid, which was "the first publicly acknowledged attack that used a digital weapon hitting a power grid and causing power outages" (CCDCOE, 2023). This attack left 225,000 people without electricity in the middle of winter (SAND & E-ISAC, 2016). The second case, the Kyivstar attack is a Russian cyber-attack on the biggest telecommunication company in Ukraine, Kyivstar, which was "one of the highest-impact disruptive cyberattacks" on the country since the start of the war" (VEON, 2024). The attack left 2 million Kyivstar subscribers in and out of Ukraine without data connectivity on mobile and fixed networks for two days" (ibid.). The last case this thesis will investigate is known as the 2022 Asylum Ambuscade cyber-attacks where Russian hackers manipulated and sent propaganda to Ukrainian refugees and humanitarian organizations, affecting thousands (Howard, 2023).

Using three cases in the Russian-Ukraine war also helps the thesis's relevance to Peace and Conflict Studies. This thesis provides a comprehensive analysis of cyber warfare within the context of modern conflicts as exemplified by the Russian-Ukraine war. It also offers a specific insight into the humanitarian impacts of warfare which enhances both the academic discourse and policymaking in the scope of contemporary conflict resolution. Lastly, cyber warfare is linked to Peace and Conflict Studies because it represents a rapidly evolving frontier in global conflicts, where digital battlegrounds can impact national security, economic stability, and civilian safety without a single physical confrontation.

1.2 Research Question and Aim

This thesis aims to critically analyse how cyber warfare in the Russian-Ukraine war challenges the existing legal and ethical framework for civilian protection. Moreover, this thesis will use a qualitative case study method on the three cases mentioned above, to

assess the effectiveness and adaptability of international norms in regulating such conflicts. The method will also help explore the broader implications of these challenges for the conduct, understanding, and governance of cyberwarfare with the guidance of this research question:

> How does cyber warfare in the Russian-Ukraine war challenge established legal and ethical norms for civilian protection, and what are the broader implications for the conduct and regulation of modern conflicts?

1.3 Delimitations

The delimitations in this thesis on the application of IHL and the Tallinn manual in the context of cyber warfare within the Russian-Ukraine war are important to highlight to focus on the scope of the research and answer the research question. For such it is important to maintain a clear study of specific legal and ethical issues rather than broader technical or geopolitical analyses.

As mentioned in the aim, for this thesis I will be following a qualitative research design. Despite the many positive outlooks of qualitative research, there are some drawbacks to qualitative case studies in general. The depth of analysis is a resource and time-consuming, which can impact project timelines and resource allocation (Yin, 2018:70). If more time had been given to this thesis, I would have increased my research area and included other conflicts to see differences and similarities between the cyber warfare and how they impact and matter to civilian security.

IHL is designed to ensure that all parties in an armed conflict are subject to the same legal and ethical standards, however, this thesis specifically focuses on Russian cyber-attack on Ukrainian targets and does not equally examine Ukrainian cyber operations against Russia. This focus was chosen due to the availability of data, and the broader geopolitical implication of Russian tactics in the cyber domain. In short, this limitation does not suggest an imbalance in the application of legal principles but rather a focused approach to study on aspect of the cyber conflict.

While cyber warfare involves complex technical elements, this thesis deliberately limits attention to these technical details to focus on the legal and ethical aspects of these cyber-attacks. This approach ensures that the thesis stays centred on the implications of cyber

operations under IHL and the Tallinn manual. Despite the Russian-Ukraine war holding a large impact on the global geo-political framework, this study specifically focuses on the legal and ethical implications of cyber warfare activities. Furthermore, within the broader realm of cyber warfare, this thesis highlights the principles of distinction and proportionality, dual-use infrastructure, the role of non-state actors, and espionage and information warfare. Other aspects and principles of cyber-attacks like cyber deterrence, and deep technical cyber analysis are also relevant in the scope of cyber warfare, however, they are not the focus of this study. Lastly, although the analysis might naturally suggest some policy implications, the primary goal of the thesis is not to develop detailed policy recommendations for the combat of cyber warfare. Instead, it aims to assess the applicability and effectiveness of existing legal and ethical norms as mentioned above.

1.4 Chapter outline

Continuing from this introduction, chapter 2 will review the relevant research related to this topic and introduce the theoretical framework foundational to this study. Following this, chapter 3 will detail the chosen research methodology, explaining the adoption of a qualitative research design that incorporates exploratory case study methods combined with legal analysis to examine the research question thoroughly. Additionally, this chapter will describe the selection of materials pertinent to the investigation of this study. Chapter 4 will employ the discussed theories and methodologies for the analysis of specific cases from the selection of materials relevant to the study's focus. Lastly, Chapter 5 will conclude the findings drawn from the analysis, providing insights into the research.

2. Theory

This chapter addresses the theoretical framework and previous research for analysing the complex dynamics of cyber warfare within the context of the Russian-Ukraine conflict. Hence, aiming to answer the research question, providing insights into the evolving nature of conflict and the legal and ethical factors that arise. The chapter will begin with an exploration of Mary Kaldor's "New Wars" theory, which signifies a shift in modern conflict. This is relevant to the thesis as it helps connect International Humanitarian Law to the contemporary methods of cyberwarfare observed in the Russian-Ukraine war. Following this, the chapter will lay out the foundations of IHL, providing the norms that lay out the legality and morality of warfare. Lastly, the chapter will use Kaldor's theory to set a connection between the Geneva Conventions - traditionally associated with the Old Wars theory – and the Tallinn Manual which reflects the New Wars Theory. In all, this chapter aims to help the reader understand the necessary tools that are used to analyse the significant legal and ethical implications of cyber warfare during the Russian-Ukraine conflict and help answer the research question.

2.1. Mary Kaldor's "New Wars" and "Old Wars" theory

Mary Kaldor's New Wars theory has played an important role in redefining how scholars and strategists understand modern conflicts. Kaldor's theory is relevant to this thesis and provides a clear framework for understanding the evolution of cyber warfare in the Russian-Ukraine war because it will prove that the case of the Power Grid cyber-attack in 2015 applies to IHL. In Kaldor's (1999) "New and Old Wars: Organized Violence in a Global Era", the theory has evolved through academic debate and different global events that have expanded its meaning. Clausewitz's theory, famously summarizing that "war is merely the continuation of policy by other means," highlights that military conflicts serve as tools for states to pursue political goals, evident in events like Russia's annexation of Crimea (Zasenko, 2024). Kaldor's New Wars theory suggests a shift towards conflicts characterized by broken states, non-state groups, and identity politics rather than the geopolitical factors emphasized by Clausewitz (Kaldor, 2012: 16). In the 'New Wars' that have emerged since the end of the Cold War, identity politics – which focuses on conceptions of who we are – has become more prevalent than geopolitics, which deals with strategic interests, or policy, which addresses the methods of achieving these interests

(Kaldor, 1999:8). This brings us further to the new war characteristic of blurring of lines between combatants and civilians, which will be investigated greatly in the analysis. In contrast to traditional wars, Kaldor's (2012) new wars are marked by asymmetry and ambiguity. Combat zones are often indistinguishable from non-combat zones and new wars are often less about achieving clear military victories and more about controlling populations through fear (ibid.). All these characteristics come across in the three cases, hence this perspective will help articulating and analysing those blurred lines.

Furthermore, Kaldor's theory also focuses on the blend of civilian and combatant roles, challenging the clear distinctions and structured battlefields, typical in Clausewitzian theory (Kaldor, 2012: 2). Kaldor further writes, that Clausewitz's idea that war is similar to a duel on a grander scale suggests a level of equality between the adversaries. However, this concept appears increasingly irrelevant in the typical conflicts of the current era, where the objective is not necessarily to defeat an opponent but to politically benefit from the ongoing violence (Kaldor, 1999: 6). The quote emphasizes how modern conflicts challenge the traditional theories to explain the reality of contemporary warfare. Which in the case of cyber warfare is often present due to its constant change in new cyber techniques and tactics. In her book, Kaldor illustrates the old wars to new wars transformation through various contemporary conflicts, highlighting how certain wars are financed not through state expenditure but through a war economy involving looting, smuggling, and control over natural resources (Ibid: 70). Which will be important to keep in mind for the analysis where I will have to find the distinction between civilians and combatants in the three cases of Russian cyber-attacks.

Kaldor's (2012) ideas on non-state actors will also be used for the analysis. These actors, which include militias, warlords, paramilitary groups, hacker groups, and terrorist organizations, are key in Kaldor's theory because they emerge in regions where state authority is absent (ibid.). Non-state actors use unique cyber techniques to conduct attacks that blur the lines between civilian and military targets, complicating the enforcement of IHL. Moreover, Kaldor states that these groups redefine the landscape of conflict by diminishing the differences between state and non-state actors.

While Kaldor's New Wars theory has influenced the understanding of modern conflicts, it has also faced criticism from various scholars who challenge its analytical aspects. Critics argue that the features Kaldor identifies in her New Wars theory have come forth

in history already and that her theory may oversimplify complex conflict aspects, which should be considered for this thesis. This perspective encourages a nuanced exploration of the interactions between state and non-state actors, and the multifaced legal implications under IHL.

One of the primary criticisms is that the aspects Kaldor describes as 'new' are, in fact, longstanding aspects of warfare (Newman, 2004). Scholars like Adam Roberts have pointed out that many of the tactics and motivations outlined by Kaldor have been evident in past conflicts. He specifically argues, "The phenomena described as 'new' have historical precedents, and what we are witnessing might be better understood as an evolution of warfare rather than a radical break from the past" (Roberts, 2010: 5). This perspective suggests that Kaldor's theory might exaggerate the details of contemporary conflicts. For this thesis, Kaldor is useful because it provides a framework to understand the complex nature of modern cyber conflicts. In the case of cyber warfare in the Russia-Ukraine War, this thesis can be rest assured that the cases analysed are some of the first incidents of state lead cyber-attacks ever recorded in history (European Parliament, 2022), hence defending Kaldor's New Wars theory.

While this critique suggests that the theory should be investigated with caution and used with other analytical perspectives, Kaldor has addressed these criticisms with a notable defence in her later works. "While it is true that many features of new wars can be found in the past, what is new is the combination of these features or the particular way these features come together in the late twentieth and early twenty-first centuries" (Kaldor, 2013: 7). The quote connects with Kaldor's idea that the globalized world, with its interconnected economies and communication technologies, has fundamentally changed the idea of conflict, like cyberwarfare in the Russia Ukraine war.

2.2. International Humanitarian Law (IHL)

IHL, which is often referred to as the laws of war, is a set of rules that seek to limit the effects of armed conflict for humanitarian reasons (ICRC, "What is Humanitarian Law?"). In other words, it aims to protect people who are not or are no longer participating in the hostilities and to restrict the means and methods of warfare (Ibid). This section will explore the origins, and key principles of IHL, which will be used in the application of the three cyber-attack cases analysed in this thesis.

IHL draws significantly from the philosophical sphere of Just War Theory. This theory articulates the moral guidelines under which war can be justifiably initiated (jus ad bellum) and the manners in which it can be ethically conducted (jus in bello) (Henriksen, 2017: 261). In the analysis, this thesis will specifically investigate jus in bello with the help of the Geneva Conventions and the Tallinn Manual, analysing cyber warfare within the IHL framework during the Russia-Ukraine war. Michael Walzer, a prominent political theorist, highlights the connection between IHL and Just War Theory, "The rules of Just War Theory have their parallels in what we now call international humanitarian law, the legal rules that restrain belligerents during the fighting" (Walzer, 1977: 44). In contemporary settings, there have been multiple researchers that claim that the application of Just War Theory through the lens of IHL continues to be relevant in addressing the ethical challenges posed by new forms of warfare. For example, as Yoram Dinstein quotes, "The principles of distinction and proportionality, derived from Just War Theory, remain central to the legal evaluation of military operations under IHL" (Dinstein, 2016: 78). The principles of distinction and proportionality in IHL require that combatants always distinguish between military targets and civilians during conflict and ensure that any military action if focused to the actual military advantage, avoiding civilian harm (Ibid.). This will highly be used throughout the analysis as all three cases have examples where the principles of distinction are ignored.

Formed from the Geneva Conventions and the Hague Conventions, the IHL forms a body of rules that aim to limit the effects of armed conflict (Henriksen, 2017). The legal structure is primarily categorized into two distinct yet complementary bodies of law: the Law of Geneva, which focuses specifically on the protection of non-combatants in wartime, and the Law of Hague, which governs the means and methods of warfare (Ibid). It is important to note that IHL has continually adapted to changes in warfare. These adaptations have been necessary to address new technological advancements and changes in warfare tactics (Ibid).

2.3. IHL and the Tallinn Manual in the scope of "Old Wars" and "New Wars"

The Geneva Conventions are the pinnacle of IHL, "The Geneva Conventions redefined the boundaries of wartime conduct, aiming to protect those who are not part of the fight"

(Keegan, 1993: 25). As the historian John Keegan discusses, the Geneva Conventions are traditionally associated with the conduct of Old Wars, state-centric conflicts involving clear distinctions between combatants and civilians (Ibid). In retrospect, the Tallinn Manual addresses the legal challenges posed by cyber warfare. "As warfare enters the digital realm, the application of traditional legal principles becomes less clear, yet more crucial" (Schmitt, 2017: 2). As Schmitt quotes, it is interesting to see how as warfare has evolved, new guidelines became necessary to address these modern challenges. Hence, the thesis will make the connection the connection on how IHL and the Tallinn Manual can be used to understand the new types of warfare, characterised by Kaldor's 'New War' tactics and actors.

There could be a connection made between the Geneva Conventions and Kaldor's New Wars theory that I would like to investigate for my analysis. One could claim that the Geneva Conventions traditionally are focused on the conflict's characteristics of 'Old Wars' in Kaldor's framework, where state actors and clear battle lines predominate. As Walzer notes, "The Geneva Conventions were created in a time when war between nation-states with uniformed armies was the norm, which directly influenced their emphasis on differentiating combatants from non-combatants" (Walzer, 1977: 264). The quote depicts the direct correlation between Kaldor's depiction of Old Wars that were focused on nation-state warfare (Kaldor, 2012). Additionally, the conventions' protocols on the protection of hospital ships, cultural artefacts, and the prohibition of certain types of weaponry, such as chemical and biological weapons, reflect the type of conventional warfare legislated against during the drafting of the Geneva Conventions (Geneva Conventions, 1949). Another example could be found in Article 3 of the Geneva Conventions, which focuses on human treatment without adverse distinction based on race, religion, or political opinion, which exemplifies the focus on traditional battle scenarios typical of Old Wars (Ibid.). Despite the traditional connection, warfare has evolved that in a way blur the lines between civilian and military targets. The quote by Kennedy represents the ongoing development and need to adapt the principles of the Geneva Conventions: "While the Geneva Conventions were adequate for the wars they were designed to regulate, the emergence of new warfare tactics, such as cyber warfare and unmanned aerial attacks, challenges their applicability" (Kennedy, 2006: 18).

The Tallinn Manual, unlike the Geneva Conventions, is explicitly used to address the complexities of modern warfare, particularly cyber warfare, which can be considered an

aspect of Kaldor's depiction of New Wars. The Tallinn Manual serves as a legal framework for understanding and applying international law to cyber conflicts, it offers guidelines that reflect the decentralized network, and other cyber warfare tactics (Schmitt, 2013). "Cyber warfare introduces a range of legal complexities that traditional laws of. Armed conflicts were not designed to manage, necessitating a specialized approach to understand and regulate these new forms of hostility" (Ibid: 102). Hence, the Tallinn manual acts as a legal manual where existing IHL may struggle to interpret these implications of cyber tactics which can be relevant to Kaldor's New Wars concept. Since published in 2013, the Tallinn Manual already has two manuals with a third version being developed this year. This is due to the need for clarification and the constant development of new cyber technology that leads to new regulations (Ibid, 2017). The reason for the creation of the Tallinn Manual is mainly due to the 2007 cyber-attacks on Estonia, which severely disrupted the country's digital infrastructure. "The 2007 cyber incidents in Estonia propelled the need to systematically analyse how existing international laws apply to this new form of warfare, which traditional legal texts did not explicitly address" (Ibid: 5). The manual explored principles such as sovereignty, state responsibility, and the applicability of IHL in cyberspace, which will all be used as a critical legal guide in the analysis. It will help in evaluating the legality of the cyber-attacks and help assess whether these incidents comply with IHL. As Watts argues, "The application of principle like proportionality in cyber operations challenges traditional interpretations, as the line between civilian and military assets is often indistinct in digital environments" (Watts, 2015: 88). In all, the manual's discussions around proportionality and distinction resemble with Kaldor's analysis of New Wars, where such principles should be revised due to the non-traditional warfare methods.

3. Methods

3.1. Design

This thesis will focus on the application of IHL and the Tallinn Manual on three distinct cyber-attacks during the Russian-Ukraine war because they help highlight the unique challenges and implications for civilian protection and international norms within the scope of modern warfare. To explore these dynamics of cyber warfare within the Russian-Ukraine war, specifically its challenges to establishing legal and ethical norms for peace and security, I have chosen to use a qualitative research design. A qualitative research design enables me to research specific cases in-depth which allows for a greater understanding and the opportunity to implement a legal framework analysis (Chambliss and Schutt, 2010: 233). I will be following an exploratory case study method, which as Yin outlines, can help provide a structured approach to exploring phenomena within a real-life context (Yin, 2018: 65) and will be further explained later in this chapter. Furthermore, the chapter will explain the choice of material which are the three cases mentioned above and how it connects with IHL and the Tallinn manual serving as the legal and ethical framework to evaluate the cases. In all, for my analysis, I will be using a mix of primary and secondary data and other published research focused on cyberwarfare and international law in the Russian-Ukraine conflict to help provide information that supports the legal and ethical findings of the thesis.

Qualitative research, as described by Creswell, is essential for researching intricate issues that require an in-depth understanding of contextual influences, processes, and experiences of those involved in the event (Creswell, 2013: 126). Hence, it allows for further exploration of the cases. For this thesis, it is essential to understand the dynamics and complexities behind cyber warfare, which involves not only technical aspects but also legal, ethical, and social dimensions. Qualitative research enables me to consider and use IHL and the Tallinn manual to analyse cyber warfare (Chambliss and Schutt, 2010: 234). Qualitative research is inherently flexible, it also allows me to adapt my methods as the study progresses further, which is much needed in the rapidly evolving field of cyber warfare (Creswell, 2013: 125). The key advantage of this is that I will be able to build on my interpretations from my findings. For this thesis specifically, I will need to adjust my

methods according to the three different types of cyber-attacks as will be seen in the analysis. Another strength of qualitative research that will be beneficial for my paper is that it allows for solid contextual insight. Hence, cyber warfare is not a factor that is dependent on itself, it is largely influenced by and influences international relations, national security, and global legal norms (Nye, 2010: 5). I will be able to examine not only the three complex cyber operations itself, but also its effects on peace, conflict, and security, using a wide contextual insight.

The exploratory case study method is well suited for this thesis because it allows for an in-depth investigation of different cyber-attacks which challenge legal and ethical norms. The exploratory case study method, as outlined by scholars Yin and Eisenhardt, provides a framework for conducting investigations that allow me to look not just into the cyber-attacks themselves but also the outer aspects such as legal, ethical, and social implications (Yin, 2018; Eisenhardt, 1989: 535). Eisenhardt highlights the flexibility of case study research as a strength (Ibid), enabling me to adapt my research based on emerging data, hence strengthening my knowledge, and allowing me to look at the cyber-attacks from different perspectives. Lastly, an exploratory case study can set foundations for theoretical insights, for instance, will help me lay out a connection between cyberwarfare and IHL (Ibid).

In order for this thesis to apply established legal and ethical norms for civilian protection to the three cases, I must first prove that the three cases fall under IHL. As stated in Common Article 2 of the Geneva Conventions: “The present Convention shall apply to all cases of declared war or of any other armed conflict which may arise between two or more of the High Contracting Parties, even if the state of war is not recognized by one of them" (ICRC, art. 2, 1946). This statement proves that IHL applies from the onset of any conflict, regardless of formal recognition or declaration. While most people would point out the start of the Russian-Ukraine conflict as the Russian military invasion in 2022, according to the independent organisation, International Crisis Group, the armed conflict began in 2014 in Eastern Ukraine when Russian-backed separatists clashed with Ukrainian government forces, which by early 2022 already resulted in 14,000 deaths (International Crisis Group, 2024). Two of the three cases take place after the 2022 invasion where two different state parties – Russia and Ukraine – conflict with one

another. Following the rules of IHL there was no official conflict between Ukraine and Russia during 2014 – 2022, hence disabling me to use the Ukrainian Power Grid Cyber-attack in 2015 as a case, since Russian separatists are not defined as the Russian state. To apply IHL to the Power Grid cyber-attack that happened in 2015, I must incorporate Kaldor's theory of New Wars to help explain why the conflict began intensifying between the two states in 2014 and not just with the 2022 invasion. In the context of the 2014 conflict, the involvement of Russian-backed separatists and the subsequent cyber-attack can be seen as part of a broader strategy that is blurred between war and politics (Kaldor, 2012). In all, the application of IHL to the power grid cyber-attack in 2015 is not only a legal necessity but also a great case to address the humanitarian implications of new war tactics.

3.2. Choices of Cases

I have decided to explore three well-known cases of cyber-attacks that occurred during the Russia-Ukraine war: the 2015 Russian cyber-attack on the Ukrainian power grid, the 2023 Russian cyber-attack on Kyivstar, and the 2022 Asylum Ambuscade cyber-attacks on Ukrainian refugees and humanitarian organizations. The three cases represent significant milestones in the realm of cyberwarfare. One could say that these events call for a need for global awareness and new cybersecurity measures to further protect civilian security, hence are good examples to analyse in this thesis. These attacks exemplify issues with proportionality, as the extensive damages to civilian life and infrastructure appear excessive compared to the unclear military advantages gained. In all, through this lens, I want to focus my analysis to shed light on how three distinct cases help as evidence to answer the research question.

3.2.1. The 2015 Russian Cyber-attack on the Ukrainian Power Grid

The 2015 Russian cyber-attack on the Ukrainian power grid was a sophisticated cyber-attack that left 230,000 residents of the Ivano-Frankivsk region without power in December 2015 (Council on Foreign Relations, 2023). The main material from the case that I will use for the analysis is the data collected from a joint analysis of the SANS (SysAdmin, Audit, Network, and Security) Institute and The Electricity Information Sharing and Analysis Center (E-ISAC) on the '2015 Cyber Attack on the Ukrainian Power Grid' (SANS & E-ISAC, 2016). This analysis "summarizes important learning points and

presents several mitigation ideas based on publicly available information on ICS incidents in Ukraine" (Ibid: iii). I will also be using other secondary sources of analyses from other independent international organizations like the Cybersecurity & Infrastructure Security Agency (CISA) (Cybersecurity & Infrastructure Security Agency, 2016) the Center for Strategic and International Studies (Center for Strategic and International Studies, 2022), and the Human Rights Watch (Human Rights Watch, 2022) for further in-depth analysis. This will help support my thesis in the form of triangulating their findings and providing more evidence to analyse it to IHL and the Tallinn Manual. The data I will be using for the 2015 Cyber Attack on the Ukrainian Power Grid provides solid evidence for IHL and the Tallinn Manual because I can assess the damage done to civilian structures and analyse the potential distinction between civilian and military targets.

3.2.2. The 2023 Russian cyber-attack on Kyivstar

The second case I will use for the analysis is "the largest cyberattack on telecom infrastructure in the world" as Kyivstar CEO, Oleksandr Komarov described it (Atlantic Council, 2022). Also known as the Kyivstar hack, was a cyber-attack in 2023, where "a widespread external cyberattack, resulted in a temporary disruption of Kyivstar's network and services, interrupting the provision of voice and data connectivity on mobile and fixed networks, international roaming, and SMS services, amongst others, for Kyivstar customers in Ukraine and abroad" (VEON, 2024). Kyivstar has around 24 million Ukrainian mobile subscribers which were all impacted by the attack (Atlantic Council, 2022). Specifically, according to multiple international news outlets, 53 people including 6 children were injured from Russian missile strikes because the air raid sirens were disrupted due to the cyber-attack (CNN, 2023 & Reuters, 2023). I will be using official government statements of the attack and similar examples like the incident mentioned above. To avoid bias I will also be using documents from The International Bar Association (IBA, 2024). Lastly, I will also be using published academic research papers like "Reflection on the Russia-Ukraine War" by Rothmans (2024) to connect and analyse with the help of IHL and the Tallinn Manual.

3.2.3. The 2022 asylum ambuscade cyber-attacks on Ukrainian refugees and humanitarian organizations.

The third case I will analyse is the cyber-attacks affecting and targeting Ukrainian refugees and humanitarian organizations in 2022. In short, "during and following the mass

movement of Ukrainian refugees out of the country, hackers affiliated with the Russian Federation and with links to Belarus began carrying out cyberattacks with intent to steal refugee data, cause fear and panic through the spread of disinformation, and slow refugee movement" (Howard, 2023). I chose this case because it provides a critical examination of how cyber warfare extends beyond military objectives, which I would like to highlight within my analysis. I also believe that this case will bring strong ethical and legal challenges in IHL and the Tallinn Manual, hence helping to answer the research question. To get the correct data for the case, I will be using numerous academic publications and reports of international cyber security companies like Proofpoint (Cass, 2022) that investigated this specific case. In order to avoid bias I will also look into independent non-governmental organisations like Access Now (Access Now, 2023), and a resolution adopted by the Human Rights Council (HRC) of the UN (HRC, Resolution 55/23).

3.3. Source Criticism

One of the primary challenges in analysing the three cases is the difficulty of pointing out cyber-attacks to specific actors. Cyber-attacks often leave limited trails and can be conducted remotely often anonymizing the perpetrators. As mentioned in the Tallinn Manual (Schmitt, 2017), this does not only complicate the factual events of each case but also poses a hurdle in analysing the legal and ethical norms for civilian protection according to IHL. For the analysis, I have chosen to use mostly data and reports based on the Ukrainian and international humanitarian organisations' perspectives. This is mostly due to the fact that Russian authorities have either remained silent or denied involvement in these cyber operations (SIPRI, 2023). Moreover, investigations into these cases suggest that the perpetrators are not direct hackers of the Russian state but rather fall into the category of non-state actors who operate independently but whose activities align with the interests or objectives of the Russian regime. Kaldor's theory of new wars, which emphasizes the role of non-state actors would help explain the dynamics within these cases (2012). It also underscores the complex connection between state and non-state actors in contemporary warfare, where cyber capabilities provide a veil of anonymity and plausible deniability that traditional warfare does not.

Furthermore, for the three cases I will be analysing, to avoid bias and keep a balanced perspective I have decided to utilize a broad range of sources that would also help triangulate various data. I will be using independent nonpartisan organisations and think tanks like the Stockholm International Peace Research Institute (SIPRI), the Center for Strategic and International Studies (CSIS) or the Council of Foreign Relations (CFR). I will also be using international humanitarian organisations like, Access Now, The Human Rights Watch, the International Bar Association (IBA), and the United Nations (UN). In all, this selection of sources will help me establish the legal and ethical norms applicable to each of the cases, which will also help contribute to a non-biased, balanced viewpoint.

3.4. Analytical Framework

For this thesis, I will integrate a legal framework analysis in correspondence with IHL which will provide a strong foundation for a thorough legal analysis. I will also be using the Tallinn manual as a guide and reference when connecting legal norms to cyber-attacks (Schmitt, 2017). As mentioned before, the Tallinn manual is a guide and reference when connecting legal norms to cyber-attacks (Schmitt, 2017). Following the legal framework analysis called, the traditional doctrinal analysis method outlined by Hoffman and Rumsey will allow me to pinpoint and analyse the specific legal challenges arising from the cyber-attacks and to critically assess the applicability of IHL for civilian safeguarding (Hoffman and Rumsey, 2017: 71). I will be using a simplified version explained in Hoffman and Rumsey which will focus on the three following factors (Ibid). Firstly, identification of relevant legal issues, which will involve pointing out the specific areas of IHL that are challenged by the cyber-attack. Secondly, a compilation and examination of legal sources will provide all legal norms, rules, and principles relevant to the identified issues. Lastly, an analysis and application of legal norms should assess whether these legal norms are adequate. Mostly, as stated in Hoffman and Rumsey (Ibid), a fourth factor is addressed, focusing on the synthesis and recommendations which evaluate the effectiveness of the current legal framework within a state, in addressing the challenges posed by cyber warfare. The three steps mentioned will be the guidelines of the analysis, splitting each of them into sections for each case for a better understanding and clarity of the analysis. I will not be focusing on connecting recommendations to current state legislation because the goal of this thesis is to only analyse the challenges existing from IHL for civilian protection, and not state-based legislation. In all, I believe

these three steps that conclude a simplified traditional doctrinal analysis method, offer a solid understanding of IHL and its positioning with cyber warfare.

4. Analysis

The chapter builds upon the foundational knowledge established in the earlier chapters to understand how cyber-attacks pose a significant challenge to IHL and the Tallinn Manual, specifically in the context of protecting civilians during the Russian-Ukrainian war. The analysis will focus on three cyber-attack cases that exemplify the complexities of cyber warfare and its implications for legal and ethical norms: the 2015 cyber-attack on the Ukrainian power grid, the cyber-attack on Kyivstar in 2022, and the 2022 cyber operations where Russian hackers targeted Ukrainian refugees and humanitarian organizations with manipulative propaganda. Each case study will include a legal analysis aimed at investigating specific violations of IHL, which will explain the legal and ethical norms challenged or breached during these attacks.

4.1. The 2015 Cyber-Attack on the Ukrainian Power Grid

In modern warfare, power grids represent dual-use infrastructure due to their critical role in supporting civilian populations for heating, lighting, and communication, making them fundamental to daily life (Zetter, 2016). On the other hand, they also serve as communication, electricity, and logistics for military purposes and operations. In Ukraine, the strategic importance of power grids has been highlighted through repeated Russian missile and cyber-attacks during the war. The targeting of Ukrainian power grids has evolved into a tactic of warfare, aiming to create both physical and psychological pressures on the civilian population, while indirectly supporting military objectives (Rothmans, 2024). This section will analyse the first accounted cyber-attack on a Ukrainian power plant where civilians were affected, pointing out both legal and ethical standards of IHL and the Tallinn Manual.

On December 23rd, 2015, at 3:30 p.m., in the Ivano-Frankivsk region of Western Ukraine residents and power control centre operators were winding down their workday when suddenly, an unexpected cyber-attack occurred. An operator noticed the cursor on his computer moving autonomously, manoeuvring to shut down the circuit breakers of multiple regional substations (SANS & E-ISAC, 2016). The curser confirmed the shutdown, leaving 230,000 people in the cold darkness for at least 6 hours before some of the power plant workers managed to place firewalls and reboot a few substations (ibid.). Average winter temperatures in Ukraine fall around minus 3 degrees Celsius and can hit

lows of down to minus 20 degrees (Human Rights Watch, 2022). This left people without or at least temporary access to electricity, water, sanitation systems, heat, and related vital services (ibid.) One can also think about businesses, or hospitals that need power to use life-saving equipment and maintain critical healthcare operations. On top of the 6 hours when all 230,000 civilians did not have power, according to the United States (US) Cybersecurity & Infrastructure Security Agency (CISA) (2021) the power plant had difficulties running its systems for the following 5 months due to the cyber-attack. The CISA conducted this evidence through incident reports, system logs, and technical assessments (CISA, 2021). Hence, for multiple months, Ukrainian civilians had to go through the winter with a lack of essential services to survive. After analysing the cyber-attack, the CISA and Ukrainian intelligence agencies concluded that "Russian nation-state based cyber actors working for Russian intelligence" accounted for the cyber-attack on the Ivano-Frankvisk power grid (CISA, 2021). These claims can be backed with data, from the independent non-profit research organisation, CSIS. CSIS also claims that Russian hackers were behind the 2015 cyber-attack on the Ukrainian Power grid, triangulating the data.

In order to evaluate in relation to IHL and the Tallinn Manual, it is important to know the reason why Russia attacked the Ukrainian power grid as it determines the legality and legitimacy of the action. For example, Articles 52 and 57 of Additional Protocol I to the Geneva Conventions (1977) state: "Attacks shall be limited strictly to military objectives," and "do everything feasible to verify that the objectives to be attacked are neither civilians nor civilian objects and are not subject to special protection but are military objectives". Russian officials did not officially comment on the cyber-attack however according to, Robert Lee (Zetter, 2016) (a former cyber warfare operations officer at the US Air Force who also participated in the CISA investigation on the case) there is a reason why Russia did attack the Ukrainian power grid. In 2015 the Ukrainian parliament was moving towards a proposal to nationalize power companies in Ukraine, some of which were owned by a prominent Russian oligarch with close connections to Putin (ibid). According to Lee, "the cyber-attack might have been a signal to Ukrainian officials against the move towards nationalization" (Ibid.). Supporting this claim is the fact that the attackers limited their damage and chose not to physically destroy the power grid equipment, which would have prolonged the power outage. According to the international non-profit, think tank, Council on Foreign Relations

(CFR), the hackers could have destroyed the power grid because in 2007 the US government demonstrated an attack that showed how hackers could physically destroy a power generator simply by remotely sending only 21 lines of malicious code (Council on Foreign Relations, 2023) therefor, the potential intent of the cyber-attack was symbolic, suggesting a retaliatory gesture and warning towards the Ukrainian government.

4.1.1. Legal perspective

In the next section, I will analyse the legal and ethical norms challenged in the case. Each segment aims to provide a detailed exploration of how the cyber-attack intersects with key norms according to IHL and the Tallinn Manual. IHL and the Tallinn Manual are applicable to this case, as outlined in the methods and theory chapters. This analysis uses Mary Kaldor's insights on modern conflicts, which support the relevance of these legal frameworks in addressing the complexities introduced by cyber warfare. Additionally, to help answer the research question, I will utilize the simplified version of the Hoffman and Rumsey legal framework (2017), as detailed in the methods chapter, to guide the analysis into each step explained by the framework (ibid.). Firstly, identifying the relevant legal issues will involve pointing out the specific areas of IHL and the Tallinn Manual that are challenged. Secondly, a compilation and examination of the norms and principles of the IHL and Tallinn Manual. Lastly, an analysis and application of the legal norms should assess whether these legal norms are adequate. This includes assessing the applicability of IHL principles and thinking about the three aspects discussed above.

4.1.1.1. Identifying the Relevant Legal Issues

This section will specify the areas of IHL, and the Tallinn Manual challenged by the 2015 cyber-attack on the Ukrainian power grid. The principle of distinction, articulated in Article 48 of the Geneva Conventions, mandates that “parties to the conflict shall at all times distinguish between the civilian population and combatants and between civilian objects and military objects” (ICRC, art. 48, 1977). The Tallinn Manual suggests, when looking into targets, that if a civilian object is being used for military purposes, it may become a legitimate target, otherwise it violates IHL when being targeted (Schmitt, 2017: 118-121). This links the principle of distinction: the distinction between a target for military purposes and not. Lastly, this section will also address Articles 52(2) and 57 which require that attacks must be directed only against military objectives providing a definite military advantage (ICRC, art. 52.2 & ICRC art. 57, 1977).

4.1.1.2. Compilation and Examination of the Norms and Principles

The second step of Hoffman and Rumsey's framework allows the thesis to dive deeper into the examination of the norms under IHL and the guidance provided by the Tallinn Manual. The principle of distinction requires all parties in a conflict to always distinguish between civilian objects and military objectives. Article 48 of the Geneva Conventions (1977) clearly delineates this obligation. As mentioned above, the Tallinn Manual highlights that if a civilian object is used for military purposes, it can become a legitimate target. Conversely, attacks on civilian infrastructures that do not serve a military function violate the principle of distinction (Schmitt, 2017: 118-121). Articles 52(2) and 57 focus on the prohibition of attacks that may cause incidental loss of civilian life, injury to civilians, or damage to civilian objects, which would be excessive in relation to the concrete and direct military advantage anticipated.

4.1.1.3. Analysis and Application

In this final section, I will apply the examined norms to assess the adequacy of the legal frameworks in dealing with the complexities of modern conflicts, a theme central to Kaldor's insights. For a legitimate military target under Article 52 (2), there must be a clear military advantage to the action. As provided in the data above, there was no indication of any direct military gain from cutting power to civilian areas, indicating that the action is disproportionate. This also implies a breach of Article 57, as the attack caused widespread damage to civilian life without a proportional military benefit. The cyber-attack was calculated, yet deliberately focused on essential power distributors that provide heat, water, and electricity for civilians. Therefore not distinguishing the civilians and military objects targeted in this case, hence violating Article 48. Especially because the cyber-attack was done with such precision and effectiveness, one can conclude that the target was chosen deliberately, making the matter of violating the norms even more severe. Adding to these considerations, Kaldor's (2012) insights on the blurred lines between state and non-state actors in modern warfare add complications to attributing responsibility. This challenges the clarity required under IHL to distinguish combatants from non-combatants and legitimate military targets from civilian ones. Furthermore, the affected targets from the power grid hosted little to no military capabilities as explained by Zetter (2016). However, the information gained about the case does not indicate that the power grid was used for such purposes, making the attack a violation of the principle

of distinction. The principle, as outlined in the Tallinn Manual, requires that all cyber operations during an armed conflict must clearly distinguish between military and civilian objects (Ibid.).

In all, this analysis of the 2015 Russian cyber-attack on the Ukrainian power grid illustrates a violation of IHL and highlights the dangers associated with cyber-attacks on critical infrastructures. Moreover, with this case, I attempted to shed light on the principles of dual-use infrastructures and distinction and proportionality which are pivotal in understanding the complexities and legal measures involved when civilian resources that serve both public and potential military functions become targets in conflicts.

4.2. The 2023 Cyber-Attack on Kyivstar

In the scope of cyber warfare, telecommunications networks have emerged as critical dual-use infrastructure, being a key supporter of communications and internet providers for both civilian and military domains. The 2023 cyber-attack on Kyivstar, Ukraine's largest telecommunications provider, disrupted communications for millions and highlighted the vulnerability of essential services to cyber operations (Peperkamp, 2024). The following section will explore the Kyivstar cyber-attack and examine the cyber-attack through the lens of IHL and the Tallinn Manual. In all, this analysis aims to shed light on the complex interplay between legal and ethical norms of cyber warfare.

On December 12th, 2023, Kyivstar, the largest mobile network operator in Ukraine, experienced a significant cyber-attack. Described by the CEO, Oleksandr Komarov, as "the most extensive attack on telecommunications infrastructure globally", the assault targeted the core network of Kyivstar, partially disabling all its functionalities for at least 2 days. The breach occurred through a compromised employee account, Komarov disclosed (Atlantic Council, 2022). According to an intelligence report of the attack from the UK Ministry of Defence (2023), the cyber-attack affected mobile and data services vital to over half of the Ukrainian population. As a result, approximately 24 million subscribers, both in Ukraine and internationally, were left without mobile and internet connectivity (Ibid.). Despite the server disruption, Kyivstar confirmed that no personal data was compromised (VEON, 2024). However, the cyber-attack did disrupt other critical services including "air raid sirens, banks, ATMs, and point-of-sale terminals" (UK Ministry of Defence, 2023). 12 hours after the initial cyber-attack in the early morning of December 14th, while all the air raid sirens were not functional due to the cyber-attack, a

barrage of Russian missiles struck Kyiv. According to research from the International Bar Association, 53 people, including six children, had been injured by the attack (IBA, 2024). An injured local told the news agency, Reuters, “There was no air raid siren. At around 4 a.m. (0200 GMT), I heard an explosion. We fled to the corridor, (the explosion wave) threw me into the doors” (ibid.). This incident marks one of the most disruptive cyber-attacks on Ukrainian networks ever, significantly impacting government resources and emergency services.

According to an official report from the Security Service Agency of Ukraine (SBU), Illia Vitiuk - the head of the cybersecurity department of the SBU – stated that the attack had minimal impact on Ukraine’s military capabilities (SBU, 2024). Moreover, according to the Vitiuk, Ukraine’s military does not depend on commercial telecom services and “only utilize distinct communication protocol and algorithms” (Ibid.). Furthermore, according to IBA, the Russian hacker group, Solntsepek claimed responsibility for the cyber-attack, which the IBA claims is connected to the Russian Armed Forces’ General Staff, specifically, Russia’s Main Intelligence Directorate (GRU) (IBA, 2024). The involvement of such groups highlights the characteristics of Mary Kaldor's New Wars theory, where non-state or quasi-state actors play significant roles in modern conflicts, blurring the lines between state and non-state warfare. Lastly, Vitiuk emphasized the severity of such cyberattacks on civilian infrastructure, suggesting they should be classified as war crimes (SBU, 2024.), further illustrating the challenges of applying traditional legal frameworks like IHL in the context of new war dynamics.

4.2.1. Legal Perspective

Just like in the previous section, this legal analysis will be using the simplified version of the Hoffman and Rumsey legal framework (2017). Split into three sections, resembling each step, identifying the legal issues, examining IHL and the Tallinn Manual, and lastly allowing me to apply an analysis of the legal and ethical norms violated or not. This will help me answer the research question and allow me to implement the chosen theory.

4.2.1.1. Identifying the Relevant Legal Issues

The analysis begins by identifying the legal issues relevant to the 2023 cyber-attack on Kyivstar. A legal norm central to this investigation is the principle of distinction under

Article 48 of Additional Protocol 1 (1977). Article 48 (ibid) states that all parties in an armed conflict, like that of the Russian-Ukraine war, are required to differentiate between military and civilian objects, which ensures that civilian infrastructure is not intentionally targeted. Moreover, the Tallinn Manual (Schmitt, 2017) states that if cyber operations result in significant harm or are part of a broader military campaign, they may be classified as acts of war. Another legal issue relevant is Article 57 sections 1 and 2 of Additional Protocol 1 (1977) which states that parties in conflict must,

> "do everything feasible to verify that the objectives to be attacked are neither civilians nor civilian objects… take all feasible precautions in the choice of means and methods of attack with a view to avoiding, and in any event to minimizing, incidental loss of civilian life, injury to civilians and damage to civilian objects… refrain from deciding to launch any attack which may be expected to cause incidental loss of civilian life, injury to civilians, damage to civilian objects, or a combination thereof" (ICRC, art. 57 (1), (2), 1977).

Lastly, articulated in Article 51 of Additional Protocol 1 (1977) as mentioned before plays a crucial role in assessing the legality of military actions. Section 5(b), states, "An attack which may be expected to cause incidental loss of civilian life, injury to civilians, damage to civilian objects, or a combination thereof, which would be excessive in relation to the concrete and direct military advantage anticipated, is prohibited" (ICRC, art. 51 (5), 1977).

4.2.1.2. Compilation and Examination of the Norms and Principles

Following the identification of legal issues, this section examines the second step of Hofmann and Rumsey's framework (2017) which is examining the foundational norms of IHL applicable to the case. As noted above, the Tallinn Manual states that if cyber operations result in significant harm or are part of a broader military campaign, they may be classified as acts of war (Schmitt, 2017). The strategic timing and effects of the Kyivstar cyber-attack, coupled with the physical missile strikes, suggest a coordinated effort to weaken Ukraine's civilian and defensive capabilities, proving that these actions are within the scope of acts of war. This analysis enables a deeper investigation into IHL, focusing on Article 57 sections 1 and 2 of Additional Protocol I (1977), which require that parties in conflict must do everything feasible to verify that the objectives to be attacked are neither civilians nor civilian objects and take all feasible precautions in the

choice of means and methods of attack with a view to avoiding, and in any event to minimizing, incidental loss of civilian life, injury to civilians, and damage to civilian objects. Lastly, Article 58 requires parties to the conflict to take precautions to protect the civilian population, individual civilians, and civilian objects under their control against the dangers resulting from military operations. This includes avoiding locating military objectives within or near densely populated areas.

4.2.1.3. Analysis and Application

After identifying and examining all applicable legal norms, this section analyses the cyber-attack with the legal norms showcased above. Given that the case disrupted critical civilian services without a demonstrable direct military advantage, it would be considered a violation under these guidelines. The cyber-attack on Kyivstar, which as noted above, significantly disrupted civilian communication services, which violates the principle of distinction. Kyivstar, the largest telecommunication provider in Ukraine has the potential to hold military objectives, however as stated by Vitiuk, Ukraine's military does not depend on commercial telecom services (SBU, 2024). This claim can be backed by a neutral source, the cyber security company, NTT Security based in Sweden (NTT Security, 2024). Thus, proving that the Russian hackers attacked with either no consideration towards civilian lives or targeted civilian infrastructure on purpose. Either way, there is no clear distinction made before or during the cyber-attack, hence, violating Article 48 of Addition Protocol 1 (1977).

Kaldor's concept of the blurred lines between state and non-state actors is particularly relevant in the case as well. The involvement of state actors in cyber operations that target or exploit civilian infrastructure, as seen in the Ukrainian context, complicates the application of traditional IHL. This blurring raises questions about responsibility and accountability, making it challenging to enforce legal norms effectively. Additionally, Kaldor (2012) discusses the transformation of warfare into a more networked and less territorially defined endeavour, which is evident in the strategic use of cyber operations to amplify the effects of traditional military attacks. This shift suggests that traditional legal frameworks like IHL might be inadequate for addressing new forms of conflict that integrate digital and physical strategies to achieve tactical advantages. This analysis reveals that the case is not only a violation of specific articles of IHL and the Tallinn Manual, but it also showcases a larger pattern of warfare where cyber operations are

used strategically to amplify the effects of physical attacks. This finding is important in addressing the research question, as it highlights how cyber warfare in the Russian-Ukraine war challenges the established legal and ethical norms for civilian protection. It suggests a shift towards more integrated approaches in warfare where digital and physical strategies are combined to achieve tactical advantages. Thus, complicating the application of traditional legal frameworks like IHL.

The cyber-attack not only disrupted the telecommunications network but also had severe secondary effects, notably the failure of air raid sirens during an air strike as mentioned before. The disabling of critical communication infrastructure and emergency response systems did not provide any discernible military advantage that could justify the extensive risk and actual harm to civilian life and property. Hence, this led to 53 people, including six children injured (IBA, 2024). Given these outcomes, the disruption of critical civilian infrastructure such as communication networks and emergency response systems, indicates that there was no proportionality towards military benefits acknowledged or done by the Russian hackers. In all, the extensive civilian harm caused by the cyber-attack on Kyivstar violates the principle of proportionality as defined in IHL. Through the analysis of the case, one can call for a critical reassessment of how cyber operations are planned and executed in conflict settings. Ensuring compliance with these norms is essential to protect civilian populations and maintain the integrity of IHL.

In all, the analysis of the 2023 cyber-attack on Kyivstar demonstrates numerous violations of IHL backed by the guidance of the Tallinn Manual. The case presents legal challenges through the targeting of dual-use infrastructure that significantly serves civilian purposes. It underscores the critical issues of distinction and proportionality under IHL. Overall, the analysis emphasizes the urgent need for enhanced protective measures and clearer guidelines to prevent and mitigate the impacts of cyber-attacks on civilian life.

4.3. The Asylum Ambuscade, Cyber-Attacks on Ukrainian Refugees and Humanitarian Organizations

As mentioned before the evolving landscape of cyber warfare, presents a complex challenge when it comes to the targeting of vulnerable populations such as refugees and humanitarian organizations. The asylum ambuscade, as defined by Proofpoint (Cass, 2022), was a series of cyber-attacks on Ukrainian refugees and humanitarian

organizations. These attacks not only disrupted essential services provided to displaced populations but also raised serious legal and ethical questions under IHL. This section of the analysis will focus on the asylum ambuscade, laying out the events of the case which will allow for a thorough legal examination through the framework of IHL and the Tallinn Manual. I will also have the principles of distinction and proportionality in relation to espionage and information warfare in mind while analysing the case.

As discussed in the Resolution adopted by the Human Rights Council (2024), multiple aggressive cyber-attacks have worsened the situation of human rights in Ukraine. In March 2022, the Russian hacker group, Ghostwriter sent phishing attacks seemingly from Ukraine's SBU targeted various Ukrainian entities, claiming to provide evacuation information (Howard, 2023). As Jānis Sārts, the director of NATO's Strategic Communications Center of Excellence states, "Ghostwriter is a Russian state-sponsored hacking group" (Howard, 2023), backing the involvement of the Russian state. Phishing as explained in Singer & Friedman (2014) is a form of cyber-attack that "uses 'spoofed' e-mails and fraudulent websites designed to fool recipients into divulging personal data such as credit card numbers, account usernames and passwords, social security numbers, etc…" (Singer & Friedman, 2014: 123). These emails, which were predominantly sent via Gmail, contained documents filled with malware that enabled access for the hackers to computers connected with the same device or networks (Cass, 2022). The Slovakia-based internet security firm ESET identified the malware and stated that the massive data breaches pose significant risks for the refugees in the forms of identity theft, manipulation and exploitation, and social and psychological damage (Brewster, 2022). In the same month, US-based Proofpoint located similar 'evacuation-themed' phishing attacks aimed at a European government body, focusing on individuals involved with managing refugee logistics (Cass, 2022). This indicates a strategic focus on disrupting operations critical to Ukrainian refugee support.

Furthermore, earlier, on February 25th, 2022, Ghostwriter launched a wiper attack on Ukrainian border stations, complicating the refugee flow into Romania (Access Now, 2023). A wiper attack is "designed to destroy data and bring systems down, typically leaving them inoperable and without the possibility of recovery" (Brooks, 2020: 87). This attack forced border agents to revert to manual processing, significantly delaying the crossing and exposing refugees to harsh winter conditions (SIPRI, 2023).

In January 2023 Ghostwriter also sent misleading emails circulated among organizations aiding refugees, for example, the NGO, Insecurity Insight, a Switzerland-based non-profit that has done work documenting attacks by the Russian Federation on Ukrainian hospitals, was hit with a mass phishing campaign (Ibid). Hence, illustrating the disruption of humanitarian organizations.

Lastly, also around January 2023, another wave of misleading e-mails circulated among the organisations aiding refugees (ibid.). These e-mails contained messages falsely claiming that Ukrainian men of military age would be forcibly returned to fight, urging recipients to insert personal details and locations of other Ukrainian soldiers (ibid.). According to Mandiant, a threat intelligence unit of Google Cloud, the emails also came from, Ghostwriter (Stone, 2023). These emails created panic and confusion among the Ukrainian refugees and humanitarian organisations that focused on aiding the refugees (Ibid.).

4.3.1. Legal Perspective

Lastly, in this legal analysis as for the previous cases, I will be using the simplified version of the Hoffman and Rumsey legal framework (2017), which will guide the investigation of the Asylum Ambuscade cyber-attacks on Ukrainian refugees and humanitarian organizations. The analysis will again be split into three sections, identifying the relevant legal issues, examining the norms and principles, and finally, analysing and applying them to the case, in all, helping answer the research question.

4.3.1.1. Identifying the Relevant Legal Issues

A relevant legal issue in this case can be seen in the Tallinn Manual which defines military objectives as objects which by their nature, location, purpose, or use make an effective contribution to military action (Schmitt, 2017: 127). Schmitt further writes that attacks are considered arbitrary if they are not directed at a specific military objective or if they employ means and methods that cannot be directed at a specific military target (ibid: 192). He also explains the principle of distinction, “Cyber operations that cannot be directed at a specific military objective, or those that cannot be controlled, are prohibited if they are expected to cause incidental loss of civilian life, injury to civilians, damage to civilian objects, or a combination thereof” (Schmitt, 2017: 100) which are all relevant

legal issues to this case. Secondly, according to the principle of necessity in IHL (Ohlin, 2016), parties to a conflict may only engage in military actions that are essential for achieving a legitimate aim and these actions must not exceed what is necessary to accomplish their military objective. Furthermore, identifying, Article 38 Protocol 1 (1977), "It is prohibited to improperly use internationally recognized distinctive emblems to shield favour, protect, or impede military operations" (ICRC, art. 38 (1), 1977). reveals a clear misuse of such emblems. Lastly, article 70 in Additional Protocol 1, states that "the protection of humanitarian relief personnel, and objects used in these operations must be respected and protected" (ICRC, art. 70 (1), 1977) which highlights the interference with humanitarian operations.

4.3.1.2. Compilation and Examination of the Norms and Principles

In exploring the legal norms shaped by the Tallinn Manual and IHL, key norms and principles relevant to the case become evident. The Tallinn Manual's definition of a military objective sets the foundational legal parameter (Schmitt, 2017: 127). Schmitt further explains that attacks are arbitrary if not directed at a specific military objective or if employing means and methods that cannot be directed at a specific military target. This is a critical point that reflects on the complex nature of the attacks in the case (ibid: 192). Additionally, the principle of distinction is crucial, the principle directly pertains to the current case where cyber operations seemingly targeted civilian infrastructures indiscriminately (Schmitt, 2017: 100). Furthermore, the principle of necessity as articulated by Ohlin (2016) underscores the legal violation of the cyber-attack, emphasizing the breach of this principle given the absence of military necessity in targeting civilian-focused infrastructures. An examination of Article 38 of Protocol 1 (1977) highlights the misuse of emblems in the conflict not only violating this norm but also leading to confusion and vulnerability during attacks. Lastly, Article 70 of Additional Protocol 1 is also of importance because it highlights the legal infringements related to the interference with humanitarian operations observed in the attacks. This underlines a significant violation of international law that impacts the efficacy and safety of humanitarian missions.

4.3.1.3. Analysis and Application

The analysis and application of IHL to this case show a clear breach of the principles of distinction and proportionality. The attacks in this case were indiscriminate, affecting

wide-ranging elements of civilian infrastructure and the daily lives of non-combatants, thereby constituting arbitrary attacks under IHL and violating the principle of distinction. Given that the targeted systems had no military utility, any civilian harm could not be justified by military necessity, violating the principle of proportionality. This analysis points to a fundamental misunderstanding or disregard for the legal constraints that govern acts of war. With Kaldor's theory of New Wars, one can point out the increasing involvement of non-state actors in modern conflicts (Kaldor, 2012). This theory helps explain the strategic targeting of civilian-focused infrastructure like refugee support systems, which, while lacking in direct military value, play a significant role in the broader strategy of war by disrupting societal functions and instilling fear objectives that align with the asymmetric warfare tactics highlighted by Kaldor (ibid.).

Targeting civilian-focused infrastructure such as the refugee support systems, does not fulfil a "legitimate military necessity" (Ohlin, 2016). The attacks primarily impacted vulnerable civilian populations and humanitarian operations, which did not contribute to any direct military advantage. In hindsight, it focuses on the opposite, preventing conflict from coming to civilians. Thus, such attacks, are violating the principle of necessity under IHL. The strategic use of a wiper attack reflects an intent to inflect long-term disruption rather than achieve a specific, limited military objective. This suggests that the attack was an excessive use of force, hence constituting a disproportionate response under IHL. The attack also destroyed the border control systems, which under IHL falls under "damaging civilian objects", again, violating the principle of distinction.

One can point out the undermining of the operational integrity and confidentiality of humanitarian data (Howard, 2023). Not only disrupting the protected operations but also endangering the lives of those who depend on the missions of Insecurity Insight for survival. Thus, this analysis can conclude that the cyber-attack on Insecurity Insight directly violates Article 70 of the Geneva Convention. In all, this attack also shows that the need for stronger protective measures and clearer legal guidelines is critical to safeguard the operations and data integrity of NGOs operating in wars such as the Ukraine-Russia war.

The legal examination of the asylum ambuscade, in which Russian cyber-attacks targeted Ukrainian refugees and humanitarian organizations, reveals multiple violations of IHL. With the findings supported by the interpretations from the Tallinn Manual, this analysis

can conclude that cyber-attacks on NGOs and civil objects do happen but are difficult to point out. Kaldor's analysis of New Wars provides a crucial theoretical framework for understanding these phenomena. It highlights how cyber warfare blurs the traditional boundaries of armed conflict and, hence, challenges the established legal and ethical norms for civilian protection, which also helps answer the research question. In all, with this analysis, I attempted to show that there is a critical need for stronger enforcement of IHL in cyber warfare but also calls for the development of clearer legal guidelines to effectively address the impacts of such cyber operations on civilian life.

5. Conclusion

Based on the analysis of the three cases, this thesis has highlighted the complex interplay between cyber warfare and IHL. The analysis has also brought out the legal and ethical challenges posed by such cyber operations. Through the application of the Tallinn Manual and IHL principles, one can conclude that there has been a consistent pattern of violations across all three cases. Each example demonstrated how cyber-attacks are often perceived as less destructive than conventional warfare, however, proves that cyber-attacks have the capability to create profound impacts on civilian populations, hence infringing upon established norms and protections ruled under IHL. In particular, the principle of distinction and proportionality have been critical in evaluating where there was no clear distinction between military and civilian objects This was the case for the power grid in the 2015 cyber-attack on the Ukrainian power grid, the telecommunications company in the 2023 cyber-attack on Kyivstar, and targeting refugees and humanitarian organisations in the 2022 Asylum Ambuscade.

This thesis has faced several limitations which are linked to the scope of data and sources, and the rapidly evolving field of cyber warfare. I chose to focus on three major cyber-attacks which represent grand examples of a major cyber-attack, from which the analysis can be looked at critically. Within the three cases, cyber-attacks in general are very covert. Much of the data regarding the three cases remains classified or undisclosed. This limitation restricts a more comprehensive analysis, really enabling me to dive deeper into its extent and thresh out the detailed outcomes of the attacks. Additionally, due to being very covert in nature, the data and sources of the Russian perspective on these three cases were often underrepresented or absent which leads to an imbalance and bias. I attempted to balance this out by using sources and data from international independent humanitarian organisations. Lastly, cyber warfare is an area of conflict that is rapidly evolving, which leads to legal and ethical standards to continuously develop. One can see this with the Tallinn Manual, which edition 3.0 is already being worked on due to new forms of cyber-attacks. Hence, the legal and ethical interpretations can quickly become outdated.

Furthermore, the thesis used Mary Kaldor's theory of New Wars which offered a clearer perspective on the nature of contemporary conflicts, especially in the context of cyber warfare. The theoretical framework was used actively in the analysis understanding the

role of non-state actors and the blurred lines between civilian and military targets which for example, complicated the principles of distinction and proportionality. In the role of non-state actors, as written in the theory chapter, these actors may not be officially affiliated with national governments but often operate with support towards them like the hacker group, Ghostwriter in the 2022 Asylum Ambuscade case. Kaldor's theory was also needed in order to prove that IHL and the Tallinn Manual were applicable to the case of the 2015 cyber-attack on the Ukrainian power grid due to its time period before the 2022 Russian invasion of Ukraine. In all cases, cyber-attacks are not fought on traditional battlefields but in situations where civilian life and military operations are linked. In all, with the usage of Kaldor's theory, one can also underline the urgent need for international law to evolve in response to these changing and developing tactics. The theoretical framework was essential for understanding the challenges posed by cyber warfare and points out the interpretation of IHL during these complex forms of warfare.

Answering the research question, this thesis brings out the urgent need for a change in international legal frameworks that can keep pace with technological advancements in warfare. Each example demonstrated violations of the numerous principles that should safeguard civilians during the complexities of modern warfare. The thesis pointed out that handbooks like the Tallinn Manual are a great start and example of how to change and develop regulations accordingly. The international community must work towards a greater consensus on defining and regulating state behaviour in cyber warfare to protect civilian populations and strengthen security. This can also be a note for further research, that there is a need to examine how international legal frameworks can be updated or how international law can connect specific actors more effectively. The constant and increased targeting of civilians in contemporary conflicts underscores the urgent need for states to adhere to the laws already in place and a need for new legal norms parallel to the constant technological development in cyber warfare. Future research could also benefit from a comparative analysis that includes Ukrainian cyber strategies to provide a balanced view of cyber warfare dynamics in the Russia-Ukrainian war. This thesis highlights how cyber warfare in the Russian-Ukraine war challenges established legal and ethical norms and concludes that these norms must be improved to help civilians from the harsh realities of cyber warfare.

6. References

6.1. Table of Legal Documents

Hague Regulations, (art. 29) ,1907.

Human Rights Council. 2024. *Resolution 55/23*.

International Committee of the Red Cross (ICRC) 1949, (art. 2), adopted 1977.

International Committee of the Red Cross (ICRC) 1949, (art. 38), adopted 1977.

International Committee of the Red Cross (ICRC) 1949, (art. 48), adopted 1977.

International Committee of the Red Cross (ICRC) 1949, (art. 51), adopted 1977.

International Committee of the Red Cross (ICRC) 1949, (art. 52.2), adopted 1977.

International Committee of the Red Cross (ICRC) 1949, (art. 57), adopted 1977.

International Committee of the Red Cross (ICRC) 1949, (art. 70), adopted 1977.

Lieber Code, (art. 88), 1863.

Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts (Protocol I), 8 June 1977.

Regulation 821/2021. *Regulation of the European Parliament and of the Council of 20 May 2021 setting up a Union regime for the control of exports, brokering, technical assistance, transit and transfer of dual-use items*. [online] Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32021R0821 [Accessed on 12th April 2024].

UN Doc. E/CN.4/Sub.2/1991/55 (December 2, 1990), available on http://www.un.org [Accessed on 12th April 2024].

6.2. Table of Academic Articles

Eisenhardt, K.M. (1989). Building Theories from Case Study Research. *The Academy of Management Review*, 14(4), pp.532-550.

Kaldor, M. (2013). "In Defence of New Wars," *Stability: International Journal of Security and Development*, 2(1), pp. 4-15.

Miller, L. H. (1964). 'The Contemporary Significance of the Doctrine of Just War.' *World Politics*, 16(2), pp. 254–286. JSTOR, [online], Available at: www.jstor.org/stable/2009507. Accessed 25 April 2024.

Newman, Edward. (2004). The 'New Wars' Debate: A Historical Perspective Is Needed. *Security Dialogue* vol. 35, no 2, pp. 173-188.

Roberts, A., (2010). "Lives and Statistics: Are 90% of War Victims Civilians?" *Survival*, 52(3), pp. 115-136.

Schuurman, Bart. (2010). "Clausewitz and the "New Wars" *Scholars. Parameters Spring*, pp. 89-100.

6.3. Table of Literature

Brooks, T. (2020). *The Art of Cybersecurity*. London: TechPress.

Chambliss D. and Schutt R. (2010). *Making Sense of The Social World*. 3rd ed, Pine Forge Press.

Clausewitz, C., von. (1832). *On War*, translated by Michael Howard and Peter Paret. Princeton: Princeton University Press, 1976.

Creswell, J.W. (2013). *Qualitative Inquiry and Research Design: Choosing Among Five Approaches.* SAGE Publications.

Dinstein, Y. (2016). *War, Aggression and Self-Defence*. 6th ed. Cambridge: Cambridge University Press.

Heller, K.J. (2022). *Low-intensity Cyber Operations and State Sovereignty in Cyberspace*. Djøf Publishing and The Centre for Military Studies.

Henriksen A. (2017). *International Law*. Oxford University Press.

Hoffman, M. and Rumsey, M., (2017). *International Legal Research in a Global Community.* Indianapolis: Indiana University Press.

Kaldor, M. (1999). *New and Old Wars: Organized Violence in a Global Era*. Stanford: Stanford University Press.

Kaldor, M. (2012). *New and Old Wars: Organised Violence in a Global Era*. 3rd ed. Stanford: Stanford University Press.

Kalyvas, S. (2006). *The Logic of Violence in Civil War*. Cambridge: Cambridge University Press.

Keegan, J. (1993). *A History of Warfare*. New York: Alfred A. Knopf.

Kennedy, D. (2006). *Of War and Law*. Princeton: Princeton University Press.

Miall, H. (2007). "*The Peacemakers: Peaceful Settlement of Disputes Since 1945*". London: Macmillan.

Nye, J.S., (2010). *Cyber Power*. Belfer Center for Science and International Affairs, Harvard Kennedy School.

Ohlin, Jens David, and Larry May. (2016). *'Necessity and the Use of Force in International Law'*, *Necessity in International Law*. New York. [online] Available at: https://doi.org/10.1093/acprof:oso/9780190622930.003.0003, accessed 19 Apr. 2024.

Plokhy, S. (2015). The Gates of Europe: A History of Ukraine. New York: Basic Books.

Ramsbotham, O., Woodhouse, T. & Miall, H. (2016). *'Contemporary conflict resolution: the prevention, management and transformation of deadly conflicts.'* 4th edn, Malden, MA: Polity Press.

Rothmans, M., Peperkamp, L. and Rietjens, S. (2024). *Reflections on the Russia-Ukraine War*. Leiden: Leiden University Press.

Schmitt, M.N. (ed.), (2017). *Tallinn Manual 2.0 on International Law Applicable to Cyber Operations.* 2nd ed. Cambridge: Cambridge University Press.

Singer, P.W., & Friedman, A. (2014). *Cybersecurity and Cyberwar: What Everyone Needs to Know*. New York: Oxford University Press.

SIPRI (Stockholm International Peace Research Institute. (2023). *SIPRI Yearbook 2023 Armaments, Disarmaments, and International Security.* Oxford, Oxford University Press.

Thürer, D. (2010). *International Humanitarian Law: Theory, Practice, Context.* Interdisciplinary Perspectives. Berlin: Springer.

Walzer, M., (1977). *Just and Unjust Wars: A Moral Argument with Historical Illustrations.* New York: Basic Books.

Yin, R. K. (2018). *Case Study Research and Applications: Design and Methods*. SAGE Publications.

Zetter, K. (2016). *Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon*. New York: Crown Publishing Group.

6.4. Table of Internet Sources

Atlantic Council. (2022). *Ukrainian telecoms hack highlights cyber dangers of Russia's invasion*. [online] Available at: https://www.atlanticcouncil.org/blogs/ukrainealert/ukrainian-telecoms-hack-highlights-cyber-dangers-of-russias-invasion/ [Accessed on 11th April 2024].

Berger, M. (2022, February 28). *400,000 Ukrainians flee to European countries, including some that previously* spurned refugees. The Washington Post. [online] Available at: https://www.washingtonpost.com/world/2022/02/26/europe-welcomes-refugees-ukraine-russia/ [Accessed on 2nd May 2024].

Brewster, T. (2022, March 4). *Warning: Hackers are targeting the Ukraine refugee crisis*. Forbes. [online] Available at: https://www.forbes.com/sites/thomasbrewster/2022/03/02/warning-hackers-are-targeting-the-ukraine-refugee-crisis/?sh=58a6104c7f8b [Accessed on 2nd May 2024].

Carnegie Endowment for International Peace. (2024). *Cyber Conflict in the Russia-Ukraine War*. [online] Available at: https://carnegieendowment.org/programs/technology/cyberconflictintherussiaukrainewar/ [Accessed on 12th April 2024].

Cass, Z., & Raggi, M. (2022). *Asylum Ambuscade: State Actor Uses Lua-based Sunseed Malware to Target European Governments and Refugee Movement.* Proofpoint. [online] Available at: https://www.proofpoint.com/us/blog/threat-insight/asylum-ambuscade-state-actor-uses-compromised-private-ukrainian-military-emails [Accessed on 12th April 2024].

Center for Strategic and International Studies (CSIS). (2023). *Responding to Russian Attacks on Ukraine's Power Sector*. [online] Available at: https://www.csis.org/analysis/responding-russian-attacks-ukraines-power-sector [Accessed on 11th April 2024].

CNN. (2023). *Ukraine cyber-attack.* [online] Available at: https://edition.cnn.com/2023/12/12/europe/ukraine-cyber-attack/index.html [Accessed on 12th April 2024].

Council on Foreign Relations (CFR). (2023). *Compromise of power grid in Eastern Ukraine*. [online] Available at: https://www.cfr.org/cyber-operations/compromise-power-grid-eastern-ukraine [Accessed on 30th April 2024].

Crisis Group. (2024). *Conflict in Ukraine's Donbas: A Visual Explainer*. [online] Available at: https://www.crisisgroup.org/content/conflict-ukraines-donbas-visual-explainer [Accessed: on 4th May 2024].

Cybersecurity & Infrastructure Security Agency (CISA). (2021). *IR-ALERT-H-16-056-01*. [online] Available at: https://www.cisa.gov/news-events/ics-alerts/ir-alert-h-16-056-01 [Accessed on 2nd May 2024].

Cybersecurity & Infrastructure Security Agency. (2016). *IR-ALERT-H-16-056-01*. [online] Available at: https://www.cisa.gov/news-events/ics-alerts/ir-alert-h-16-056-01 [Accessed on 11th April 2024].

European Parliament. (2022). *Briefing on Russia's war on Ukraine: Timeline of Cyber Attacks.* [online] Available at: https://www.europarl.europa.eu/RegData/etudes/BRIE/2022/733549/EPRS_BRI(2022)733549_EN.pdf [Accessed on 30th April 2024].

Gisel, L., Rodenhäuser, T. and Dörmann, K. (2021). Twenty years on: International humanitarian law and the protection of civilians against the effects of cyber operations during armed conflicts. *International Review of the Red Cross*. [online] Available at: https://international-review.icrc.org/articles/twenty-years-international-humanitarian-law-and-protection-civilians-against-effects-cyber-913 [Accessed on 11th April 2024].

Howard, L. (2023). *The Ukraine War: Cyberattacks Targeting Refugees and Humanitarian Organizations*. Jackson School of International Studies. [online] Available at: https://jsis.washington.edu/news/the-ukraine-war-cyberattacks-targeting-refugees-and-humanitarian-organizations/ [Accessed on 12th April 2024].

Human Rights Watch. (2022). *Ukraine: Russian attacks on energy grid threaten civilians*. [online] Available at: https://www.hrw.org/news/2022/12/06/ukraine-russian-attacks-energy-grid-threaten-civilians [Accessed on 2nd May 2024].

ICRC Law and Policy Blog. (2023). *Foghorns of War: IHL and Information Operations during Armed Conflic*t. [online] Available at: https://blogs.icrc.org/law-and-

policy/2023/10/12/foghorns-of-war-ihl-and-information-operations-during-armed-conflict/ [Accessed on 12th April 2024].

ICRC. (2019). *International Humanitarian Law and Cyber Operations during Armed Conflicts*, 2019. [online] Available at: https://www.icrc.org/en/download/file/108983/icrc_ihl-and-cyber-operations-during-armed-conflicts.pdf [Accessed on 2nd May 2024].

Ilves, T.H. (2014). *Statement at the 69th session of the United Nations General Assembly*. [pdf] Available at: https://gadebate.un.org/sites/default/files/gastatements/69/ee_en_25.pdf [Accessed on 12th April 2024].

International Bar Association (IBA). (2024). *Cyberattacks as war crimes.* [online] Available at: https://www.ibanet.org/Cyberattacks-as-war-crimes [Accessed: on 4th May 2024].

International Committee of the Red Cross (ICRC). (2022). *What is International Humanitarian Law?* [pdf] Available at: https://www.icrc.org/en/doc/assets/files/other/what_is_ihl.pdf [Accessed on 19th April 2024].

Koh, H.H. (2012). International Law in Cyberspace. *Harvard International Law Journal 54*, [online], Available at: https://openyls.law.yale.edu/bitstream/handle/20.500.13051/4383/International_Law_in_Cyberspace__54_Harvard_International_Law_Journal_Online_1__2012_.pdf?sequence=2&isAllowed=y [Accessed on 11th April 2024].

NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE). (2023). *Power grid cyberattack in Ukraine (2015)*. [online] Available at: https://cyberlaw.ccdcoe.org/wiki/Power_grid_cyberattack_in_Ukraine_(2015)#:~:text=The%20Ukrainian%20incident%20is%20the,has%20been%20conducted%20totally%20remotely. [Accessed on 19th April 2024].

NTT Security, 2024. *Russian hacker claims responsibility for massive cyberattack in Ukraine*. [online] Available at: https://se.security.ntt/en/russian-hacker-claims-responsibility-for-massive-cyberattack-in-ukraine/ [Accessed: on 12 April 2024].

Reuters. (2023). *Dozens injured in Kyiv in Russia's second missile assault this week on Ukraine.* [online] Available at: https://www.reuters.com/world/europe/dozens-injured-kyiv-russias-second-missile-assault-this-week-ukraine-2023-12-13/ [Accessed on 12th April 2024].

SANS and E-ISAC. (2016). *Analysis of the Cyber Attack on the Ukrainian Power Grid*. [pdf] Available at: https://nsarchive.gwu.edu/sites/default/files/documents/3891751/SANS-and-Electricity-Information-Sharing-and.pdf [Accessed on 11th April 2024].

Security Service of Ukraine (SBU). (2024). *SBU Identifies hackers who attack Kyivstar*. [online] Available at: https://www.ukrinform.ua/rubric-ato/3848169-illa-vituk-nacalnik-departamentu-kiberbezpeki-sbu.html?fbclid=IwAR0Uqgk7SzgttuV-lCiLsCTaHtzZTV_HzOgyWjyyLW7bBcnONY814LUFWwg_aem_ASu3pHfj5rMzq8HPLklFzEmoOcdzMmbVOw9VsKN5rZMI7gbqZJvyUo_d0LiNIGAL_rkkXSA2e4D2ZmnTjs5l8gUF [Accessed on 2nd May 2024].

Sheldon, J. B. (2024, January 4). *cyberwar*. *Encyclopedia Britannica*. [online] Available at: https://www.britannica.com/topic/cyberwar [Accessed: on 4th May 2024].

Stone, J. (2023, March 22). *A propaganda group is using fake emails to target Ukrainian refugees*. Bloomberg. [online] Available at: https://www.bloomberg.com/news/newsletters/2023-03-22/a-propaganda-group-is-using-fake-emails-to-target-ukrainian-refugees[Accessed on 2nd May 2024].

UK Ministry of Defence. (2023). *Intelligence Update* [Twitter]. Available at: https://twitter.com/DefenceHQ/status/1735993232247476720 [Accessed on 2nd May 2024].

VEON. (2024). *Kyivstar completes preliminary assessment of the financial impact of the cyberattack*. [online] Available at: https://www.veon.com/newsroom/press-

releases/kyivstar-completes-preliminary-assessment-of-the-financial-impact-of-the-cyberattack/ [Accessed on 12th April 2024].

World Bank. (2011). *World Development Report 2011: Conflict, Security and development.* [online] Available at: http://go.worldbank.org/UCTHLNS530 [Accessed on 12th April 2024].

Zasenko, O. Eliseyovich , Makuch, . Andrij , Hajda, . Lubomyr A. , Yerofeyev, . Ivan Alekseyevich , Kryzhanivsky, . Stepan Andriyovich and Stebelsky, . Ihor (2024, April 29). *Ukraine*. *Encyclopedia Britannica*. [online] Available at: https://www.britannica.com/place/Ukraine. [Accessed on 19th April 2024].