UCP Journal *of* Law & Legal Education
Vol. 2, Issue 1 (July - December 2023)

Cyberwarfare: Exploring the Inadequacies of Classical International Humanitarian Law

Khizar Ahmad*, Fatima Sajid**, Wejden Bourkrain***

Abstract

Cyberwarfare is a creation of the tech era that grew rapidly in the past three decades. Cyber operations have unveiled the massive potential of cyberwarfare capabilities to cause havoc in the real world. Technology has facilitated individuals, states, and other non-state actors to engage in coercive actions. It, therefore, becomes crucial to investigate the adequacy of classical International Humanitarian Law (IHL) to cater to the vicissitudes of technology warfare. This paper seeks to examine the relationship between IHL and cyberwarfare. It investigates the present legal regimes applicable to cyberwarfare and evaluates the applicability and limitations of the current rules of IHL, lex lata, to cyber operations. It discusses the 'Tallinn Manual, a comprehensive study by an International Group of Experts (IGE) on the international law of cyberwarfare. The paper aims to provide a realistic and critical perspective on the current legal approaches to cyber-warfare. The paper emphasises that the applicability of IHL is essential in the present world, and the rapidly growing technologies necessitate the parallel growth of IHL. This article underscores the absence of a legally binding International Law Convention that specifically governs cyberwarfare within the international realm as the rapidly evolving nature of cyberwarfare demands clear rules and regulations to govern cyber operations. Such a convention would promote adherence to international law in cyberspace and encourage cooperation between states in addressing cyber threats.

Keywords: Cyberwarfare, international humanitarian law, Tallinn manual, cyber security, cyber operations

***** Lawyer and academic in (Azad) Jammu & Kashmir, email: contact.khizarahmad@gmail.com. ** Bahauddin Zakariya University, email: fatimas.mirza2407@gmail.com *** Faculté des Sciences Juridiques, Politiques et Sociales, Tunisia, email: wejdenboukrain1@gmail.com
Article History: Received; 08, August 2023; Received in revised form 8, December 2023; Accepted 11, December 2023
Available online: 30 January, 2024

Introduction

IHL, commonly known as the law of armed conflict or *jus in bello*, constitutes a set of regulations primarily designed to mitigate the humanitarian impact of armed conflicts. In essence, IHL encompasses the international legal norms that establish baseline standards of humanity that must be upheld in any scenario involving armed conflict (Melzer & Kuster, 2016). The regulation of warfare as a legal construct emerged in the nineteenth century. However, the comprehensive codification of IHL did not occur until the latter half of the twentieth century.

Primarily, classical International Humanitarian Law (IHL) encompasses the Law of The Hague, encapsulated in the Hague Conventions of 1899 and 1907. These conventions delineate the rights and obligations of belligerents during military operations, setting constraints on the permissible methods of harming the enemy. Additionally, classical IHL mainly comprises the Four Geneva Conventions of 1949, strategically crafted to protect both military personnel who have ceased active participation in a conflict and individuals not directly engaged in hostilities, such as civilians (Filipa Vrdoljak, 2011).

Notably, the drafters of IHL did not contemplate its application to cyber operations, where the definitions and significance of expressions 'attack' and 'military objects' etc. have evolved significantly (Additional Protocol, 1977) with the evolution of technology. While the earliest incident of Morris Worm affected thousands of computers in 1988 (Kelty, 2011), the historic cyber-attack, which had the potential to result in severe devastation and harm, took place when a 14-year-old named James successfully infiltrated the computer system that managed the operations of the floodgates at Roosevelt Dam in Arizona (Spafford, 1989, p. 455). It was reported that the real-world damage would have been caused by the release of billions of gallons of water downstream ("Cyber-Attacks by Al Qaeda Feared - The Washington Post", n.d.). Any malicious endeavour that seeks to acquire, disrupt, withhold, impair, or obliterate the resources of an information system or the information it contains ("Cyber Attack - Glossary | CSRC", n.d.). Cyber-attacks exhibit diverse natures and attributions, and the continuous progress in technology has amplified the dependence on computer systems as well as the looming threats they pose to the

present world. While the Geneva Conventions and their Additional Protocols define means and methods for conventional warfare, they do not define the armed attack and use of force in the context of cyberwarfare. This research addresses the modern question of whether the IHL caters to the present threats or necessitates expansions. Whether pre-existing notions of 'use of force', 'civilian objects', and 'armed attack' aid the application of IHL? Does NATO's sponsored 'Tallinn Manual offer an effective regime for eminent legal challenges?

Presently, cyber-attacks pose more threats to the security of the country than conventional methods of attack. Therefore, this paper aims to look at the development of IHL in the context of cyberwarfare and analyse the limitations imposed by the conventional definitions.

Literature Review

Fundamentally, the compelling aspiration to safeguard human lives from the unmitigated horrors of war prompted the enactment of the Geneva Conventions and subsequent Protocols, aiming to regulate the conduct of armed conflicts ("Human Rights in War", n.d.). The global civilian infrastructure, spanning a diverse array of sectors, is interconnected through the Internet (Tortonesi, Wrona, & Suri, 2019).

The issue of applying IHL to cyberwarfare has been a subject of scholarly debate over the years. The literature review comprises various sources, each providing a unique perspective on the topic. According to Osinga (2011), the classical IHL includes the four Geneva Conventions of 1949 and their two additional protocols of 1977 (Osinga & Roorda, 2016). These conventions are designed to protect people who do not directly participate in hostilities and to reduce the effects of armed conflicts. However, it is unclear whether these conventions are sufficient to address cyberwarfare issues (Harrison Dinniss, 2012). Some jurists believe that data and systems can be identified as protected in cyber conflicts under the Geneva Conventions. The article concludes that applying existing IHL to cyber-conflict is still an open question (Sutherland, Xynos, Jones, & Blyth, 2015, p. 35). Durbin suggests that the current legal framework for IHL is inadequate in addressing the unique challenges that cyber operations present. There is a need for a more

refined approach to using IHL in the context of cyberwarfare, which involves creating a specific set of legal principles for both the justification and the manner of conducting cyber operations. It has been argued that developing such an approach will require an enhanced understanding of the character of cyber operations and their influence on the principles of distinction, proportionality, and military necessity (Jordan, 2021).

It has already been examined how IHL regulates cyber operations in the situation of international armed conflicts, specifically regarding the qualification of cyber operations as 'attack' and the applicability of rules that restrict the conduct of hostilities (Horowitz, 2020). Amanda has argued for a narrow interpretation of the concept of an attack, which would limit the applicability of most substantive provisions that protect civilians and civilian objects under Additional Protocol I (Bills, 2017). Marco Roscini has discussed the emerging legal landscape for cybersecurity and IHL alongside the challenges in applying traditional legal concepts to this new domain. It has been argued that the existing legal framework is inadequate to address the challenges posed by cyber operations in armed conflict and proposes some solutions to them (Roscini, 2018). Mačák maintains that the reluctance of states to bind themselves to certain interpretations of legal principles has driven international law on cybersecurity to a downfall that has created a power vacuum (Mačák, 2016). Resultantly, non-state-driven initiatives establishing norms such as Microsoft's cyber norms proposal and the 'Tallinn Manual' project have emerged to fill this void. It has been stated that states are posed with ample opportunity to reclaim a central position in law-making and develop new legal norms and standards for cybersecurity (Mačák, 2016, p. 134). It has been reiterated over the past years to develop a universal notion of cyberspace because of the persistent, significant vulnerabilities and several threats in global communications.

Dörmann presents another viewpoint by arguing that the legal framework prevailing currently is sufficient to cover cyber operations, but there is a necessity for additional guidance to tackle specific issues. The author highlights the significance of upholding the principles of IHL in cyberspace to minimize the adverse impact on non-combatants and civilians (Dörmann., 2018). Schmitt has taken a similar approach by exploring the role of International Law

in cyberspace by analysing Koh's speech and 'Tallinn Manual 2.0. He also affirms that international law spreads over cyberspace, but new norms and principles are needed to address the unique challenges posed by cyberspace (Schmitt, 2017). The need for states to work together to develop international law principles to address the challenges surrounding cyber operations, such as attribution and response to cyber-attacks, has also been emphasised.

Despite the abundance of literature on the application of IHL to cyberwarfare, several areas in research require attention. One significant gap is the absence of clear and universally accepted definitions in the cyber arena, which creates confusion in determining the suitability of existing IHL conventions for cyber operations. Moreover, there is a need to explore the part of non-state actors in developing legal norms and principles for cyberspace (Koloßa, 2019).

Another gap is the lack of clarity regarding interpreting the concept of 'attack' in the cyber operations realm, which limits the application of substantive provisions of IHL protecting civilians and their objects. Furthermore, there is a need for more specific guidance on the conduct of cyber operations, particularly on the principles of distinction, proportionality, and military necessity. There is a dearth of a universally accepted and codified international convention or treaty that explicitly governs cyberwarfare. Existing laws and norms that apply to cyber operations, such as IHL and the United Nations (hereinafter UN) Charter, are not explicitly tailored to cyberspace's unique characteristics and challenges. A universally agreed-upon convention could provide probable solutions and guidance on the legal framework for cyberwarfare. Finally, states need to work together to develop international law principles to deal with the challenges unique to cyber operations, including attribution and response to cyber-attacks.

Research Methodology

This paper employs a qualitative and doctrinal research method to analyse the relevant sources of international law, specifically IHL, and literature about cyberwarfare. The scholarship relies on primary sources such as treaties, state practice, customary international law, and judicial decisions to identify the existing principles and rules of IHL. Secondary sources such as books,

articles, reports, and commentaries have also been used to critically examine the challenges and gaps in applying IHL to cyberwarfare and to evaluate the proposals and recommendations for developing new laws (*lex ferenda*).

The data collection entailed a systematic review of primary legal documents and scholarly works pertaining to IHL and cyberwarfare. The analysis included a thorough examination of these sources, identifying recurring themes, contradictions, and areas of consensus. The choice of a qualitative and doctrinal research approach was inspired by the need for an in-depth exploration of legal principles and their application to cyberwarfare.

The paper also discusses the Tallinn Manual as a significant contribution to interpreting and clarifying international law in cyberspace. The objective of this paper is to provide a comprehensive and balanced assessment of the current State of IHL and its adequacy for regulating cyberwarfare.

The multidisciplinary approach integrates legal analysis with insights from political science, cybersecurity, and ethics, providing a holistic understanding of the subject matter. Acknowledging the limitations of this methodology, the paper suggests areas for further research and invites scholarly discourse on refining and expanding the research framework.

Cyberspace and Warfare

Cyberspace is a new dimension of warfare that is most vulnerable to exploitation and abuse by individuals, states, and other non-state entities alike. The rapid increase in the frequency of cyber-attacks has led to a change in how warfare is conducted (Panwar, 2018). The specific cyber activities entailing initial attacks are subject to debate; however, it is worth noting that a series of cyberattacks that occurred within the past two decades have contributed to our understanding of the urgency of the matter. A series of coordinated cyberattacks directed towards Estonian governmental, financial, and media infrastructure systems in April 2007 introduced a novel domain prone to damage. These attacks are the very first large-scale cyberwarfare offensives against a nation-state (Herzog, 2011).

In 2010, Stuxnet, a malware program affected Iran's Natanz nuclear facility by infiltrating the industrial systems controlling

facility (Broeders et al. 2022). It caused disruptions in approximately 1,000 centrifuges used for uranium enrichment (Singer & Friedman, 2014, p. 116). It is widely believed that the United States and Israel jointly developed it to sabotage the Nuclear Program and was specifically designed to target centrifuges while exploiting unknown software vulnerabilities (Langner, 2013). The worm's deployment was a significant moment in cyberwarfare, as it marked one of the first instances of a physical damage to industrial equipment by cyber weapon. This event revealed the potential usage of cyber-attacks as a tool to conduct warfare and raised apprehensions about the security of critical infrastructure systems around the globe (Fruhlinger, 2022). It is said that cyber war only kills a bunch of baby electrons, whereas the Stuxnet showed the world that cyber war could potentially kill real babies (Rosenzweig, 2013).

In May 2017, a widespread cyber-attack targeted numerous civilian infrastructures in more than one hundred countries, using ransomware called WannaCry (Ryan, 2021, p. 70). The attack originated using a vulnerability in the Microsoft Windows operating system, for which a patch was released two months before the attack. The attackers demanded payment in Bitcoin in exchange for the decryption of the affected files, and it was estimated that the attack caused billions of dollars in damages (Farringer, 2016). The undeniable capacity of cyberattacks to inflict significant harm is a reality today, with cyberwarfare now established as a prominent feature of modern-day conflicts. Therefore, it is necessary to analyse the factors that are unique to cyberattacks.

Peculiar Challenges

The cyber atmosphere is home to a plethora of complicated fragments that hinder the applicability of the law. Anonymity is the foremost challenge posed in the cyber landscape because the initial susceptibility of the web lies in identifying malicious actors, as it is easy to conduct harmful activities from a remote location, concealing true identity behind a fictitious or constantly changing digital persona (Andress & Winterfeld, 2013). The sheer expansiveness of the internet further complicates the detection of such individuals. Secondly, it is tough to distinguish between various types of cyberactivity. Due to the uniformity of 1s and 0s in

the logic layer, it becomes difficult to differentiate between ostensibly similar-looking espionage and a full-scale cyberattack (Madubuike-Ekwe, 2021). The ubiquity of the internet has created enhanced imbalances of power. While in the physical world, only nation-states and large-scale insurgents can compete effectively in cyberspace, even small non-state actors can challenge nation-states (Perkovich & Levite, 2017). Individuals with complex relationships can transmit information worldwide, which can result in massive malicious activities. Conclusively, the internet is a borderless domain where information travels globally at a breakneck pace, without any limitations or borders. This feature creates a vacuum for activities to be conducted across national boundaries, which is impossible to achieve in the physical world. Although some countries have attempted to erect boundaries on the internet, it remains a globalised domain (Shirky, 2011). It is evident that the regulation of a substantially different environment from the one in which we currently live and interact cannot be accomplished using traditional customs that emerged a century ago.

Lex Lata in CyberSphere

Use of Force under International Law

The Use of Force is prohibited internationally under the United Nations Charter. Article 2(4) of the United Nation's Charter states that:

> "All Members shall refrain in their international relations from the threat or use of force against the territorial sovereignty or political independence of any state, or in any other manner inconsistent with the Purposes of the United Nation".

It is a predominantly significant article that international legal experts have labelled as "the cornerstone of peace in the Charter" and "the heart of the United Nations Charter." (Yoo, 2004, p. 781).

The difference between war and other kinds of use of force has been eliminated by Article 2(4) of the UN Charter (Yoo, 2004). Every unauthorised use of force or threat of force, regardless of the justification, is prohibited. Not just in times of war, but generally, force is forbidden (Sukin & Weiner, 2021). It is crucial to ascertain

whether there has been a use of force because if there has not, the victim state may have fewer options than in the case where there has been. There is not a universally accepted definition or standard for 'use of force' or 'threat of use of force'. In the Black Law Dictionary, 'force' is defined as "power, violence, or pressure against a person or thing" (Black & Nolan, 1990, p. 644). This connotes that the force may include not only armed force but also economic and political coercion. It is pertinent to note here that these kinds of coercion do not fall under the ambit of prohibition in Article 2(4). As a result of an in-depth analysis of the contextual reference of the norm within the UN Charter, it can be inferred that 'force', in the meaning of Article 2(4), connotes 'armed force' only. The structure and language used in The Friendly Relations Declaration imply that Article 2(4) ought to be interpreted with a restricted understanding of force, particularly concerning military or armed force (Butchard, 2018, p. 240).

Use of Force in Cyberwarfare

The question that emerges next is when a cyber operation crosses the threshold to be categorised as the use of armed force, and this constitutes the central theme of this portion of the paper. Black's Law Dictionary defines 'armed' as "equipped with a weapon" or "involving the use of a weapon" (Black & Nolan, 1990, p. 108). A weapon is an instrument used or designed to be used to injure or kill someone. Roscini (2018) draws attention to the fact that almost every item can be used as a weapon if it is being held with hostile intent (p. 463). When referring to malicious code as 'weaponised', it suggests that the code possesses attributes designed to function as a means of causing disturbance or harm, much like a kinetic weapon. In the Advisory Opinion regarding the Legality of Nuclear Weapons, the International Court of Justice (ICJ) affirmed that Articles 2(4), 51, and 41 are not specific to particular armaments. They are applicable to any employment of force, irrespective of the weaponry utilised (*Legality of the Use by a State of Nuclear Weapons in Armed Conflict*, 1996).

It can be inferred that the method of carrying out a cyber operation is inconsequential in determining whether it constitutes the use of force. If such force is present, the use of cyber technology does not alter its classification. The Court's previous statements

indicate that weaponry need not be inherently explosive or created solely for destructive purposes (*Legality of the Threat or Use of Nuclear Weapons*, 1996, para. 35). Biological and chemical weapons, which are non-kinetic and have both peaceful and harmful applications, would still tantamount to use of force by the affected State (*Legality of the Threat or Use of Nuclear Weapons*, 1996, p. 96). Furthermore, the ICJ implicitly acknowledged that non-kinetic force could result in a violation of Article 2(4) when it labelled the United States arming and training of the members of guerrilla forces as a use or threat of force against Nicaragua (*Military and Paramilitary Activities in and against Nicaragua*, 1984, para. 242).

Classification of Cyber Operation

Three main approaches exist to classify cyber operations under Article 2(4). However, there is an ongoing debate about their applicability when compared to the conventional idea of the use of force. One of the approaches is the instrument-based approach; it refers to the means and methods used to commit an act, such as weapons (McGavran, 2009, p. 269). This approach helps differentiate armed forces from economic and political coercion (Tsagourias, 2012). However, this approach does not align well with cyber operations because of its emphasis on physical means. According to this approach, a faulty code cannot constitute the use of force regardless of its consequences. A literal analysis of the UN Charter indicates that a new weapon is similar to a conventional weapon, the chances are higher for it to constitute use of force or an armed attack (Tsagourias, 2012).

In the second approach, which is target-based, it is argued that the cyber-attack must target critical national infrastructure (NCI) for it to constitute the use of force (Tsagourias, 2012, p. 236). If the attack is directed against NCI, then the effects become meaningless. There are two problems, however. First, the attack's effects do not seem to matter as long as it targets NCI. However, this approach is too broad, and a cyber operation that only causes inconvenience or aims to collect information qualifies to be a use of force. Secondly, a universal definition of critical national infrastructure does not exist, which may cause variance in the practices in different countries (Tsagourias, 2012).

While the instrument-based and target-based approaches may provide a straight forward way to categorise cyber incidents, they are too limited to account for the intricacy of cyber operations and may also be too inclusive. In contrast, the effect-based approach has garnered more support and acknowledgement due to the fact that the primary concern of states is what the cyber operation results in rather than the type of weapon or target involved (Nguyen, 2013; Simmons, 2014). The objective of the effect-based approach is to recognize cyber operations which are similar to other kinetic or non-kinetic actions which are seen as the use of force by the international community (Kuru, 2017; National Research Council, 2010). However, this approach fails to consider how modern societies rely on a closely knitted network of computers. This facilitates the vulnerability of physical infrastructures incapacitated without necessarily harming them physically (Tsagourias, 2012, p. 239).

'Scale and effects' as a phrase are derived from the Nicaragua Judgment, where the court distinguished between 'mere frontier incident' and an armed attack (*Military and Paramilitary Activities in and against Nicaragua*, 1984, para. 195). Rule 11 of the Tallinn Manual stipulates that a cyber operation may be considered as a use of force when its scale and effects are comparable to non-cyber operations rising to the level of a use of force (Eaton, 2021, p. 710).

Scale refers to the size or scope of a cyber-attack. Scale can be measured in terms of the number of systems affected, the geographic reach of the attack, or the amount of data compromised. A cyber-attack on a small scale may only affect a single computer or a small group of computers, while a large-scale attack can affect thousands or even millions of systems. The scale of an attack can help to determine the severity of the threat it poses (Lotrionte, 2018).

Effects refer to the impact of a cyber-attack. Effects can include financial losses, damage to reputation, or disruption of critical infrastructure. The effects of a cyber-attack can be immediate, for instance, a Denial of Service (DoS) attack that takes a website offline, or they can be long-term, such as a data breach that compromises sensitive information. The effects of an attack can help determine the potential harm to individuals or organizations. Another stance taken in the realm of self-defence and the problem of attribution is defined as:

> "An act or the beginning of a series of acts of an armed force of considerable magnitude and intensity (i.e., scale)

> which have as their consequences (i.e. effects) the infliction of substantial destruction upon important elements of the target State namely, upon its people, economic and security infrastructure, destruction of aspects of its governmental authority, i.e. its political independence, as well as damage to, or deprivation of its physical element namely, its territory" (Tsagourias, 2012, p. 231).

The destruction that is often intended by a cyber-attack will not usually be achieved by damaging or disrupting the computer systems directly but through the indirect effects of such attacks. Those indirect effects start to show on computer systems that are controlled by the computer system at which the attack is intended (Nguyen, 2013). There can be multiple effects of a cyber-attack, but the notion that armed force is such a force that results in instant damage or injuries should be reviewed in the context of cyberwarfare.

In addition to the Tallinn Manual, which helps determine whether a cyber-attack would amount to the 'Use of Force', there is a non-exhaustive list of eight criteria which were developed by IGE. The criteria include severity, immediacy, directness, invasiveness, measurability, military character, state involvement and presumptive legitimacy (Schmitt, 2022).

It can be deduced that a cyber-attack which results in loss of life or injury to persons and damage to physical property will be considered as a violation of the prohibition on the use of force under Article 2(4) of the UN Charter. However, there has never been a cyber-attack which had caused such consequences except for the explosion that affected Soviet Gas Pipeline in Siberia allegedly caused by the US CIA (Bronk, 2014; Rid & McBurney, 2012).

Armed Attack in Cyberwarfare

The term 'attacks' has been defined in Article 49(1) of Additional Protocol 1 (hereinafter' AP1) (ICRC, 1977) which reflects customary international law as act[s] of violence against the opponent, may it be in offence or in defence (Dörmann, 2004, p. 3). Whereas the expression 'violence' connotes physical act or behaviour involving physical force (Melzer N., 2008). The literal definition of an 'armed attack' would be any attack where there is a

use of weapon. Although the cyber operations do not employ traditional weapons, they still require infrastructure which makes up the cyberspace, thus potentially qualifying it as a weapon. About what makes anything a weapon, Karl Zemanek (2012) in 'Armed Attack' mentions that:

> "[I]t is neither the designation of a device, nor its normal use, which make it a weapon, but the intent which it is used and the effect. The use of any device or number of devices, which results in a considerable loss of life and/or extensive destruction of property must therefore be deemed to fulfil the conditions of an 'armed attack"(p. 600).

This was further reaffirmed by the Security Council after the 9/11 attacks when planes which collided with the towers were recognised as weapons (UNSC, 2001). Moreover, Rule 13 of the Tallinn Manual allows the State to practice its right of self-defence in conflicts where the cyber operation increases to the level of an armed attack depending upon its effects and scale (Schmitt, 2013, p. 53).

Therefore, it can be inferred that an attack can be referred as an armed attack even if there are no conventional weapons being used. But as mentioned above, a weapon can be any device which used with the intention of causing substantive loss of life or damage to the property (*Oil Platforms (Islamic Republic of Iran v. United States of America)*, 2003, p. 191). With the everyday development of technology, an attack on cyberspace has the tendency to cause destruction, even loss of life, and thus, any cyberattack can become an armed attack.

Civilian Objects and Military Objectives in Cyber Realm

Objects that are not Military objectives are civilian objects and are defined in Article 52(2) of Additional Protocol I (API) (1977), and the scope of military objectives is restricted to those entities that provide a valuable input to military operations by their location, nature, purpose, or use, and by capturing, partially destructing or neutralising it would provide a clear military benefit.

According to Article 52(3) of API, an object that is used for civilian purposes naturally will be presumed not to be used for military action, unless proven otherwise. However, most cyber

infrastructures are dual-use, helping both military and civilian roles (Lahmann, 2012). Thus, if such infrastructure is used to make an effective advantage to military action in future, it will lose its civilian status and become a legitimate military target (Henckaerts, 2009). This advances the issue that all civilian data centres and cyber infrastructures around the world may be considered as legitimate military objectives, because military data stored within them can be subject to military use in future. Tallinn Manual 2.0 discusses this issue.

Tallinn Manual

The Tallinn Manuals on the International Law Applicable to Cyberwarfare are the most exhaustive and detailed study to date on the applicability of contemporary international law to cyberwarfare. If it has not already, it may very well succeed in the authors' goal of joining the ranks of the Manual on International Law Applicable to Air and Missile Warfare and the San Remo Manual on International Law Applicable to Armed Conflicts at Sea as one of the authoritative (though non-binding) manuals outlining how international law is applied to specific forms of warfare, frequently cited and count on by civilian and military practitioners worldwide (Henderson, 2010).

The frequency of these cyber-events and the dangers they pose to both individual states and the global society as a whole have compelled governments and multinational corporations (Chrapavy, 2016; Clapper, 2015) to take cognizance and seek explanations. The North Atlantic Treaty Organization (NATO) is one of the international organizations, and its Cooperative Cyber Defence Centre of Excellence (CCDCOE) is one of them. CCDCOE, which is based in Tallinn, Estonia, helped create the first Tallinn Manual on the International Law Relevant to Cyberwarfare (Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations, 2017). It is a useful tool for politicians, lawyers, and military experts to comprehend the legal framework guiding cyber operations.

Tallinn Manual 1.0

There are two sections in the Manual. The first section discusses how international law, including the concepts of sovereignty, jurisdiction, and state accountability, might be applied

to cyberwarfare. The definition of cyberwarfare, the use of force, and the targeting of people and things are only a few of the specific topics covered in the Manual's second section (Schmitt, 2013). A key contribution to our understanding of the legal framework governing cyberwarfare is the Tallinn Manual 1.0. It is a useful tool for decision-makers, military specialists, and attorneys who wish to comprehend the laws relating to the use of computers and the internet in combat.

Tallinn Manual 2.0

The Tallinn Manual 2.0 is a thorough manual that focuses on how international law should be used in cyber operations. The Tallinn Manual 1.0 has been updated and enlarged in this version. Experts in international law analysed and interpreted the pre-existing legal framework for cyber activities under international law as they prepared the guidebook. The manual addresses a broad range of issues relating to cyber operations, such as the concepts of the use of force and cyber espionage. It also discusses the definition of cyber operations, the legal standing of cyber players, and how such actions during armed conflict should be governed by IHL. There are four sections to the Manual. Cyberspace and basic international law are covered in Part I. Cyberspace and specialised international legal systems are covered in Part II. Part III, deals with international peace, security, and cyber operations. Part IV deals with the law of cyber activities (Schmitt, 2013).

The CCDCOE operates independently from NATO's overarching command structure, even though NATO accredits each operational centre. In order to participate in a centre's operations, member nations are required to sign a memorandum of understanding (Jančárková & Toompere, n.d.). The Tallinn Manual is thus comparable to other legal guides controlling marine and aerial combat in that it is an excellent but ultimately advisory legal document (Anderson, Tallinn Manual). The Tallinn Manual promises to have an impact on future legal evolution despite its non-binding nature. It looks at cyber-attacks from the standpoint of IHL, concentrating on how cyber-attacks are subject to jus ad bellum and jus in Bello. The Manual does not concentrate on the traditional framework of electronic warfare or problems like intellectual property theft, espionage, or other cyber security issues that do not

call for an investigation under IHL, particularly under jus ad bellum (Kilovaty, 2014).

The international group of experts known as Tallinn 2.0 had diversity in terms of its composition, with members originating from Thailand, Japan, China, and Belarus, and possessing expertise in various fundamental areas such as human rights, space law, and international telecommunications law (Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations, 2017). This diversity was strategically planned to counteract the criticism. Along with other nations and organizations, the International Committee of the Red Cross (ICRC) was also invited to take part by sending observers to both groups (Crawford, 2021). The project didn't result in a piece of legislation or a manual that could be used as such. As stated in the introduction;

> "Ultimately, Tallinn Manual 2.0 must be understood only as an expression of the opinions of the two International Groups of Experts as to the state of the law" (Jensen, 2017, p. 738).

This Manual takes into account the legislation as it was in June 2016, when the International Groups of Experts first adopted the Manual. It is true that it is not a manual, does not represent progressive development of the law, and is apolitical in nature. In other words, the *lex lata* is meant to be objectively restated in the Tallinn Manual 2.0 (Crawford, 2021; Jensen, 2017).

Both manuals' content was created using very different methods, but they both used the same methods to bring the material to a close. Rules, which are written in large, black characters and appear in both manuals, demand unanimous agreement from all experts, or consensus. Each rule is followed with a very lengthy discussion that is written in regular font to set it apart from the rule (Jensen, 2017). The commentary defines and provides justifications for the rules, and specifies on how to apply the rules, scenarios, and examples. Most crucially, it also addresses expert disagreement. For instance, the experts concurred that a state's citizens must be subject to prescriptive nationality jurisdiction even while they are abroad, but they couldn't agree on whether the data pertaining to that person was subject to the extraterritorial enforcement authority of the national State. According to Rule 10, which all of the Experts accepted;

> "A State may exercise extraterritorial prescriptive jurisdiction relating to cyber activities: (a) conducted by its nationals; ..." (Tallinn Manual 2.0, 2017 Rule 10(a), p. 60).

However, the commentary to a later rule notes that only a few experts distinguished between prescriptive jurisdiction over a country's citizens' online activities and the jurisdiction over the data produced during those activities (Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations, 2017, p. 63). They believed that the State's control over data was frequently unrelated to its control over the online behaviours of its citizenry. Thus, all Experts concurred that the State in which the data is located will continue to have complete control over the data.

When the Experts completed writing Tallinn 2.0, the Dutch government organised a series of meetings with states so that they could assess and provide feedback on the Manual's content before it was finalised. Over fifty countries, including all of the permanent members of the Security Council, participated in these conferences (Schmitt, 2013). This feedback provided priceless insights into how governments saw the application of international law with regard to cyber activities, even though it was not necessarily incorporated in the Manual since it only represents the Experts' judgments (Jensen, 2017). In addition, peer reviewers were consulted over certain of the Manual's sections. The Experts were then given all outside input, including that from states and peers, for review as the draught rules and comments were being put together. This extensive process, in relation to Tallinn 2.0 specifically, enabled the consideration and eventual approval of a considerably wider range of opinions and talents than are gathered in any other single source. The Tallinn Manuals would provide a distinctive and comprehensive declaration of the international law regulating cyber operations (Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations, 2017).

The Tallinn Manual does address several legal gaps in the existing laws governing cyberwarfare. It specifies the laws governing the use of force in cyberspace and offers guidance on topics including the use of cyber espionage and the defence of critical infrastructure (Madubuike-Ekwe, 2021; Schmitt, 2017). The Tallinn Manual does not, however, provide a comprehensive response to all the legal questions posed by cyberwarfare. As cyber dangers and attacks continue to evolve, there will likely be ongoing

discussions about how international law should be changed to reflect these challenges.

Limitations of the Tallinn Manual in Addressing Legal Issues in Cyberwarfare

The Tallinn Manual successfully provides a framework for understanding how the present international law is applied to cyber operations, including issues like the use of force, attribution, and state responsibility. However, legal experts have debated that the Manual has restrictions and may not be enough to address a range of trials modelled by cyberwarfare.

For instance, Jack Goldsmith (2017), a professor of law at Harvard Law School, warned that the Tallinn Manual might be overly broad in its use of international law in cyber operations. Goldsmith maintains that the Manual's stance on self-defence may be challenging as it may sanction states to take anticipatory cyber-attacks against other states under certain circumstances. Goldsmith also suggests that the Manual might have failed to counter the issue of non-state actors and their vital part in cyber operations (Jack Goldsmith & Alex Loomis, 2021; Loomis, 2022).

Additionally, some legal specialists have also concluded that the Tallinn Manual may not be all-inclusive to cover all evolving legal issues in cyberwarfare. For instance, some may rightly argue that Manual does not disclose the issue of cyber espionage, which is admittedly becoming a genuine problem for governments around the world (Loomis, 2022).

States can contribute to clarifying the regulations regarding cyber operations and encourage greater respect for international law in cyberspace by codifying the Tallinn Manual's principles into a convention. Building agreements and fostering cooperation on cyber concerns can also be facilitated by involving states in the process.

Addressing Legal Loopholes in Cyberwarfare by Tallinn Manual

The Tallinn Manual is a well-written work that deserves to be recognised internationally, but several issues with its contents will perplex legal experts and politicians. The instruction is not

empirical, to start. The Tallinn Manual differs from a common law court ruling in that it only contains the Experts' conclusions. To provide an analogy, it could be said that the Manual is a compilation of 95 case holdings with barely adequate to extremely scant justifications. It appears as though the Manual exists in some vacuum ephemera unrelated to policy considerations, current trends, and historical events because there is no comparison of opposing opinions and no examination of the facts. Second, the Manual hardly ever resolves disputed matters and when it does, summaries of the expert panel's opinions are presented. However, for academics and researchers, these inclusions serve no useful purpose.

A study of international law that is relevant to cyber activities, particularly cyberwarfare, is found in the Tallinn Manual. Tallinn 2.0 is intended to serve as the starting point for a longer and more significant conversation (Jensen, 2017). This resource serves as the ideal starting point for discussions concerning the international legal framework governing cyber operations due to its thoroughness, meticulous analysis and findings, and integration of state and peer viewpoints. Even among the Experts who created the Tallinn Manuals, there are still a lot of points of contention and confusion (Jensen, 2017). Additionally, there are numerous instances where states have kept their public statements and actions about cyber operations to themselves (Moynihan, 2019). Insight and comprehension are desperately needed in this still-evolving field of law in order to develop fresh solutions to pressing issues. However, Tallinn 2.0 is to be considered as the first step in the law on cyber operations until states define precisely where the law is headed.

Conclusion and Recommendations: Rethinking IHL for Cyberwarfare

The robust development of technology has brought about a new era of warfare that challenges the applicability and effectiveness of classical IHL. Cyber operations have demonstrated their potential to disrupt essential civilian infrastructure, posing significant threats to global security. This research paper has examined the relationship between IHL and cyberwarfare, evaluating the applicability and limitations of current legal concepts and frameworks.

The Tallinn Manual has significantly contributed to the humanization of cyber conflicts by providing a framework for understanding how existing international law applies to cyber operations. However, the Manual has certain limitations that require further attention. More representation from states and including dissenting opinions would enhance Manual's usefulness for those wishing to follow the legal development in this novel area. The rapidly evolving nature of cyberwarfare demands a global convention that can set clear rules and regulations to govern cyber operations. Such a convention would promote adherence to international law in cyberspace and encourage collaboration between states in addressing cyber threats. Including states in developing this convention would facilitate agreement and cooperation on critical cyber issues. Therefore, there is a dire need to emphasize legal scholarship pinpointing the shortcomings of IHL and proposing possible solutions to the most pertinent cyber legal issues. We recommend that states prioritize legal and policy development efforts on cyberwarfare to strengthen the applicability of IHL in the contemporary world. The international community must work together to foster greater cooperation, agreement, and respect for international law in cyberspace to ensure a secure and peaceful future.

References

Andress, J., & Winterfeld, S. (2013). Cyber Warfare: Techniques, Tactics and Tools for Security Practitioners. Elsevier.

Bills, A. (2017). Cyber Warfare and Jus in Bello – The Regulation of Cyber 'Attacks' under International Humanitarian Law (Lund University). Lund University. Retrieved from https: //lup.lub.lu.se/luur/download?func=downloadFile&recordOId=8907825&fileOId=8916280

Black, H. C., & Nolan, J. R. (1990). *Black's law dictionary: Definitions of the terms and phrases of American and English jurisprudence, ancient and modern* (6th ed). St. Paul, Minn: West Pub. Co.

Broeders, D., De Busser, E., Cristiano, F., & Tropina, T. (2022). Revisiting past cyber operations in light of new cyber norms and interpretations of international law: Inching towards lines in the sand? *Journal of Cyber Policy*, *7*(1), 97–135. https://doi.org/10.1080/23738871.2022.2041061

Bronk, C. (2014). Hacks on gas: energy, cybersecurity, and u.s. defense.

Butchard, P. M. (2018). Back to San Francisco: Explaining the Inherent Contradictions of Article 2(4) of the UN Charter. *Journal of Conflict and Security Law*, *23*(2), 229–267. https://doi.org/10.1093/jcsl/kry010

Cheng, L. D. (2019). The 2017 WannaCry ransomware attack: A comprehensive analysis. *Journal of Information Privacy and Security,*. doi:10.1080/15536548.2018.1502576

CSRC. (n.d.). Computer Security Resource Center. Retrieved from Information Technology Laboratory: https://csrc.nist.gov/glossary/term/cyber_attack

Chrapavy, P. (2016). Cybersecurity risks: Are they inflated? *Salus Journal*, *4*(2),19-31.

Clapper, J. R. (2015). US Intelligence Community [Statement for the Record]. US Senate: Senate Armed Services Committee.

Crawford, E. (2021). *Non-Binding Instruments in International Humanitarian Law: State-Directed Non-Binding Instruments, and Non-Binding Instruments Created by Expert Groups. In E. Crawford, Non-Binding Norms in International Humanitarian Law*, 84–129. Oxford University Press. https://doi.org/10.1093/oso/9780198819851.003.0005

Cyber Attack—Glossary | CSRC. (n.d.). Retrieved January 9, 2024, from https://csrc.nist.gov/glossary/term/cyber_attack

Cyber-Attacks by Al Qaeda Feared—The Washington Post. (n.d.). Retrieved January 9, 2024, from https://www.

washingtonpost.com/archive/politics/2002/06/27/cyber-attacks-by-al-qaeda-feared/5d9d6b05-fe79-432f-8245-7c8e9bb45813/

Dörmann, K. (2004, November 19). Applicability of the Additional Protocols to Computer Network Attacks—ICRC. Presented at the International Expert Conference on Computer Network Attacks and the Applicability of International Humanitarian Law, Stockholm. Stockholm. Retrieved from https://www.icrc.org/en/doc/resources/documents/misc/68lg92.htm

Dörmann, K. (2005). Applicability of the Additional Protocols to Computer Network Attacks. International Review of the Red Cross, 87(859). Retrieved from https://www.icrc.org/en/doc/resources/documents/misc/68lg92.htm

Dörmann., K. (2018). Applicability of international humanitarian law to cyber operations during armed conflict. *International Law Studies, 94*, 1-25.

Durbin, A. (2016). Cyber warfare and the applicability of international humanitarian law. *Journal of Conflict & Security Law, 21*(2), 185-208.

Eaton, T. (2021). Self-Defense to Cyber Force: Combatting the Notion of 'Scale And Effect'.

Farringer, D. R. (2016). Send Us the Bitcoin or Patients Will Die: Addressing the Risks of Ransomware Attacks on Hospitals. Seattle University Law Review, 40, 937.

Fruhlinger, J. (2022, August 31). Stuxnet explained: The first known cyberweapon. CSO Online Retrieved from https://www.csoonline.com/article/3218104/stuxnet-explained-the-first-known-cyberweapon.html

Filipa Vrdoljak, A. (2011). Cultural Heritage in Human Rights and Humanitarian Law. In O. Ben-Naftali (Ed.), International Humanitarian Law and International Human Rights Law (1st

ed., 250–302. Oxford University PressOxford. https://doi.org/10.1093/acprof:oso/9780191001604.003.0007

Fruhlinger, J. (2022, August 31). Stuxnet explained: The first known cyberweapon | CSO Online. Retrieved January 9, 2024, from https://www.csoonline.com/article/562691/stuxnet-explained-the-first-known-cyberweapon.html

Gellman, B. (. (2002). Cyber-attacks by Al Qaeda feared. Washington DC: Washington Post. washingtonpost.com/archive/politics/2002/06/27/cyber-attacks-by-al-qaeda-feared/5d9d6b05-fe79-432f-8245-7c8e9bb45813/

Harrison Dinniss, H. (2012). *Cyberwarfare and the Laws of War (1st ed.). Cambridge University* Press. https://doi.org/10.1017/CBO9780511894527

Henderson, I. (2010). Manual on International Law Applicable to Air and Missile Warfare: A Review. Retrieved from https://papers.ssrn.com/abstract=2200060

Herzog, S. (2011). Revisiting the Estonian Cyber Attacks: Digital Threats and Multinational Responses. *Journal of Strategic Security, 4*(2), 49–60.

Harknett, R. J. (2016). Securing the internet of things: A proposed framework. *Strategic Studies Quarterly*, *10*(4), 85-106.

Henckaerts, J. M. (2009). *Volume I: rules. in J.-M. Henckaerts, customary international humanitarian law*. Cambridge University Press.

Herzog, S. (2011). Revisiting the Estonian cyber attacks: Digital threats and multinational responses. *Journal of Strategic Security*, *4*(2), 49-60. Retrieved from https://doi.org/10.5038/1944-0472.4.2.3

Horowitz, J. (2020). Cyber Operations under International Humanitarian Law: Perspectives from the ICRC | ASIL. Retrieved from https://www.asil.org/insights/volume/24

/issue/11/cyber-operations-under-international-humanitarian-law-perspectives-icrc

Human Rights in War: On the Entangled Foundations - ProQuest. (n.d.). Retrieved January 9, 2024, from https://www.proquest.com/docview/2120722223?sourcetype=Scholarly%20Journals

Iain Sutherland, K. X. (2015). The Geneva Conventions and Cyber-Warfare. *The RUSI Journal, 160*(4), 30-39. doi:10.1080/03071847.2015.1079044

ICRC, A. A. (1977). Additional Protocol 1 to the Geneva Conventions. Geneva: International Committee of Red Cross.

Jack Goldsmith & Alex Loomis. (2021, April 30). "Defend Forward" and Sovereignty. Retrieved January 10, 2024, from Default website: https://www.lawfaremedia.org/article/defend-forward-and-sovereignty

Jordan, W. J. (2021). Controlling Cyberwarfare: International Laws of Armed Conflict and Human Rights in the Cyber Realm. UWSpace. Retrieved from http://hdl.handle.net/10012/17090

Jančárková, T., & Toompere, G. (n.d.). National CERT/CSIRT – Mandate and Organisation.

Jensen, E. T. (2017). The Tallinn Manual 2.0: Highlights and Insights. *48*.

Kelty, C. (2011). The Morris Worm. Limn, 1(1). Retrieved from https://escholarship.org/uc/item/8t12q5bj

Kilovaty, I. (2014). Cyber Warfare and the Jus Ad Bellum Challenges: Evaluation in the Light of the Tallinn Manual on the International Law Applicable to Cyber Warfare. 5(1).

Koloßa, S. (2019). Is There Really a Need for a New "Digital Geneva Convention"? Humanitäres Völkerrecht: *Journal of*

International Law of Peace and Armed Conflict, 2(1/2), 37–52.

Kuru, H. (2017). Prohibition of Use of Force and Cyber Operations as "Force."

Langner, R. (2013). A Technical Analysis of What Stuxnet's Creators Tried to Achieve.

Legality of the Threat or Use of Nuclear Weapons. , (International Court of Justice July 8, 1996).

Lahmann, R. G. (2012). Cyber Warfare: Applying the Principle of Distinction in an Interconnected Space,. Israel Law Review, 45(3), 381-402.

Li, J. L. (2018). WannaCry ransomware: Analysis, encryption, and decryption. Computers and Security, 77, 53-69. doi:https://doi.org/10.1016/j.cose.2018.03.011

Libicki, M. C. (2015). The defender's dilemma: Charting a course toward cybersecurity. Rand Corporation.

Legality of the Use by a State of Nuclear Weapons in Armed Conflict. , (International Court of Justice July 8, 1996).

Loomis, A. (2022). Defend Forward and Sovereignty. In J. Goldsmith (Ed.), The United States' Defend Forward Cyber Strategy (pp. 151–180; By A. Loomis). Oxford University Press. https://doi.org/10.1093/oso/9780197601792.003.0008

Lotrionte, C. (2018). Reconsidering the Consequences for State-Sponsored Hostile Cyber Operations Under International Law. *The Cyber Defense Review, 3*(2), 73–114.

Mačák, K. (2016). Is the international law of cyber security in crisis? 2016 8th International Conference on Cyber Conflict (CyCon), 127–139. Tallinn, Estonia: IEEE. https://doi. org/10.1109/CYCON.2016.7529431

Madubuike-Ekwe, J. N. (2021). Cyberattack and the Use of Force in International Law. *Beijing Law Review, 12*(02), 631–649. https://doi.org/10.4236/blr.2021.122034

McGavran, W. (2009). Intended Consequences: Regulating Cyber Attacks. Tulane Journal of Technology & Intellectual Property, 12. Retrieved from https://journals.tulane.edu /TIP/article/view/2573

Melzer, N., & Kuster, E. (2016). New IHL handbook: International Humanitarian Law: A Comprehensive Introduction (Vol. 98). Cambridge University Press. Retrieved from https://www.cambridge.org/core/journals/international-review-of-the-red-cross/article/abs/new-ihl-handbook/CBC9B774D97D398A261EFF2CFAAD9A03

Mačák, K. (2016). Is the international law of cyber security in crisis? 8th International Conference on Cyber Conflict (CyCon) 2016, (pp. 127-139).

Melzer, N. (2008). Targeted killing in international law. Oxford University Press.

Melzer, N., & Kuster, E. (2016). International humanitarian law. A Comprehensive Introduction.

Military and Paramilitary Activities in and against Nicaragua. , (International Court Of Justice November 26, 1984).

Moynihan, H. (2019). The Application of International Law to State Cyberattacks: Sovereignty and Non-intervention.

National Research Council. (2010). *Proceedings of a Workshop on Deterring Cyberattacks: Informing Strategies and Developing Options for U.S. Policy* (p. 12997). Washington, D.C.: National Academies Press. https://doi.org/10.17226 /12997

Nguyen, R. (2013). Navigating "Jus Ad Bellum" in the Age of Cyber Warfare. California Law Review, 101(4), 1079–1129.

Oil Platforms (Islamic Republic of Iran v. United States of America). , (International Court of Justice November 6, 2003).

Okpaleke, F., & Burton, J. (2020). US grand strategy and the use of unmanned aerial vehicles during the George W. Bush administration. In Emerging technologies and international. Routledge, 153-170.

Osinga, F. P., & Roorda, M. P. (2016). From Douhet to drones, air warfare, and the evolution of targeting. Targeting: The challenges of modern warfare, 27-76.

Panwar, L. G. S. (2018, January 8). Future WarsCyberspace: The Fifth Dimension of Warfare – Part I. Retrieved January 9, 2024, from Future Wars website: https://futurewars. rspanwar.net/cyberspace-the-fifth-dimension-of-warfare-part-i/

Perkovich, G., & Levite, A. (Eds.). (2017). Understanding cyber conflict: 14 analogies. Washington, DC: Georgetown University Press.

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. (n.d.). Retrieved January 9, 2024, from IHL Databases International Humanitarian Law Databases website: https://ihl-databases. icrc.org/en/ihl-treaties/api-1977

Roscini, M. (2018). Cyber Operations: Identifying the Problem and the Applicable Law (Chapter 1). In *M. Roscini, Cyber Operations and the Use of Force in International Law (Vol. 23)*. Oxford:Oxford University Press.

Rosenzweig, P. (2013). Cyber warfare: how conflicts in cyberspace are challenging America and changing the world. California: ABC-CLIO.

Rid, T., & McBurney, P. (2012). Cyber-Weapons. *The RUSI Journal*, *157*(1), 6–13. https://doi.org/10.1080/03071847.2012.664354

Ryan, M. (2021). Ransomware Revolution: The Rise of a Prodigious Cyber Threat. Cham: Springer International Publishing. https://doi.org/10.1007/978-3-030-66583-8

Schmitt, M. N. (Ed.). (2013). *Tallinn manual on the international law applicable to cyber warfare: Prepared by the international group of experts at the invitation of the NATO Cooperative Cyber Defence Centre of Excellence*. Cambridge ; New York: Cambridge University Press.

Schmitt, M. N. (Ed.). (2017). *The use of force. In Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (2nd ed., 328–356). Cambridge University Press. https://doi.org/10.1017/9781316822524.020

Schmitt, M. N. (2022, July 28). Cyber Symposium—The Evolution of Cyber Jus ad Bellum Thresholds. Retrieved January 13, 2024, from Lieber Institute West Point website: https://lieber.westpoint.edu/evolution-cyber-jus-ad-bellum-thresholds/

Shirky, C. (2011). The Political Power of Social Media: Technology, the Public Sphere, and Political Change. *Foreign Affairs*, *90*(1), 28–41.

Simmons, N. (2014). A Brave New World: Applying International Law of War to Cyber-Attacks. *Journal of Law & Cyber Warfare*, *4*(1), 42–108.

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

Spafford, E. H. (1989, September). The internet worm incident. In European Software Engineering Conference (pp. 446-468). Berlin, Heidelberg: Springer Berlin Heidelberg.

Sukin, L., & Weiner, A. S. (2021, June 7). War and Words: The International Use of Force in the United Nations Charter Era [SSRN Scholarly Paper]. Rochester, NY. Retrieved from https://papers.ssrn.com/abstract=3862024

Schmitt, M. N. (2017). International law in cyberspace: The Koh speech and Tallinn Manual 2.0. *Journal of Conflict & Security Law, 22*(2), 299-326.

Shirky, C. (2011). The political power of social media: Technology, the public sphere, and political change. *Foreign Affairs, 90*(1), 28-41. Retrieved from https://www.foreignaffairs .com/articles/2010-12-20/political-power-social-media

Singer, P. W. (2014). *Cybersecurity and Cyberwar: What everyone needs to know*. Oxford, UK: Oxford University Press. doi:10.1093/acprof:oso/9780199918119.001.0001

Spafford, E. &. (2017). *The Morris Worm. In Computer Viruses and Malware*. Springer. Retrieved from https://doi.org/10.1007 /978-3-319-63239-9_4

Sutherland, I., Xynos, K., Jones, A., & Blyth, A. (2015). The Geneva Conventions and Cyber-Warfare: A Technical Approach. *The RUSI Journal, 160*(4), 30–39. https://doi.org /10.1080/03071847.2015.1079044

Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations (2nd ed.). (2017). Cambridge: Cambridge University Press. https://doi.org/10.1017/9781316822524

Tsagourias, N. (2012). Cyber Attacks, Self-Defence and the Problem of Attribution. Retrieved from https://papers.ssrn. com/abstract=2538271

Tortonesi, M., Wrona, K., & Suri, N. (2019). Secured distributed processing and dissemination of information in smart city environments. IEEE Internet of Things Magazine, 2(2), 38-43.

United Nations. (1948). Charter of the United Nations. United Nations.

UNSC. (2001). Resolution 1373 (2001) (Resolution No. S/RES/1373 (2001); p. 4). United Nations. Retrieved from United Nations website: unodc.org/pdf/crime/terrorism/res_1373_english.pdf

Van Dijk, B. (2018). Human rights in war: On the entangled Foundations of the 1949 Geneva Conventions. American Journal of International Law, 112(4), 553-582.

Yoo, J. (2004). Using Force. *The University of Chicago Law Review, 71*(3), 729–797.

Zemanek, K. (2012). "Armed Attack". In R. Wolfrum (Ed.), The Max Planck encyclopedia of public international law (p. 600). Oxford ; New York: Oxford University Press.