Applicability Of International Humanitarian Law In Cyberspace

Captain. Khalifa A. Alkuwari
Phd Researcher And Faculty Member - The Police Academy . State of Qatar

Applicability Of International Humanitarian Law In Cyberspace

Captain. Khalifa A. Alkuwari
Phd Researcher And Faculty Member - The Police Academy . State of Qatar

ABSTRACT

The escalating use of cyberspace in warfare has become a pressing concern globally, given the far-reaching and potentially devastating consequences it holds. Cyber hostilities can affect a broad spectrum of human activities, from disrupting electricity supply to compromising communication networks, impacting virtually every facet of modern life. The vulnerability of any internet-connected device highlights the urgent need for robust legal structures to regulate the employment of cyberspace in warfare.

While International Humanitarian Law provides overarching regulations for warfare, its application to cyber hostilities presents unique challenges. This paper titled the 'Applicability of International Humanitarian Law in Cyberspace delves into the complexities of applying the established principles of International Humanitarian Law, traditionally geared towards kinetic warfare, to the realm of cyberattacks. It examines the possibility and practicality of extending the existing laws of war, as defined by International Humanitarian Law, to encompass cyber hostilities, offering insights into the legal and ethical consequences of broadening its scope.

Key words: Cyber Security, cyber warfare, international Humanitarian Law, Human Rights, Law.

List Of Abbreviationss:

DDoS - Distributed Denial of Service attacks
ICRC - International Committee of the Red Cross
ICJ - International Court of Justice
IHL - International Humanitarian Law
AP - Additional Protocols
IT - Information Technology
UNGA - United Nations General Assembly

المُلخَّص

قابلية تطبيق القانون الإنساني الدولي في الفضاء السيبراني

النقيب/ خليفة أحمد الكواري
باحث دكتوراه وعضو هيئة التدريس- أكاديمية الشرطة. دولة قطر

أصبح الاستخدام المتزايد للفضاء الإلكتروني في الحروب مصدر قلق عالمي، نظرًا للعواقب الواسعة النطاق والمدمرة المحتملة التي يحملها. يمكن للأعمال العدائية الإلكترونية أن تؤثر على طيف واسع من الأنشطة البشرية، بدءًا من تعطيل إمدادات الكهرباء وحتى اختراق شبكات الاتصالات، مما يؤثر على كل جانب تقريبًا من جوانب الحياة الحديثة. تسلط هذه الحالة الضوء على الحاجة الملحة إلى بنى قانونية متينة لتنظيم استخدام الفضاء الإلكتروني في الحروب.

بينما يقدم القانون الدولي الإنساني قواعد شاملة للحروب، فإن تطبيقه على الأعمال العدائية الإلكترونية يطرح تحديات فريدة. يتناول هذا البحث، الذي يحمل عنوان «تطبيق القانون الدولي الإنساني في الفضاء الإلكتروني»، التعقيدات المتعلقة بتطبيق مبادئ القانون الدولي الإنساني الراسخة، التي كانت موجهة تقليديًا نحو الحروب الحركية، على عالم الهجمات الإلكترونية. يفحص البحث إمكانية وعملية توسيع القوانين الحالية للحرب، كما هو محدد بالقانون الدولي الإنساني، لتشمل الأعمال العدائية الإلكترونية، مقدمًا رؤى حول العواقب القانونية والأخلاقية لتوسيع نطاقه.

الكلمات المفتاحية: أمن السيبراني، الحرب السيبرانية، القانون الدولي الإنساني، حقوق الانسان، القانون الدولي.

Introduction:

In recent years, there has been a marked increase in the frequency of cyberattacks, which pose a significant threat to national security.(1) These attacks have the potential to disrupt crucial infrastructure, including electrical grids, air defense systems, and nuclear facilities. This escalation has led to suggestions that cyberattacks should be classified as military operations. However, these modern forms of aggression differ greatly from traditional armed attacks originally governed by International Humanitarian Law (IHL).

The relevance of IHL in the context of cyber hostilities warrants careful examination. IHL, a specialized branch of public international law, is applicable during times of armed conflict. It aims to regulate the conduct of belligerents and is predicated on the principle that even in warfare, certain rules must be upheld.(2) For an action to be subject to IHL, it must either be part of an ongoing armed conflict or possess the potential to independently instigate such a conflict.(3) Thus, the application of IHL to cyber hostilities hinges on their occurrence within the framework of an armed conflict or their capacity to independently trigger one.(4) This text explores the intricate relationship between cyber hostilities and IHL, investigating how these modern forms of warfare might be integrated into the established legal principles governing armed conflict.

Armed conflict, as defined in international law, occurs when there is a use of armed violence between two or more parties.(5) This armed violence can manifest as either international or non-international in nature. An international armed conflict is characterized by engagement between two or more high contracting states,(6) whereas a non-international armed conflict involves hostilities between a state government and one or more non-state armed groups, or between such groups themselves within astate'sterritory.(7)

(1) Pandey, Tripathi and Vashist, "A Survey of Cyber Security Trends, Emerging Technologies and Threats." Studies in Computational Intelligence (2022) 19 – 33.

(2) Nilz, Mezler, International Humanitarian Law: A Comprehensive Introduction. (International Committee of the Red Cross, 2016), 15 – 17.

(3) Ibid

(4) David, E. Graham, "Cyber Threats and the Law of War" Journal of National Security Law and Policy (2010) 4, 87

(5) The Prosecutor v. Dusko Tadić, (Tadic's case) (Decision on the Defence Motion for Interlocutory Appeal on Jurisdiction) IT-94-1-A (2 October 1995) [70]

(6) Ibid

(7) International Committee of the Red Cross (ICRC), Geneva Convention for the Amelioration of the Condition of the Wounded and Sick in Armed forces in the Field (1st Geneva Convention) (GC 1) 12 August 1949, 75 UNTS 287; Common Article 2

The contemporary landscape of global conflicts includes various instances of both types of armed conflicts. For example, Russia's invasion of Ukraine represents an international armed conflict due to the involvement of sovereign states.(8) In contrast, the recent conflict in Afghanistan between the Taliban and the former government, occurring within the borders of a single country and involving non-state actors, is an instance of a non-international armed conflict.(9) The increasing use of sophisticated weapons in both international and non-international armed conflicts is a common trait that poses a significant threat to the long-term safety and well-being of humanity. While many of these advanced weapons are prohibited by the laws of war, the recent trend of utilizing cyberspace as a theater of warfare has sparked serious concerns among the global community and policy-makers.

This apprehension is evident in the actions of the United Nations, which has formed various expert groups to delve into how international law might be applied within the realm of cyberspace.(10) Through these collaborative efforts and discussions, a general consensus has emerged among states affirming that international law, including the principles and rules of warfare, is indeed applicable to activities conducted in cyberspace.(11) Such initiatives reflect a growing recognition of the need to address the unique challenges posed by cyber warfare, ensuring that the conduct of hostilities in this new domain adheres to established international legal standards. This evolving consensus marks a crucial step towards maintaining global peace and security in an increasingly digital world.

Despite the agreement that international law applies to cyberspace, there remains a notable lack of consensus on how the principles of IHL specifically apply in the cyber context.(12) This gap in consensus allows entities engaged in cyber hostilities to potentially evade criminal liability, highlighting a critical area of concern in the field of international law. This research is thus significant, as it seeks to investigate how the protections afforded by IHL can be effectively applied in the realm of cyber warfare.

(8) ICRC, Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of Non- International Armed Conflicts (Protocol 11), 8 June 1977 (AP II), Article 3

(9) Ibid, Article 2

(10) Kriangsak Kittichaisaree. Public International Law of Cyberspace. (Springer, 2017) 335 – 356.

(11) United Nations General Assembly, "Group of Governmental Experts on Advancing Responsible State Behavior in Cyberspace in the Context of International Security" (July 2021) A/76/135, Para. 71

(12) François Delerue, "Reinterpretation or Contestation of International Law in Cyberspace?" Israel Law Review (2019) 52 (3), 295 – 326.

For clarity and consistency in this discussion, it is important to define what we refer to as 'cyberspace.' While a universally accepted definition is elusive, for the purposes of this paper, cyberspace is understood to encompass any virtual environment, device, or medium that has an online presence. It is commonly characterized as a domain where digital information is processed, stored, and transmitted through digital signals and electromagnetic radiation.(13) Cyber hostilities, which often escalate into cyberattacks, represent a critical area of concern in modern warfare, particularly as they transcend traditional geographic boundaries through cyberspace. In an era where networks and infrastructures are increasingly interconnected, the exchange of information and data across these platforms has become faster and more efficient. This interconnectedness, however, also amplifies the potential impact of cyberattacks. These cyberattacks, defined as cyber operations capable of causing injury or death to individuals or damage or destruction to objects, are especially pertinent when conducted within the context of an armed conflict.(14) This paper focuses on such attacks, exploring their relevance and implications in the realm of international warfare. The ability of these cyber operations to reach beyond physical borders and affect both tangible and intangible assets underscores the necessity of adapting traditional warfare principles to address the unique challenges posed by cyber hostilities.

The pervasive integration of digital networks in everyday activities—ranging from online banking and communication through blogs and emails, to the management of complex systems and infrastructures—brings to the forefront the critical importance of addressing cyber hostilities. In today's interconnected world, the potential for both State and non-State actors to intentionally inflict harm on these networks and the data they contain is a significant concern.

The escalating reliance on and the widespread adoption of digital platforms have propelled cyberspace into becoming a new and complex domain of warfare.(15) This evolution raises a crucial question: How can the principles of IHL be effectively

(13) Azelmo. Erin. "Cyberspace in international law: does the internet negate the relevance of territoriality in international law. Studia Diplomatica 58 (2015): 153

(14) Smith, Michael. Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations, (Cambridge University Press 2017), 415

(15) Gian Piero Siroli, "Considerations on the Cyber Domain as the new worldwide Battlefield" International Spectator 53 (2) (2018) 111 – 123.

applied and enforced in the context of cyber hostilities? As we delve deeper into an era where the digital and physical realms are intricately linked, understanding and adapting the norms and rules of IHL to address the unique challenges posed by cyber warfare becomes increasingly imperative.

A. CYBER HOSTILITIES: A NEW DIMENSION IN WARFARE AND ITS LEGAL IMPLICATIONS UNDER INTERNATIONAL HUMANITARIAN LAW

Traditionally, warfare has been conducted across four domains: land, air, sea, and space.(16) However, the rapid advancement of technology has ushered in the era of cyber warfare, increasingly recognized as a fifth domain. This addition of cyber warfare brings with it significant legal ramifications under the laws of war.(17) It is important to conceptualize cyber warfare not as an isolated domain but as both a means and a method of warfare. Such an understanding facilitates the application of IHL principles to cyber hostilities.

By integrating cyber warfare within the established frameworks of IHL, it becomes possible to extend the existing legal norms and rules to this new domain. This approach is essential for ensuring that the conduct of hostilities in cyberspace adheres to internationally recognized standards, maintaining the protections and regulations that IHL provides in the context of modern warfare.

i. Cyber Hostilities as a means of warfare

The use of cyber hostilities as a means of warfare refers to the weapons employed in the conduct of hostilities. IHL permits states to select any means of warfare they deem appropriate, provided it complies with the provisions of the law.(18) In determining the means of warfare, states must keep in mind that the only legitimate objective of war is to weaken the adversary.(19) Therefore, any means of warfare

(16) David Jordan, James D Kiras, David J Lonsdale, Ian Speller, Christopher Tuck, C Dale Walton. Understanding Modern Warfare. (Cambridge University Press, 2016).

(17) Tim Grant, "On the Military Geography of Cyberspace" Leading Issues in Cyber Warfare and Security: Cyber warfare Security 2 (2015) 119

(18) Cordula Droege, "Get Off my Cloud: Cyber Warfare, International Humanitarian Law and the Protection of Civilians" International Review of the Red Cross 94 (886) (2012), 533 – 578.

(19) Declaration Renouncing the Use, in Time of War, of Explosive Projectiles Under 400 Grammes Weight (Saint Petersburg, 29 November/ December 1868), Preambular Paragraph

adopted must be directed towards this objective and must not result in unnecessary suffering or injury to humans.(20) Weapons that fail to meet these requirements are prohibited, as are those that are inherently indiscriminate, meaning those that cannot be targeted at a specific military objective or whose effects cannot be limited.(21) States engaging in cyber hostilities as a means of warfare must take these considerations into account when selecting cyber weapons to deploy. Some commonly used cyber weapons include ransomware, bonnet, stuxnet, malware, and others.(22)

Stuxnet is widely regarded as the most prominent cyber weapon that has been employed by states over the years. It gained notoriety for its role in the Estonian cyberattacks of 2007, which were part of a larger political dispute between Russia and Estonia concerning the removal of a Soviet-era monument in Tallinn.(23) While the motivations behind the attack are of interest, the primary focus is on the weapon used: Stuxnet. This cyber weapon has been hailed as a "game changer" due to its ability to infiltrate and damage power grids and power plants that were previously thought to be impervious to cyberattacks.(24) Stuxnet was designed to propagate rapidly across multiple computers, even in the absence of an internet connection, through USB drives.(25) Its stealthy and covert nature made it difficult to detect, as it could spread undetected between Windows computers that lacked an internet connection. This virus operates in the following stages which include exploiting vulnerabilities in both hardware and software components of operating systems and networks, aiming to infiltrate as many target systems as possible, and employing a rapid self - replication mechanism to propagate itself extensively and deeply. One notorious example of its destructive capability was demonstrated when it infiltrated Siemens' Step7 software, which is widely used for coding industrial automation systems.(26) By penetrating the software, it compromised the logic controllers, thereby enabling its creators to spy on industrial systems and potentially gain control over the entire system.(27)

(20) ICRC, Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflict (Protocol I) 8 June 1977 (AP 1) Art. 35(2)

(21) ICRC, Customary International Humanitarian Law, 2005, Volume 1 (CIHL), Rule 72 CIHL

(22) Trey Herr, "PrEP: A Framework for Malware and Cyber Weapons" Journal of Information Warfare (13), issue 1 (2014), 87. 106.

(23) Herzog, Stephen, "Revisiting the Estonian Cyber Attacks: Digital Threats and Multinational Responses" Journal of Strategic Security 4, issue no. 63 (2011): 49

(24) Milevski, Lucas "Stuxnet and Strategy: A Special Operation in Cyberspace?" Joint Forces Quarterly 64, (2011)

(25) Rao, Siddharth Prakash. "Stuxnet, A New Cyberwar Weapon: Analysis from a Technical Point of View." ResearchGate, (2014). https://doi.org/10.13140/2.1.1419.5205.

(26) Ibid

(27) Ibid

Certainly, stuxnet is capable of launching indiscriminate attacks without the ability to differentiate between civilian infrastructure and military targets. As a result, its use as a cyber weapon by states should be discouraged due to its indiscriminate nature, which contravenes the principles of IHL. Furthermore, in recent times, states have adopted another type of cyber weapon known as Wannacry ransomware, The Wannacry ransomware attack was a worldwide cyberattack perpetrated by the Wannacry ransomware cryptoworm, which encrypted data and required cryptocurrency ransom payments from devices using the Microsoft Windows operating system.(28) Researchers have found similarities between the WannaCry code and programs utilized by state hackers in prior attacks. Nevertheless, they emphasized that determining the attack's origin as a state actor was premature at that pointintime.(29)

On June 27th, 2017, a devastating ransomware attack known as NotPetYa struck Ukraine.(30) The malware was distributed through software updates to the country's most widely used tax-filing software. Once on an organization's network, the malware swiftly spread to all accessible computer systems. The consequences of the attack were far-reaching, causing disruption to cash registers in supermarkets, financial institutions, medical facilities, subway ticket sales points, vital facilities, industrial production enterprises, and governmental organizations. In a matter of hours, almost all aspects of Ukrainian life were brought to a standstill.(31) These examples serve as a stark reminder of the destructive potential of cyber weapons, and as such, it is imperative that states agree to regulate cyber weapons in a manner similar to that of kinetic weapons, as outlined in the principles of international humanitarian law.

ii. Cyber Hostilities as a Method of Warfare

Warfare strategies encompass a range of approaches that nations may utilize to achieve their military goals. While states have the discretion to select their tactics

(28) Akbanov, Maxat, Vassilios G. Vassilakis, and Michael D. Logothetis. "WannaCry Ransomware: Analysis of Infection, Persistence, Recovery Prevention and Propagation Mechanisms." Journal of Telecommunications and Information Technology 1, (2019): 113–24.

(29) Ibid

(30) Smith, Michael. & Biller, Jefferey, "The NotPetya Cyber Operation as a Case Study of International Law" EJIL: Talk! (2017) <https://www.ejiltalk.org/the-notpetya-cyber-operation-as-a-case-study-of international-law/> accessed November 30, 2023

(31) Ibid

and strategies during hostilities, IHL imposes restrictions on certain methods. Among the prohibited tactics are denial of quarter,(32) deceitful actions such as perfidy or treachery,(33) and the misuse of recognized emblems, signs, and uniforms.(34)

In the realm of cyber warfare, IHL does not explicitly outline which military strategies or tactics are permissible or forbidden in cyberspace. Nonetheless, a direct interpretation of IHL principles related to kinetic warfare provides insights into the types of methods that should be avoided. Historically observed cyber strategies include Denial of Service attacks, interception and redirection of internet traffic to capture data, alteration or destruction of network data, and gaining undetected control over computers and networks.(35) Other methods involve cyber espionage, website defacement, propaganda dissemination, illicit acquisition of confidential data, use of counterfeit hardware, and software theft or destruction.

During the Estonian cyber-attack, several cyber tactics were deployed, this includes threats such as Distributed Denial of Service attacks (DDoS), malformed web queries and email spam, ping and UDP floods. There were also sophisticated attempts to infiltrate systems, such as SQL injection. Affected systems included websites, email servers, DNS servers, and routers.(36) The most noticeable were the attacks on websites, impacting various sectors, including the state authorities, president, legislature, police, banks, ISPs, online media, numerous small businesses, and local government websites. (37)

Cyberattacks often target infrastructure that lacks military significance, and their destruction typically does not advance military objectives. It is crucial to remind states engaged in cyber hostilities about the forbidden means and methods of warfare under International Law, emphasizing that cyber conflicts are not exempt from these prohibitions. Conversely, if cyber hostilities are considered a distinct fifth domain

(32) Additional Protocol 1. Article 40

(33) Ibid, Article 37

(34) Ibid, Article 39

(35) Grange, Miranda. Cyber warfare and the law of armed conflict. (Research paper, University of Wellington, 2014): 4 -8.

(36) Boyte, Kenneth, "A Comparative Analysis of the Cyberattacks Against Estonia, the United States, and Ukraine: Exemplifying the Evolution of Internet-Supported Warfare". International Journal of Cyberwarfare and Terrorism 7, issue no. 54 (2017)

(37) Remenyi, Dan. ECIW2008- 7th European Conference on Information Warfare and Security (Academic Conferences Limited) 2008.

of warfare, rather than merely a tactic within warfare, then the established rules of war governing other domains should be equivalently applicable to cyber warfare. This perspective necessitates the application of traditional warfare principles to the cyber domain, ensuring a consistent and lawful approach across all forms of military engagement.

iii. Legal Implications of Cyber Hostilities

A pivotal concern in modern warfare is the evolution from purely physical combat to hostilities in cyberspace, a shift not anticipated during the original formulation of IHL. This development raises a crucial question: Is there a need for a new legal framework to govern cyber hostilities, or can the existing principles of IHL be effectively adapted to this domain? This section, along with the next, argues that the current principles of IHL can be aptly extended to cyber warfare, thereby encompassing cyber hostilities as a new means and method of warfare under its purview.

The International Court of Justice (ICJ) has affirmed that IHL is applicable to all forms of warfare and to all types of weapons, encompassing those from the past, present, and future.(38) Similarly, the International Committee of the Red Cross (ICRC), as the guardians of IHL, unanimously recognizes that IHL extends to future means and methods of warfare, including cyber hostilities.(39) Furthermore, the obligation of states to conduct weapon reviews suggests that IHL was designed to regulate evolving weaponry, even those developed long after the original rules were codified. This obligation requires states to assess new methods and means of warfare, ensuring their compliance with IHL principles before deployment.(40) Cyber weapons, therefore, must be evaluated against these criteria.

Ultimately, there is no doubt that the principles of IHL are applicable to cyberspace. However, the challenge lies in how specific principles such as distinction, proportionality, precaution, humanity, and military necessity are applied within this domain. The subsequent section will present an argument addressing this issue.

(38) Legality of the Threat or Use of Nuclear Weapons (Advisory Opinion) ICJ 3, ICJ Reports, (8 July 1996) [86]
(39) International Committee of the Red Cross, "International Humanitarian Law and Cyber Operations during Armed Conflicts", International Review of the Red Cross 102, Issue no. 913 (2020): 481 – 492
(40) Additional Protocol 1. Article 36

B. TAKING IHL TO THE CYBERSPACE: CYBER OPERATIONS IN INTERNATIONAL ARMED CONFLICTS

According to Common Article 2, IHL is applicable in "all cases of declared war or any other armed conflict between two or more of the High Contracting Parties, irrespective of whether a state of war is acknowledged by one of them."(41) This provision brings any armed conflict between states under the ambit of IHL. A pivotal inquiry arises: Does launching a cyberattack against vital infrastructure of another state constitute an international armed conflict?

The authors of the Tallinn Manual, a significant authority on cyber warfare, concurred that cyber operations could amount to international armed conflict.(42) This view is shared by several states and ICRC. The ICRC posits that there's no basis for distinguishing between cyber operations and kinetic operations when both result in civilian or combatant casualties.(43) France, for instance, has articulated that cyber operations indicative of hostilities between states can signify an international armed conflict. The decisive factor lies in whether autonomous cyber operations reach the requisite level of violence to be classified as armed conflict."(44)

The debate around the applicability of IHL in cyberspace primarily revolves around how principles like distinction, proportionality, precaution, military necessity, and humanity are applied within this domain. Among these, the principle of distinction, as the cornerstone of IHL, is critical. Therefore, a detailed examination of how the principle of distinction applies to cyberspace is essential.

i. **Applying the Principle of distinction to the cyberspace**

The principle of distinction is a key principle in warfare and is considered essential, mandating belligerents to consistently differentiate the between civilians and combatants, as well as between civilian objects and military objectives.(45)

(41) Geneva Convention for the Amelioration of the Wounded and Sick in armed forces in the field. Article 2

(42) Smith. Talinn Manual 2.0. Rule 83, paragraphs 13 - 15

(43) Laurent, Rodenhäuser, Tillman, and Knut Dörmann,. "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 102, Issue no. 913 (2020): 287 - 334

(44) NATO Cooperative Cyber Defence Centre of Excellence. National Position of France (2019) - International Cyber Law: Interactive Toolkit. (International cyber law: interactive toolkit) 2023.

(45) Laurie R Blank, "Taking Distinction to the Next Level: Accountability for Fighters' Failure to Distinguish

Civilians are defined as individuals who are not, or no longer, actively participating in hostilities, in contrast to combatants who are members of an armed force directly engaged in conflict.(46) Combatants are permitted to bear arms openly; civilians are not and could face legal prosecution for doing so by their national jurisdictions.(47) This principle unequivocally prohibits intentional harm or direct attacks on civilians, though it acknowledges the possibility of collateral damage or unintended harm to civilians under certain conditions.(48)

Challenges of Distinction in Cyberspace:

While distinguishing between civilians and combatants in traditional kinetic warfare is relatively straightforward, thanks to established legal definitions and criteria, the unique nature of cyberspace complicates this distinction. The challenge lies in identifying whether the person behind a potentially targeted computer system is a civilian or a cyber combatant. This difficulty in differentiation is crucial because the application of IHL principles to cyber warfare largely hinges on this distinction. Therefore, it is vital to explore methods to accurately distinguish civilians from cyber combatants in the realm of cyber warfare.

Distinguishing Non-Combatant Civilians from Cyber Combatants in IHL

IHL establishes criteria to classify individuals as combatants: "(i) bearing arms openly; (ii) displaying a distinct sign recognizable from a distance; (iii) being under a responsible commander; (iv) conducting operations in conformity with the laws and customs of war; and (v) being a party to the conflict."(49) In cyber warfare, the latter three criteria are instrumental in identifying cyber combatants. A member of a state's armed forces engaged in cyber hostilities typically meets these conditions and is thus considered a legitimate target.

---

themselves from Civilians" Virginia Law Review (2016) 56, 83.

(46) Emily Crawford, Identifying the Enemy: Civilian Participation in armed conflict, (Oxford University Press, 2015).

(47) Additional Protocol 1. Article 44(3)

(48) Meyer, Jeanne, "Tearing Down the Facade: A Critical Look at the Current Law on Targeting the Will of the Enemy and Air Force Doctrine". Armed Forces Review 51 (2002): 143

(49) Dinnis, Heather Harrison. "Participants in Conflict – Cyber Warriors, Patriotic Hackers and the Laws of War", in Dan Saxon (ed.). International Humanitarian Law and the Changing Technology of War, (Martinus Nijhoff, Publishers, 2012), 245

While the first and second criteria listed above may not be necessary for determining who qualifies as a cyber combatant, the third, fourth, and fifth criteria are useful for making such determinations. Based on these criteria, individuals who are members of the armed forces of a state involved in cyber hostilities can be considered cyber combatants and would therefore be legitimate targets for attack. As members of the state's armed forces, it is presumed that these individuals have already satisfied the requirements of organization, responsible command, and compliance with the law. As a result, cyberattacks should be directed solely at these individuals, who are referred to as cyber combatants.

However, if a group of hacktivists, who have no connection to the state in which they reside, carry out offensive cyber operations against another state, IHL would not apply. This is because IHL only applies to organized armed groups or members of the armed forces of a state engaged in hostilities.(50) In such cases, the hacktivists may not be organized, under responsible command, or comply with IHL provisions. Therefore, cyber combatants should only be considered individuals who are engaged in cyber hostilities and meet the criteria outlined above.

Recognizing the classification of individuals to be considered as cyber combatants, it is imperative to note that any person not falling within the aforementioned categories is considered a civilian and may not be targeted unless they actively participate in cyber hostilities. The question that arises is at what point can it be determined that an individual is engaged in direct participation in cyber hostilities - when they merely introduce malicious code into a cyber network, when they only write the code without executing it, or when they instruct the creation of the code in the first place?

The Law does not define what constitutes direct participation in hostilities to start with.(51) However, the interpretative guide on the concept of direct participation in hostilities, published by ICRC proposes three cumulative components to make up the act of direct participation in hostilities. First, potential to seriously impair military operations or cause harm;(52) Second, a direct causal link between the act and the harm; and third, intent to cause the required harm.(53) For cyber activities carried out by civilians to be considered as direct participation in hostilities, certain conditions must be satisfied:

(50) David Kretzmer, "Rethinking Applicability of IHL in non-international armed conflicts" Israel Law Review 42 (1) (2009) 8 – 45.

(51) Additional Protocol 1, Article 51 (1)

(52) Melzer, Nils. Interpretative Guidance on the notion of Direct participation in hostilities under International Humanitarian Law. (International Committee of the Red Cross, 2009), 46

(53) Ibid

i. Requirement for Physical Harm, Injury, or Death:

The first criterion for an act to be considered direct participation in hostilities is that it must result in physical harm, injury, or death.(54) Experts who developed the Tallinn Manual concur that an act must either intend or actually achieve a significant negative impact on those to whom such attack is directed for it to qualify as a direct participation in hostilities. The act of engaging in military operations or using capabilities in a manner that targets or harms protected individuals or objects, resulting in death, injury, or damage to property would qualify as direct participation in hostilities.(55)Accordingly, a cyber operation that only disrupts a radio frequency or steals important data without further consequences would not be regarded as direct participation in hostilities. What this entails is that direct participation in hostilities requires a differentiation based on the consequences of the operation: if a cyber-attack targets critical infrastructure like a power grid or a moving train, causing derailment and resulting in casualties, it is considered direct participation. Similarly, a cyberattack leading to an airplane crash would meet this criterion. Additionally, cyber operations primarily aimed at spreading propaganda or misinformation about an adversary do not constitute direct participation in hostilities, provided they do not cause physical harm. An example is the Estonian cyberattack mentioned earlier in this paper, which caused disruption but did not result in harm, death, or injury. Such operations do not meet the threshold of direct participation based on the criterion of physical harm.(56).

ii. Requirement for the existence of a direct causal link:

The second criterion for classifying an act as direct participation in hostilities is establishing a direct causal link between the act and its anticipated outcome.(57) This means the harm caused by the cyber operation should be directly traceable to the action taken. Researchers suggest that the concept of "proximate causality", encompassing both subjective and objective perspectives, is particularly apt for cyber operations. Objectively, this means the harm from the cyberattack is a foreseeable and normal outcome. Subjectively, it implies that the harm should

(54) Pandey, Anand Bhushan, Ashish Tripathi, and Prem Chand Vashist. "A Survey of Cyber Security Trends, Emerging Technologies and Threats." Studies in Computational Intelligence, 2022, 19–33.

(55) Smith. Talinn Manual 2.0. 429

(56) Turns, Davis, "Cyber Warfare and the Notion of Direct Participation in Hostilities", Journal of conflict and Security Law 17 (2012): 286

(57) Nils Mezler, "Keeping the Balance Between Military Necessity and Humanity: A Response to Four Critiques of the ICRC's Interpretative Guidance on the Notion of Direct Participation in Hostilities" NYU Journal of International Law and Politics 42 (2009) 831

be anticipated by those responsible for the operation.(58) Drawing an analogy, if civilians are engaged in general IT functions, such as managing email platforms or operating websites, they would not be considered as directly participating in hostilities. In these cases, the link between their actions and any potential damage is not proximate; the harm is not a natural consequence of their work, and they might not foresee any harmful outcomes. Conversely, an individual specifically recruited to carry out hostile cyber operations would likely meet the proximate causality criterion, as their actions are directly linked to the intended harmful outcome.(59)

iii. There must be the existence of a belligerent intent:

The final criterion for classifying an act as direct participation in hostilities is the belligerent nexus requirement. This necessitates that the cyberattack must be conducted with a specific intent to cause the anticipated effect.(60) The action must be purposefully aimed at achieving a particular outcome that impacts the adversary in the context of an armed conflict.

In summary, for a civilian to be considered as having directly participated in hostilities in the cyber context, all three aforementioned elements must be satisfied. These include the requirement for the operation to cause physical harm, injury, or death (the first element), the necessity of a direct causal link between the act and its harm (the second element), and the belligerent nexus, where the action is conducted with the intent to cause the specific harmful effect (the third element).

Distinguishing Civilian Objects from Military Objectives in Cyberspace.

Along with differentiating between civilians and combatants, it is crucial for belligerents in cyber warfare to distinguish between military objectives and civilian objects. Military objectives are defined as items that significantly contribute to military operations due to their characteristics, location, purpose, or function.(61) The destruction, seizure, or incapacitation of these objects as a key aspect of military

(58) Cheng, Bin. General Principles of Law as Applied by International Courts and Tribunals. (Cambridge University Press, 1987), 181

(59) Huang, Zhixiong and Ying, Yaohui. "The Application of the Principle of Distinction in the Cyber Context: A Chinese Perspective", International Review of the Red Cross 102, issue 913 (2020): 335 – 365

(60) David, Turns, "Cyberwarfare and the Notion of Direct Participation in Hostilities" Journal of Conflict and Security Law 17 (2) (2012) 279 – 297.

(61) David, Turns, "Military Objectives" in David Turn. Routledge Handbook of the Law of Armed Conflict. (Routledge 2016) 139 – 156.

strategy, either partially or entirely, can offer a significant military advantage in the prevailing circumstances.(62) Conversely, civilian objects are those not considered as military objectives.(63) Applying these definitions to cyber warfare is complex due to the interconnected nature of cyberspace. A single piece of cyber infrastructure might simultaneously contribute to military activities and equally serve civilian needs. Essential infrastructure like bridges, power plants, and even digital components such as routers and computers often have dual uses. IHL stipulates that attacks on dual-purpose objects must consider the principle of proportionality. The incidental damage to civilian property must not be excessive relative to the military advantage anticipated.(64) For instance, targeting a state's banking facilities to restrict an adversary's funding might offer a military advantage. However, such actions contravene IHL principles, as these facilities also serve civilian purposes. When attacking dual-use objects becomes militarily necessary, the principles of precaution must be adhered to by belligerents ensuring all feasible steps are taken to confirm the military nature of targets and minimize civilian impact.(65) Belligerents are obligated to take constant care to protect civilians. One essential precaution in cyber warfare is verifying the nature of the targeted object and providing adequate warning to civilians potentially affected by the attack. While challenging, this step is crucial and feasible. Non-observance of these principles in cyber warfare is tantamount to breaching IHL, just as in kinetic warfare.(66)

III. Applying the Principle of Proportionality in Cyberspace

The application of the principle of proportionality is crucial in cyber warfare due to the interconnected nature of the internet. In cyberspace, civilian objects and military objectives are often intertwined, leading to a scenario where attacks on military targets could inadvertently damage civilian objects. The principle of proportionality aims to guarantee that any unintentional harm caused to civilian objects during military operations is not excessively disproportionate to the anticipated military benefit.(67) The principle of proportionality precludes attacks

(62) Additional Protocol 1, Art 52(2)
(63) Ibid, Article 52(1)
(64) Ibid, Article 52(3)
(65) Ibid, Article 57 (2) (a) (I)
(66) ibid, Article 57 (1)
(67) Ian, Henderson, Kate Reece "Proportionality under International Humanitarian Law: The Reasonable Military Commander Standard and Reverberating Effects" Vanderbilt Journal of Transnational Law 51 (2018) 835

that are expected to cause significant incidental harm to civilians or civilian objects, unless the anticipated military advantage is directly proportional to the expected harm.(68) This means that a cyberattack resulting in significant civilian losses or damage, without corresponding substantial military gain, is not permissible.

In cyberspace, collateral damage to civilians as a result of direct attacks on military objectives is often inevitable. Cyberattacks targeting military assets might utilize civilian communication channels or infrastructure, thereby risking these civilian elements. However, the principle stipulates that such collateral damage must not be excessive when weighed against the military gain sought. The term 'excessive' in international law is not explicitly defined, making its application complex.(69)

It is argued that determining excessiveness involves more than merely quantifying civilian casualties against military gains. A holistic assessment is required, considering the overall impact and consequences of the action. Each situation must be evaluated individually to determine proportionality. For example, targeting a civilian aircraft's control system because it carries a few combatants would likely be deemed excessive. The ratio of civilian harm to military benefit is a key factor in this evaluation.

Ultimately, when a cyberattack against a dual-use infrastructure is militarily necessary, The civilian harm that arises from military operations should be proportional to the benefit that is anticipated from those operations. The principle of proportionality thus plays a critical role in balancing military objectives with the need to minimize civilian harm in cyber warfare.

CYBERATTACK AS A WAR CRIME, AND THE JURISDICTION OF THE INTERNATIONAL CRIMINAL COURT TO PROSECUTE FOR CYBERATTACKS

War crimes are grave violations of the Geneva Convention of 12 August 1949,(70) the Additional Protocols and the Principles of IHL in general, provided the violations occur in the context of an armed conflict.(71) The Rome Statute of the International

(68) Additional Protocol 1, Article 51(5) (b)

(69) Rogers, APV. Law on the Battlefield (3rd edn, Manchester University Press, 2012), 25 - 6

(70) The United Nations Rome Statute of the International Criminal Court, 2187, U.N.T.S. 90, entered into force July 2, 2002, (Rome Statute) Article 8 (2)

(71) Alexander, Schwarz, "War Crimes" Max Planck Encyclopedia of Public International Law (2014)

Criminal Court lists certain conducts that would qualify as war crimes. This includes willful killing, torture, inhuman treatment, etc.(72) While some of these war crimes like unlawful deportation or transfer or unlawful confinement cannot be committed in the cyberspace, others can be committed in the cyberspace. For instance, the war crime of intentionally directing attack against civilian objects or objects which are not military objectives.(73) This is possible because the major objects of attacks in the cyberspace are data stored in the internet. This raises the important question; should data be considered as 'objects' within the meaning of 'objects' in the Rome Statute? According to the Oxford English Dictionary, "data" is defined as "an item of information,". It is specifically defined as [q]uantities, letters, or symbols that a computer performs operations on, taken as a whole, in the context of computing. (74) Computer data is used for a variety of applications. Actually, data is necessary for both the internal workings of a computer and the information that is stored on it. Specific data types—sometimes in the form of software like Microsoft Windows or Apple iOS—are used to instruct computers on how to operate. Additional data is used to create what are known as log files, which are used to document various technical events that occur continuously in the computer system while it is being used and operated. The most obvious application of data is probably in the form of information storage for later daily needs. A portion of this data may appear to the computer user as documents, images, or other formats. These formats can range from user-friendly ones like Word and PDF files to more complex ones that are more likely to be used by computer experts, like diagnostics or programming.(75)

Expert opinion is divided on whether computer data should be categorized as 'objects' which destruction would amount to a war crime. Some contend that data, being intangible, should not be considered as objects, while others advocate for its protection under IHL. Some scholars argue from a technical standpoint, interpreting the term 'object' in IHL as implying tangible or physical properties.(76) They assert that since data is intangible, it does not fit the definition of an 'object' within the context of Additional Protocol I (AP 1) of the Geneva Conventions.(77)

(72) Article 8 of the Rome Statute

(73) Ibid

(74) All references to the Oxford English Dictionary are to its online version. See 'Welcome' (Oxford English Dictionary: The Definitive Record of the English Language)

(75) Ori Pomson 'objects' the Legal Status of Computer Data under International Humanitarian Law" (2023) Journal of Conflict and Security Law (28)2 349 – 389. 3

(76) Ibid

(77) McCormack, Tim, "International Humanitarian Law and the Targeting of Data" International Law Studies 94 (2018): 222

The Group of Experts responsible for the Tallinn Manual concurs that tangible elements of cyber infrastructure, like computers and networks, are objects.(78) However, they disagree on categorizing data as an object. The prevailing view is that an attack on data alone should not be considered an attack on civilian objects as defined in the Additional Protocols, due to its intangibility of the data and the specific wording of the protocols.(79) Nevertheless, they agree that certain cyber operations targeting data may qualify as attacks, especially if they impact the functionality of cyber infrastructure or have other tangible consequences.(80) Regardless of the above argument by experts, I submit that not recognizing data as an object within IHL poses a risk, as the destruction of essential civilian data during armed conflicts would then fall outside IHL's regulatory scope. This could leave civilians unprotected in cyberspace, contradicting the foundational principles of IHL established by Henry Dunant following the Battle of Solferino in 1859, which emphasized humanity and civilian protection.(81) Furthermore, cyberattacks which target objects designated for civilian purposes must be considered as war crime provided that they cause similar effects as would kinetic attacks and are committed within the context of an armed conflict. For instance, nothing stops a cyber attack which takes down a power grid or disrupts the workings of a hospital facility from being regarded as a war crime. It is not just about the means by which the crime was committed -cyberspace- it is the crime itself, and its effect. When a cyberattack qualifies as a war crime, the ICC would naturally assume jurisdiction based on Article 8 of the Rome Statute which gives the ICC jurisdiction over war crimes.

GEOPOLITICAL DYNAMICS, LEGAL CHALLENGES AND RECOMMENDATIONS

The traditional concept of state power, rooted in territorial control and geographical boundaries, faces challenges in the digital era. Historically, political power and influence have been tied to physical spaces, but the emergence of

(78) Tallinn Manual 2.0 (n 3) 437. See also Laurie R Blank and Gregory P Noone, International Law and Armed Conflict (2nd edn, Wolters Kluwer 2019) 466.
(79) Smith. Talinn Manual 2.0. 437
(80) Ibid
(81) Dunant, Henry. A Memory of Solferino. (Ravenio Books, 2013)

cyberspace raises questions about the applicability of these traditional frameworks.(82) Cyber hostilities introduce complex issues regarding state sovereignty over digital spaces. While a strict interpretation of sovereignty suggests control over cyber infrastructures within a state's territory, the borderless nature of the internet complicates this notion.

A major obstacle in applying IHL principles to cyber hostilities is the difficulty of attribution. (83) Cyber combatants often aim to remain anonymous and untraceable, potentially targeting civilian infrastructure while obscuring their origins. Unlike drone warfare, where origins and movements can be tracked, cyberattacks can originate from remote, unknown locations, making it challenging to identify the perpetrators. While this work strives to clarify the distinction between combatants and civilians in cyber warfare, the task remains complex, especially when civilians are used to launch attacks. To mitigate these challenges, states should employ advanced technical tools for tracing cyberattacks, enhancing their ability to attribute attacks correctly.(84) Developing robust defensive mechanisms and software against cyber weapons is also crucial for protecting civilians. Separating military and civilian cyber infrastructures can further shield civilians from the fallout of cyber hostilities. States must adapt to the unique challenges posed by cyber warfare. This includes evolving their legal frameworks, enhancing cyber defenses, and ensuring clear demarcations between civilian and military digital assets. By doing so, states can better protect their sovereignty and civilian populations in the face of evolving cyber threats.

CONCLUSION/RECOMMENDATIONS

With ongoing advancements in science and technology, the development of sophisticated cyber weapons by states is inevitable. These weapons pose significant risks to civilians and the general public. States increasingly rely on cyber hostilities

(82) Sheldon, John B, "Geopolitics and Cyber Power: Why Geography Still Matters," American Foreign Policy Interests 36, issue no. 5 (2014): 286

(83) Humna, Sohail, "Fault Lines in the Application of International Humanitarian Law to Cyber Warfare" Journal of Digital Forensics, Security and Law 17 (1) (2022) 8

(84) Howard Lipson "Tracking and Tracing Cyberattacks: Technical Challenges and Global Policy Issue" (Carniege Mellon University, 2002).

due to their cost-effectiveness and the reduced risk of physical casualties among combatants. Despite legal frameworks guaranteeing civilian protection, challenges persist in applying the principles of International Humanitarian Law (IHL) to cyber warfare. The controversy centers on adapting these essential principles to the unique context of cyberspace. It is therefore recommended that states should acknowledge that IHL is applicable to cyber hostilities. This recognition aligns with the intent of IHL to encompass present and future methods of warfare, including cyber operations. Viewing cyber hostilities within the framework of IHL is crucial, considering states' obligations to review new weapons and methods of warfare. States should also consider data in cyberspace as part of 'objects' eligible for protection under IHL. In cases where data constitutes a civilian object, it should be protected, and conversely, if it serves as a military objective, it may be a legitimate target of attack.

The conclusion underscores the urgency for states to adapt their strategies and legal interpretations to the realities of cyber warfare. This adaptation is necessary to ensure that civilians remain protected under the evolving landscape of international conflicts and cyber hostilities.

BIBLIOGRAPHY

Books

- Rogers, APV. Law on the Battlefield (3rd edn, Manchester University Press, 2012)
- Cheng, Bin. General Principles of Law as Applied by International Courts and Tribunals. (Cambridge University Press, 1987)
- Emily Crawford, Identifying the Enemy: Civilian Participation in armed conflict, (Oxford University Press, 2015).
- David Jordan, James D Kiras, David J Lonsdale, Ian Speller, Christopher Tuck, C Dale Walton. Understanding Modern Warfare. (Cambridge University Press, 2016).
- Dunant, Henry. A Memory of Solferino. (Ravenio Books 2013)
- Kriangsak Kittichaisaree. Public International Law of Cyberspace. (Springer, 2017)
- Melzer, Nilz. Interpretative Guidance on the notion of Direct participation in hostilities under International Humanitarian Law, (International Committee of the Red Cross 2009)
- Rogers, APV. Law on the Battlefield (3rd edn, Manchester University Press 2012)
- Remenyi Dan. ECIW2008- 7th European Conference on Information Warfare and Security (Academic Conferences Limited, 2008)
- Smith, Michael N (ed). Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations. (Cambridge University Press, 2017)

Contribution to Books

- Dinnis Heather Harrison. “Participants in Conflict – Cyber Warriors, Patriotic Hackers and the Laws of War” in Dan Saxon (Ed). International Humanitarian Law and the Changing Technology of War. (Martinus Nijhoff Publishers, 2013)

- David, Turns, "Military Objectives" in David Turn. Routledge Handbook of the Law of Armed Conflict. (Routledge 2016) 139 – 156.

- Journal Articles

- Alexander, Schwarz, "War Crimes" Max Planck Encyclopedia of Public International Law (2014)

- Azelmo E, "cyberspace in international law: does the internet negate the relevance of territoriality in international law", Studia Diplomatica 58 (2005): 153

- Akbanov, Maxat, Vassilakis, Vassillos G, and Logothetis, Michael D, "WannaCry Ransomware: Analysis of Infection, Persistence, Recovery Prevention and Propagation Mechanisms", Journal of Telecommunications and Information Technology 1 (2019): 113 – 124

- Boyte, Kenneth J, "A Comparative Analysis of the Cyberattacks Against Estonia, the United States, and Ukraine: Exemplifying the Evolution of Internet-Supported Warfare." International Journal of Cyberwarfare and Terrorism 7 (2017)

- Cordula, Droege, "Get Off my Cloud: Cyber Warfare, International Humanitarian Law and the Protection of Civilians" International Review of the Red Cross 94 (886) (2012), 533 – 578.

- David, E. Graham, "Cyber Threats and the Law of War" Journal of National Security Law and Policy (2010) 4, 87

- David Kretzmer, "Rethinking Applicability of IHL in non-international armed conflicts" Israel Law Review 42 (1) (2009) 8 – 45.

- International Committee of the Red Cross, "International Humanitarian Law and Cyber Operations during Armed Conflicts", International Review of the Red Cross 102, Issue no. 913 (2020): 481 – 492

- Gian Piero Siroli, "Considerations on the Cyber Domain as the new worldwide Battlefield" International Spectator 53 (2) (2018) 111 – 123.

- Herzog, Stephen, "Revisiting the Estonian Cyber Attacks: Digital Threats and Multinational Responses." Journal of Strategic Security 4, issue no. 2 (2011): 49 - 60

- Huang, Zhixiong and Ying, Yaohui. "The Application of the Principle of Distinction in the Cyber Context: A Chinese Perspective", International Review of the Red Cross 102, issue 913 (2020): 335 – 365

- Humna, Sohail, "Fault Lines in the Application of International Humanitarian Law to Cyber Warfare" Journal of Digital Forensics, Security and Law 17 (1) (2022) 8

- Howard Lipson "Tracking and Tracing Cyberattacks: Technical Challenges and Global Policy Issue" Carniege Mellon University, (2002).

- Ian, Henderson, Kate Reece "Proportionality under International Humanitarian Law: The Reasonable Military Commander Standard and Reverberating Effects" Vanderbilt Journal of Transnational Law 51 (2018) 835

- Jeanne, Meyer, "Tearing Down the Facade: A Critical Look at the Current Law on Targeting the Will of the Enemy and Air Force Doctrine", The Air Force Law Review 51 (2001)

- Laurent, Laurent, Rodenhäuser, Tillman, and Knut Dörmann, "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 102, Issue no. 913 (2020): 287 – 334

- Laurie, R Blank, "Taking Distinction to the Next Level: Accountability for Fighters' Failure to Distinguish themselves from Civilians" Virginia Law Review (2016) 56, 83.

- McCormack T, "International Humanitarian Law and the Targeting of Data", International Law Studies 94 (2018) 222

- Milevski, Lukas, 'Stuxnet and Strategy: A Special Operation in Cyberspace?', Joint Forces Quarterly 64 (2011): 63, 64 – 69

- Nils Mezler, "Keeping the Balance Between Military Necessity and Humanity: A

Response to Four Critiques of the ICRC's Interpretative Guidance on the Notion of Direct Participation in Hostilities" NYU Journal of International Law and Politics 42 (2009) 831

- Ori, Pomson 'objects' the Legal Status of Computer Data under International Humanitarian Law" (2023) Journal of Conflict and Security Law (28)2 349 – 389. 3

- Pandey, Anand Bhushan, Ashish Tripathi, and Prem Chand Vashist. "A Survey of Cyber Security Trends, Emerging Technologies and Threats." Studies in Computational Intelligence (2022), 19–33. https://doi.org/10.1007/978-981-16-8012-0_2.

- Turns, David, "Cyber Warfare and the Notion of Direct Participation in Hostilities", Journal of Conflict and Security Law 17, Issue no. 2 (2022): 279 – 297

- Tim, Grant, "On the Military Geography of Cyberspace" Leading Issues in Cyber Warfare and Security: Cyber warfare Security 2 (2015) 119

- Trey, Herr, "PrEP: A Framework for Malware and Cyber Weapons" Journal of Information Warfare (13), issue 1 (2014), 87. 106.

- Sheldon, John B, "Geopolitics and Cyber Power: Why Geography Still Matter", American Foreign Policy Interests 36, Issue no. 5 (2014): 286 – 293

Internet Sources

- Grange, Mirande, 'Cyber warfare and the law of armed conflict' (Research paper, University of Wellington, 2014) 1< https://core.ac.uk/reader/41339676> accessed 1 December 2023

- NATO Cooperative Cyber Defence Centre of Excellence, "National Position of France (2019) - International Cyber Law: Interactive Toolkit" (International cyber law: interactive toolkit, February 13, 2023) <https://cyberlaw.ccdcoe.org/wiki/National_position_of_France_(2019)#cite_note-3> Retrieved December 1, 2023

- Rao SP, "Stuxnet, A New Cyberwar Weapon: Analysis from a Technical Point of

View" (ResearchGate, May 5, 2014) <https://doi.org/10.13140/2.1.1419.5205> Retrieved November 27, 2023

- Smith M and Biller LCJ, "The NotPetya Cyber Operation as a Case Study of International Law" (EJIL: Talk! July 11, 2017) <https://www.ejiltalk.org/the-notpetya-cyber-operation-as-a-case-study-of-international-law/> accessed November 30, 2023

- Sheldon, John B, "Geopolitics and Cyber Power: Why Geography Still Matters," American Foreign Policy Interests 36, issue no. 5 (2014): 286

- United Nations General Assembly (UNGA), Group of Governmental Exerts on Development in the field of Information and Telecommunications in the Context of International Security" (2013) doc A/68/98, 19; <https://documentsddsny.un.org/doc/UNDOC/GEN/N13/371/66/PDF/N337166.pdf?OpenElement> accessed 30 November 2023

List of Statutes

- Declaration Renouncing the Use, in Time of War, of Explosive Projectiles Under 400 Grammes Weight, Saint Petersburg, 29 November/ December 1868

- International Committee of the Red Cross, Geneva Convention for the Amelioration of the Condition of the Wounded and Sick in Armed forces in the Field (1st Geneva Convention) 12 August 1949, 75 UNTS 287

- International Committee of the Red Cross, Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of Non-International Armed Conflicts (Protocol II), 8 June 1977

- International Committee of the Red Cross, Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflict (Protocol I) 8 June 1977

- The United Nations Rome Statute of the International Criminal Court, 2187, U.N.T.S. 90, entered into force July 2, 2002, (Rome Statute)