The International Framework for Cyber-Attacks Under the Rules of International Humanitarian Law

Tareq Al-Billeh [a,*], Jessica Al-Mudanat [a], Abdulaziz Almamari [b], Tawfiq Khashashneh[c], Odai Al-Hailat [d]

[a] Faculty of Law, Applied Science Private University, Amman, Jordan.
[b] Faculty of Law, Al-Zahra College for Women, Muscat, Oman.
[c] Faculty of Law, Ajloun National University, Ajloun, Jordan.
[d] Faculty of Law, Gulf University-Kingdom of Bahrain, Sanad, Bahrain.

*Corresponding Author: t_billeh@asu.edu.jo

ARTICLE INFO

Article history
Received: March 11, 2025
Revised: July 2, 2025
Accepted: July 17, 2025

Keywords
Cyber-Attacks;
Criminal Court;
International Humanitarian Law;
Tallinn Manual;

ABSTRACT

The research paper analyses the extent of enforcement of the rules of international humanitarian law on perpetrators of cyber-attacks by stating the nature of cyber-attacks and identifying the types of cyber-attacks, highlighting international efforts to regulate cyber-attacks under international humanitarian law, deducing the extent of the suitability of the rules of international humanitarian law that govern cyber-attacks, and determining the extent of the jurisdiction of the International Criminal Court to punish perpetrators of cyber-attacks. This study followed the analytical and critical approach by reviewing the rules of international humanitarian law and the extent of their applicability to cyber-attacks. Finally, the study came to a conclusion with a list of results and suggestions. The most important of these is that the way international justice is done needs to change completely so that the International Criminal Court can better handle cybercrimes. This is to ensure that the inclusion of cybercrimes under the jurisdiction of the International Criminal Court aligns with the principles of international humanitarian law, while also highlighting the similarities between cyber weapons and conventional weapons. This is achieved through collaboration between legal and technical experts in addressing the intricacies of cybercrimes, promoting accountability, and bolstering justice in the digital era.

1. Introduction

The remarkable development in technological and technical fields has led to the emergence of many risks to international peace and security, so that cyber-attacks are being committed on a large scale without being restricted to a specific geographical area.[1] In fact, cyber-attacks are seen as one of the most important issues in international humanitarian law. This is because states should not use cyber-attacks that directly or indirectly affect other states and should take all

[1] Ahmad AL-Hawamleh, 'Predictions of Cybersecurity Experts on Future Cyber-Attacks and Related Cybersecurity Measures', *International Journal of Advanced Computer Science and Applications*, 14.2 (2023), 801–809 https://doi.org/10.14569/IJACSA.2023.0140292

possible precautions to avoid these effects.[2] The world has frequently seen fundamental transformations instigated by technological advancement.[3] The advent of the Internet and the rise of artificial intelligence have emerged as predominant trends in contemporary transformations, possessing substantial potential to influence many aspects of life, including military affairs and geopolitical dynamics.[4]

Therefore, cyber-attacks carried out through cyberspace raise many issues regarding the extent of the application of international humanitarian law, so cyberspace should be considered a battlefield when it comes to studying international humanitarian law by identifying some of the main issues arising from the application of the rules of international humanitarian law to cyber-attacks in armed conflicts by targeting dual-use cyber infrastructure and data.[5] Despite the long-standing disregard for this aspect of cyberweapons, there is a growing recognition of its implications for global security. The impact of cyberweapons' transient nature on the deployment incentive structure has been the subject of recent research. Additionally, some academics have focused on how the transient nature of cyberweapons alters the incentives for making investments in these capabilities.[6]

The problem of the study lies in the need for an international organization for cyber-attacks in light of international humanitarian law, so that the weapons used in wars have become cyber weapons instead of conventional weapons. Through this study, we will show the extent to which the rules of international humanitarian law are enforced on perpetrators of cyber-attacks. In fact, Jordan experienced 1297 cyber incidents during the first quarter of 2025, the majority of which were of medium severity, with no high-severity incidents recorded. The percentage of cyber incidents monitored in the first quarter of 2025 decreased by 11% compared to the fourth quarter of last year. Some organizations were subjected to ransom ware attacks, and a number of websites and social media pages impersonating national institutions were monitored. The incidents that occurred in the first quarter of 2025 were distributed according to severity as

---

[2] Giacomo Biggio, 'International Humanitarian Law and the Protection of the Civilian Population in Cyberspace: Towards a Human Dignity-Oriented Interpretation of the Notion of Cyber Attack under Article 49 of Additional Protocol I. The Military Law and the Law of War Review', *Edward Elgar Publishing*, 59.1 (2021), 114–140 https://doi.org/10.4337/mllwr.2021.01.06

[3] Hamzeh abu issa, Mahmoud Ismail, and Omar Aamar, 'Unauthorized access crime in Jordanian law (comparative study)', *Digital Investigation*, 28 (2019), 104-111 https://doi.org/10.1016/j.diin.2019.01.006

[4] Ara Yeremyan and Lilit Yeremyan, 'International Law Issues of Cyber Defense', *Moscow Journal of International Law*, 2 (2022), 85–100 https://doi.org/10.24833/0869-0049-2022-2-85-100

[5] Yuchong Li and Qinghui Liu, 'A Comprehensive Review Study of Cyber-Attacks and Cyber Security; Emerging Trends and Recent Developments', *Energy Reports*, 7 (2021), 8176–8186 https://doi.org/10.1016/j.egyr.2021.08.126

[6] Clara Pettoello-Mantovani, 'Cybercrimes: An Emerging Category of Offenses within the Frame of the International Criminal Court Jurisdiction." International Journal of Law and Politics Studies', *Al-Kindi Center for Research and Development*, 6.2 (2024), 6–11 https://doi.org/10.32996/ijlps.2024.6.2.2

follows: 1% were serious, 76% were medium, and 23% were low.[7] In Oman, the 6th Cyber security Forum, held from May 13-14, 2025, focused on building a network with industry leaders, investors, and potential partners; showcasing products and services at technology exhibitions featuring local and regional entities; exchanging knowledge and expertise with major companies and supporting institutions; promoting and marketing innovations and technological solutions; and seeking financing and investment opportunities for business development and expansion.[8] In Bahrain, the National Cyber security Center participated in the meetings of the Arab Cyber security Ministers Council on May 28, 2025. The meetings addressed the adoption of the annual plan of the Arab Cyber security Ministers Council and discussed Arab topics, initiatives, and priorities aimed at strengthening joint Arab action in the field of cyber security to confront emerging cyber threats at the Arab level.[9]

Recognising the urgent necessity to regulate cyber-attacks through international treaties and agreements currently under negotiation, it is also essential to identify the appropriate international court to adjudicate disputes arising from cyber-attacks and to ascertain whether the International Criminal Court possesses jurisdiction over such disputes.[10] Thus, there are many research papers that have addressed cyber-attacks. Among these studies is a study titled "Putin's power play: Russia's attacks on Ukraine's electric power infrastructure violate international law", which concluded that "International humanitarian law is a part of public international law that tries to keep fights from getting out of hand and protect people who aren't fighting. As a result of international humanitarian law, combatants are not allowed to attack civilians or facilities that are necessary for civilians to stay alive. Attacks that are likely to cause too many civilian deaths, injuries, or damage to civilian property are against international humanitarian law. This is because the direct military advantage expected is not worth the extra harm that will be done to civilians and civilian infrastructure".[11] Another study titled "Cyber operations and automatic hack backs under international law on necessity", which concluded that "Hack backs are a type of active defense strategy implemented in reaction to cybersecurity threats, involving actions that extend outside the victim's systems or networks to minimize or avert the threat.

[7] National Cybersecurity Center, The National Cybersecurity Center Issues its Cybersecurity Posture Report for the First Quarter of 2025. Amman, Jordan https://ncsc.jo/Ar/NewsDetails/Q1_2025_Report_NCSCJO

[8] National Cyber Security Centre, 6th Cybersecurity Forum, Oman, Muscat. https://cert.gov.om/news/270

[9] The National Cybersecurity Center. The National Cybersecurity Center participates in the meetings of the Arab Cybersecurity Ministers Council. Bahrain. https://www.ncsc.gov.bh/en/media-center/news-details

[10] Adasi Nsanawaji Igakuboon, 'An Appraisal of The Legal Framework for The Protection of Civilians in Cyber-Warfare Under International Humanitarian Law', International Journal of Research and Scientific Innovation, 9.7 (2022), 14–26 https://doi.org/10.51244/ijrsi.2022.9702

[11] Julia E Sullivan and Dmitriy Kamensky, 'Putin's Power Play: Russia's Attacks on Ukraine's Electric Power Infrastructure Violate International Law', *The Electricity Journal*, 37.2 (2024), 107371–71 https://doi.org/10.1016/j.tej.2024.107371

Automatic hack backs are systems that, when engaged, can execute certain operations autonomously without direct human intervention. The plea of necessity in international law on State accountability allows States to implement measures that would typically be illegal to counter cyber operations posing a serious and immediate threat to their vital interests".[12] And another study titled "Law in orbit: International legal perspectives on cyber-attacks targeting space systems", which concluded that "Space sector systems facilitate essential operations and are frequently incorporated into current telecommunications infrastructure to improve network connectivity, coverage, and capacity. Although statements from international organizations confirm the relevance of international law to cyber-attacks, the intricacies of cyberspace, along with the distinctive characteristics of space infrastructure, present obstacles to effective application".[13] And another study titled "Cyber-attacks on critical infrastructures and satellite communications", which concluded that "The cyber-attack on the Ukrainian positioning network at the onset of the current Russia-Ukraine conflict illustrated the significant consequences that the branching of satellite lines can impose on communication systems. The transformation of ground-based networks has heightened concerns regarding the susceptibility of vital infrastructure to cyber-attacks and technological malfunctions. Cyber attackers are increasingly focusing on industrial control systems instead of data theft, resulting in more sophisticated and consequential operations".[14]

Another study titled "EU sanctions in response to cyber-attacks as crime-based emergency measures", which concluded that "This study aims to examine the increasing implementation of administrative measures in addressing cybercrimes by studying the particular instance of sanctions imposed in reaction to cyber-attacks. They establish an innovative penalties framework focused on criminal activity, forming the basis for individualized deterrent against hostile cyber actors, and include asset freezes and visa prohibitions. This essay examines the ambiguous distinction between crime-related sanctions as administrative or criminal law actions. The study contends that although crime-based sanctions for cyber-attacks exhibit certain parallels with criminal law measures, they continue to serve as complementary instruments for crime prevention. Their administrative structure

[12] Samuli Haataja, 'Cyber operations and automatic hack backs under international law on necessity', *Computer Law & Security Review*, 53 (2024), 105992 https://doi.org/10.1016/j.clsr.2024.105992

[13] Brianna Bace, Yasir Gökce, and Unal Tatar, 'Law in Orbit: International Legal Perspectives on Cyberattacks Targeting Space Systems', *Telecommunications Policy*, 48.4 (2024), 102739–39, https://doi.org/10.1016/j.telpol.2024.102739

[14] Antonio Carlo and Kim Obergfaell, 'Cyber attacks on critical infrastructures and satellite communications', *International Journal of Critical Infrastructure Protection*, 46 (2024), 100701 https://doi.org/10.1016/j.ijcip.2024.100701

facilitates an emergency reaction to harmful cyber operations that would be impermissible under a more rigorous evidential requirement".[15]

Therefore, our research paper differs from previous papers in that it addresses the extent to which international humanitarian law rules are enforced regarding perpetrators of cyber-attacks. It defines the nature and types of these attacks, focuses on global initiatives to regulate them under international humanitarian law, assesses the applicability of these legal rules to these attacks, and evaluates the jurisdiction of the International Criminal Court to punish their perpetrators. The study's findings indicate a comprehensive shift in the approach to international justice to enable the ICC to address cybercrimes more effectively. This aims to ensure that the inclusion of cybercrimes within the ICC's jurisdiction is consistent with the principles of international humanitarian law, while emphasizing the similarities between cyber weapons and conventional weapons.

Accordingly, this study seeks to explore a series of fundamental legal questions central to the research inquiry. The principal issues examined include the definition and classification of "cyber-attacks" within existing legal frameworks; the applicability of international humanitarian law to cyber-attacks; the legal protections afforded by international humanitarian law in relation to the conduct of cyber-attacks; the jurisdictional scope of the International Criminal Court in prosecuting individuals responsible for cyber-attacks; and the types of criminal sanctions imposed by the International Criminal Court on perpetrators of such acts. The subject of the extent to which the rules of international humanitarian law are enforced on perpetrators of cyber-attacks is a modern and rare subject due to its significant impact on practical reality in light of the increase in cyber-attacks, their destruction of countries' infrastructure, and the serious damage caused to countries as a result of cyber-attacks.

The importance of the study also lies in the difficulty of applying the rules of international humanitarian law to cyber-attacks, as these rules are deficient and do not keep pace with contemporary technological and technical developments, in addition to the lack of international courts specialized in considering cyber-attacks in order to deter and deter perpetrators of cybercrimes. From this standpoint, the importance of the study appears in addressing these cases that are difficult for the international community in order to confront the devastating effects of cyber-attacks. The study aimed to clarify the nature of cyber-attacks, identify the types of cyber-attacks, clarify international efforts to regulate cyber-attacks under international humanitarian law, deduce the extent of the suitability of the rules of international humanitarian law that govern cyber-attacks, and determine the extent

[15] Yuliya Miadzvetskaya, 'EU sanctions in response to cyber-attacks as crime-based emergency measures', *Computer Law & Security Review*, 54 (2024), 106010 https://doi.org/10.1016/j.clsr.2024.106010

of the jurisdiction of the International Criminal Court in punishing perpetrators of cyber-attacks.

2. Research Method

Cyber-attacks encompass a broader scope than what is traditionally defined as information operations. Information operations combine the basic capabilities of electronic warfare, psychological tactics, computer network strategies, military deception, and security operations, along with specialized support and related skills, to influence, disrupt, destroy, or control human decision-making processes within national institutions.[16] Therefore, this study will follow the analytical and comparative approach by reviewing the rules of international humanitarian law and their applicability to cyber-attacks, in addition to analyzing modern international agreements and conventions related to cyber-attacks in order to reach practical solutions to confront the devastating effects of these cyber-attacks.

The study also requires the use of the critical approach by highlighting and commenting on jurisprudential and judicial trends and stating the shortcomings and deficiencies in the rules of international humanitarian law, the jurisdiction of the International Criminal Court, and the researcher's opinion on the extent to which the rules of international humanitarian law are enforced on perpetrators of cyber-attacks, and the extent of the jurisdiction of the International Criminal Court to punish perpetrators of cyber-attacks. The theoretical foundation of this paper is derived from the contributions of academics and international scholars in international law, particularly international humanitarian law, military theorists, international treaties, commentaries on those treaties, and national cyber defense and cybersecurity strategies. The research was conducted using both general and specific scientific methods of cognition, including the dialectical method, comparative legal approach, interpretative method, and methods of deduction, induction, analysis, and synthesis, among others.[17]

3. Results and Discussion

Definition, Classification, and Legal Status of Cyber-Attacks

The use of cyber technologies during armed conflicts poses significant interpretive challenges, such as determining what type of cyber operations can be considered an "attack".[18] The concept of attack is fundamental to the law of targeting, which includes a set of rules that focus on the principles of distinction, proportionality, and precaution, with the aim of reducing the level of violence that

[16] Uche Nnawulezi and Salim Bashir Magashi, 'Evolving Roles of the International Institutions in the Implementation Mechanisms of the Rules of International Humanitarian Law', *Kutafin Law Review*, 9.4 (2022), 684–712 https://doi.org/10.17803/2313-5395.2022.4.22.684-712

[17] Uche Nnawulezi, Kelechi Onyegbule and Charis Godson Ukanwa, 'Evolving Roles of the United Nations Agencies on the Implementation Mechanisms of the Rules of International Humanitarian Law', *The Nigerian Juridical Review*, 16 (2022), 43–63 https://doi.org/10.56284/tnjr.v16i1.12

[18] Craig J. Johnson, Kimberly J. Ferguson-Walter, Robert S. Gutzwiller, Dakota D. Scott and Nancy Cooke, 'Investigating Cyber Attacker Team Cognition', *Proceedings of the Human Factors and Ergonomics Society Annual Meeting*, 66.1 (2022), 105–109 https://doi.org/10.1177/1071181322661132

warring parties can lawfully use on the battlefield.[19] These rules are based on the need to enhance the protection of the dignity of civilians, which is the main goal of contemporary international humanitarian law.[20]

The Convention on Cybercrime does not provide a formal definition for cybercrime. However, looking at cybercrime through the lens of the convention's subsection, we can say that it includes a wide range of criminal offenses, such as those that violate the privacy, integrity, and availability of computer data and systems; computer-related offenses; content-related offenses; and copyright infringement and related rights offenses, all of which are harmful to society.[21] The terminology surrounding computer crime remains inconsistent; some scholars refer to it as "computer abuse," "computer fraud," "computer-related crime," "computer-assisted crime," or simply "computer crime." Ultimately, the term most prevalently utilized is "computer crime," owing to its frequent application in international relations.[22]

Therefore, there are multiple jurisprudential definitions of cyber-attacks. The Australian Federal Police have defined cyber-attacks as crimes directed at computers or information communication technologies, including unauthorized access and attacks on computer networks and the theft of data and information on electronic devices.[23] The cyber warfare episodes in Estonia and Iran serve as tangible case studies for scholars and professionals in the field to inform national and international policy development. In recent years, nations and international organizations recognize the urgency and acknowledge the threats and difficulties that require attention.[24] The Tallinn Manual was created regarding the International Law Applicable to Cyber Warfare, resulting from the efforts of an independent

[19] Wouter Werner, 'Say That Again, Please: Repetition in the Tallinn Manual', *In Repetition and International Law*, (2022), 95–114 https://doi.org/10.1017/9781009039666.005

[20] Loger Kotenko, Elena Fedorchenko, Evgenia Novikova and Ashish Jha, 'Cyber Attacker Profiling for Risk Analysis Based on Machine Learning', *Sensors*, 23.4, (2023) https://doi.org/10.3390/s23042028

[21] Hemen Philip Faga, 'The Implications of Transnational Cyber Threats in International Humanitarian Law: Analysing the Distinction Between Cybercrime, Cyber Attack, and Cyber Warfare in the 21st Century', *Baltic Journal of Law and Politics*, 10.1 (2017), 1-34 https://doi.org/10.1515/bjlp-2017-0001

[22] M. V. Hrushko, 'Attribution Of Cyberattacks As A Prerequisite For Ensuring Responsible Behavior In Cyberspace', *Constitutional State*, 43 (2021), 195–201 https://doi.org/10.18524/2411-2054.2021.43.241002

[23] Amal M. R, and Venkadesh P, 'Hybrid H-DOC: A bait for analyzing cyber attacker behavior', *International Journal of Electrical and Computer Engineering Systems*, 14.1, (2023), 37–44 https://doi.org/10.32985/ijeces.14.1.5

[24] Michael Gervais, 'Cyber Attacks and the Laws of War', *SSRN Electronic Journal*, 1 (2012), 1-45 https://doi.org/10.2139/ssrn.1939615

international expert panel invited by the NATO Cooperative Cyber Defense Centre of Excellence.[25]

Article 92 of the Tallinn Manual 2.0 defines a cyber-attack as "a cyber-operation, whether offensive or defensive, that is reasonably expected to result in injury or death to persons, or damage or destruction of property".[26] This definition is based on Article 49(1) of the First Additional Protocol to the Geneva Conventions of 1949, which states, "Acts of violence against an adversary, whether in the course of attack or defense".[27] A section of legal jurisprudence considers cyber-attacks to be "actions that are primarily aimed at accessing digital data that may belong to a specific person or a specific state, i.e., they are considered sensitive military data and information".[28] Another section of legal jurisprudence defined cyber-attacks as "a set of measures and procedures that a state takes in order to attack enemy information systems with the aim of influencing and damaging them, and at the same time in order to defend the information systems of the attacking state".[29]

As for the US Strategic Command, it defined cyber-attacks as "the adaptation of computer system operations with the aim of preventing opponents from effectively using those systems, in addition to infiltrating information systems, data, and communication networks with the aim of collecting, possessing, and analyzing the data and information they contain".[30] In this sense, the Tallinn Manual 2.0 states that "any cyber operation that amounts to an armed attack in scope and effects is considered a 'use of force' if it is carried out by a state or is otherwise attributable to it." The experts also unanimously concluded that some cyber operations may be serious enough to qualify as an "armed attack" under the Charter.[31]

However, the experts agreed that minor damage does not meet the minimum threshold of damage required. In short, the Tallinn Manual 2.0 does not deny that some cyber operations may be considered armed attacks, leading to an armed

---

[25] Mieke Eoyang, and Chimène Keitner, 'Cybercrime vs. Cyberwar: Paradigms for Addressing Malicious Cyber Activity', *Journal of National Security Law and Policy*, 1 (2020), 1-21 http://dx.doi.org/10.2139/ssrn.3599588

[26] Michael N. Schmitt, 'Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations', Article 92. *Cambridge University Press*, (2017) https://doi.org/10.1017/9781316822524

[27] Article 49(1) of the First Additional Protocol to the Geneva Conventions of 1949. https://www.icrc.org/sites/default/files/external/doc/en/assets/files/other/icrc_002_0321.pdf

[28] Ke Zhen Huang, Yi Feng Lian, Deng Guo Feng, Hai Xia Zhang, Di Wu, and Xiang Liang Ma, 'Method of Cyber Attack Attribution Based on Graph Model', *Ruan Jian Xue Bao/Journal of Software*, 33.2, (2022) 683–698. https://doi.org/10.13328/j.cnki.jos.006314

[29] Yan Zhang, Degang Zhu, Menglin Wang, Junhan Li, and Jie Zhang, 'A comparative study of cyber security intrusion detection in healthcare systems', *International Journal of Critical Infrastructure Protection*, 44. (2024) https://doi.org/10.1016/j.ijcip.2023.100658

[30] Mohammad Hasan Daraji and Omar Saleh AL-Okour, 'Cyber-Attacks in Accordance With International Humanitarian Law', *Dirasat: Shari'a and Law Sciences*, 51.1 (2024), 1-12 https://doi.org/10.35516/law.v51i1.786

[31] Michael N. Schmitt, 'Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations', Article 92. *Cambridge University Press*, (2017) https://doi.org/10.1017/9781316822524

conflict. In compliance with international humanitarian law, Tallinn Manual 2.0 proposes a set of rules to limit the range of legitimate military targets that cyber-attacks can target.[32]

The common understanding of what an attack is in the context of cyberspace isn't very broad, so it can't fully protect civilians from cyber operations that happen during armed conflicts. Therefore, it is proposed to adopt a dignity-based interpretation of the concept of "violence," which is considered the basis for the concept of attack in this context.[33] This interpretation should go beyond mere physical harm to also include serious psychological and economic violence as essential conditions for a cyber-operation to be classified as an "attack".[34] However, using cyber technologies during times of armed conflict brings up important questions about what kinds of cyber operations can be considered an "attack." The rules that govern this include the principles of distinction, proportionality, and precaution, which limit the amount of violence that warring parties are legally allowed to use. These rules aim to enhance the protection of the dignity of civilians, which is the main goal of modern international humanitarian law.[35]

Therefore, it becomes clear to us that cyber-attacks are illegal technical actions, activities, and behaviors based on hacking and unauthorized access to information systems or confidential digital data of a specific party, with the aim of accessing them either to destroy them or to gain information for the benefit of a specific country or even for the purpose of illicit gain.[36] A cyber-attack is a deliberate attempt by a country, individual, or specific party to target the information system of countries. Military and economic motives often drive these attacks, but they can also involve the theft, modification, or destruction of data and information. In other words, the goals of a cyber-attack vary between hacking the electronic system and

[32] Joseph N. Madubuike-Ekwe, 'Cyberattack and the Use of Force in International Law', *Beijing Law Review*, 12.2 (2021), 631–49 https://doi.org/10.4236/blr.2021.122034

[33] Hamzeh Abu Issa and Abdullah Alkhseilat, 'The Cyber Espionage Crimes in the Jordanian Law', *International Journal of Electronic Security and Digital Forensics*, 14.2 (2022), 111-123 https://doi.org/10.1504/ijesdf.2022.121203

[34] Oliver Kessler, and Wouter Werner, 'Expertise, Uncertainty, and International Law: A Study of the Tallinn Manual on Cyberwarfare', *Leiden Journal of International Law*, 26.4 (2013), 793–810 https://doi.org/10.1017/S0922156513000410031

[35] Elaine Fahey, 'The Evolution of EU–US Cybersecurity Law and Policy: On Drivers of Convergence', *Journal of European Integration*, 46.7 (2024), 1073–1088 https://doi.org/10.1080/07036337.2024.2411240

[36] Pritik A. Shah, and Marcos Roberto Tovani-Palone, 'Surgical Care Services in Inaccessible Zones: Targeted Palliative Care Accessibility Models for Patients in Resource-Limited Settings', *The International Journal of Health Planning and* Management, 37.S1 (2022), 243–49 https://doi.org/10.1002/hpm.3580

stealing, modifying, or destroying electronic data or electronic information that belongs to countries.[37]

The contemporary cyber kill chains are becoming progressively intricate. The assailants employ a diverse array of attack vectors to execute cyber-attacks. The European Union Agency for Cyber security defines an attack vector as a method through which a threat agent exploits weaknesses or vulnerabilities in assets to attain a specific objective. For example, one attack vector may signify a public web system with vulnerabilities that can be exploited to reveal a malicious URL.[38] The types of cyber-attacks include sabotaging and misusing electronic information, stealing electronic data, forging and falsifying electronic information, violating privacy by accessing individuals' electronic accounts, electronic eavesdropping, electronic espionage,[39] electronic defamation, illegal entry into networks with the intent to misuse and sabotage electronic information and data, hacking electronic data and information, and cyberterrorism.[40]

From this standpoint, cyber-attacks vary into several forms and actions and are not represented by a single action and include the following: The first type: Cyber espionage: This is when information is obtained illegally, where electronic digital means are used to obtain this information, such that the espionage is carried out by individuals but in a technical manner or via satellites.[41] The second type: Cyber terrorism: This is when certain individuals or entities spread terrorist ideas out of panic or influence the ideas of a certain group of people by using social media or media as a means to spread extremist ideas and convince individuals to join these

[37] Daniel W. Woods and Sezaneh Seymour, 'Evidence-Based Cybersecurity Policy? A Meta-Review of Security Control Effectiveness', *Journal of Cyber Policy*, 8.3 (2024), 1–19 https://doi.org/10.1080/23738871.2024.2335461

[38] Fernando J. Rendón-Segador, Juan A. Álvarez-García, and Angel Jesús Varela-Vaca, 'Paying Attention to Cyber-Attacks: A Multi-Layer Perceptron with Self-Attention Mechanism', *Computers and Security*, 132 (2023), 103318 https://doi.org/10.1016/j.cose.2023.103318

[39] John C. Richardson, 'Stuxnet as Cyberwarfare: Applying the Law of War to the Virtual Battlefield', *SSRN Electronic Journal*, 1 (2012), 1-38 https://doi.org/10.2139/ssrn.1892888

[40] B. Pratama and M. Bamatraf, 'Tallinn Manual: Cyber Warfare in Indonesian Regulation', *In IOP Conference Series: Earth and Environmental Science*, 729 (2021), 1-8 https://doi.org/10.1088/1755-1315/729/1/012033

[41] Noor Al-Khawajah, Tareq Al-Billeh, and Majd Manasra, 'Digital Forensic Challenges in Jordanian Cybercrime Law', *Pakistan Journal of Criminology*, 15.3 (2023), 29-44. https://www.pjcriminology.com/publications/digital-forensic-challenges-in-jordanian-cybercrime-law/

groups.[42] The third type: Cyber wars: Where the parties plan to fight and determine the targets that will be attacked via cyberspace.[43]

The Tallinn Manual 1.0 emphasizes cyber-to-cyber operations, including those targeting a nation's critical infrastructure or cyber-attacks aimed at system control by adversaries. The Tallinn Manual does not address legal matters of kinetic-to-cyber actions, such as an airstrike targeting a cyber-control center, which are governed by the regulations of armed conflict.[44] The Tallinn Manual 1.0 does not cater to the common perception of cybersecurity. Cyber espionage, intellectual property theft, and criminal activities in cyberspace, while significant concerns for the state, are excluded from the regulatory framework of the Tallinn Manual 1.0.[45] The Tallinn Manual 1.0 uses treaties, court cases, and other sources to come up with 95 (ninety-five) black-letter rules that countries involved in cyberwarfare can use as guidance. These rules cover cyber operations in neutral territories.[46]

The Relevance of International Humanitarian Law in Cyber-Attacks

In the contemporary era, States actively conduct the majority of their economic, commercial, cultural, social, and governmental activities and interactions at various levels, involving individuals, non-governmental organizations, and government institutions, within cyberspace.[47] In numerous cyber-attacks, human behavioral factors and reactions to harmful stimuli constitute the most vulnerable link in facilitating a successful breach. Behaviors including distraction, negligence,

[42] Mohammed Al Makhmari, Ali Al-Hammouri, Tareq Al-Billeh and Abdulaziz Almamari, 'Criminal Liability for Misuse of Social Media in Omani and UAE Legislation', International Journal of Cyber Criminology, 18.2 (2024) 92-106 https://cybercrimejournal.com/menuscript/index.php/cybercrimejournal/article/view/420/121

[43] Papawadee Tanodomdej, 'The Tallinn Manuals and the Making of the International Law on Cyber Operations', *Masaryk University Journal of Law and Technology*, 13.1 (2019), 67–85 https://doi.org/10.5817/MUJLT2019-1-4

[44] Tawfiq Khashashneh, Tareq Al-Billeh, Ali Al-Hammouri, and Roua Belghit, 'The Importance of Digital Technology in Extracting Electronic Evidence: How Can Digital Technology be used at Crime Scenes?', *Pakistan Journal of Criminology*, 15.4 (2023), 69-85 https://www.pjcriminology.com/publications/the-importance-of-digital-technology-in-extracting-electronic-evidence-how-can-digital-technology-be-used-at-crime-scenes/

[45] Dan Efrony, and Yuval Shany, 'A Rule Book on the Shelf? Tallinn Manual 2.0 on Cyberoperations and Subsequent State Practice', *American Journal of International Law*, 112.4 (2018), 583–657 https://doi.org/10.1017/ajil.2018.86

[46] Kubo Maˇc´ak, 'INTERNATIONAL LAW AND PRACTICE From Cyber Norms to Cyber Rules: Re-Engaging States as Law-Makers', *Leiden Journal of International Law*, 30 (2020), 877–899 https://doi.org/10.1017/S0922156517000358

[47] Ebru Oğurlu, 'International Law in Cyberspace: An Evaluation of the Tallinn Manuals', *Annales de La Faculte de Droit d'Istanbul*, 73 (2023), 327–44 https://doi.org/10.26650/annales.2023.73.0010

curiosity, noncompliance with security policies, and insufficient awareness of cyber dangers can result in significant harm or perhaps facilitate an attack.[48]

Therefore, many states around the world face challenges related to cyber-attacks and risks associated with wireless communication technologies.[49] Today's world is highly dependent on digital technology, which makes protecting data from cyber-attacks a complex issue. These attacks usually aim to cause financial harm to states around the world and may have military or political purposes.[50] From this standpoint, the experts of the Tallinn Manual 2.0 unanimously agreed that some cyber operations may be serious enough to be classified as hostile acts under the concept of the UN Charter. It was therefore concluded that the right to use force in self-defense extends to those armed attacks carried out through cyber operations, even if they do not require the use of conventional weapons.[51]

In this manual, a high threshold has been set for cyber operations that can be considered an armed attack. For example, the experts noted that "there is general agreement that cyber operations that merely cause inconvenience or irritation to the civilian population do not amount to an attack".[52] In addition, the following activities in cyberspace are not considered armed attacks: "electronic intelligence, electronic collection and theft, as well as cyber operations involving short or periodic interruption of nonessential electronic services".[53] Prior to the implementation of the Tallinn Manual 2.0, there were several unresolved issues resulting from divisions between states' positions and practices regarding the definition of "damage or destruction of objects." The first issue concerns whether

[48] Faisal Quader, and Vandana P. Janeja, 'Insights into Organizational Security Readiness: Lessons Learned from Cyber-Attack Case Studies', *Journal of Cybersecurity and Privacy*, 1.4 (2021), 638-659 https://doi.org/10.3390/jcp1040032

[49] Tareq Al-Billeh, Abdullah Alkhseilat, and Lana AL-Khalaileh, 'Scope of Penalties of Offences in Jordanian Public Office', *Pakistan Journal of Criminology*, 15.2 (2023), 341-356 https://www.pjcriminology.com/publications/scope-of-penalties-of-offences-in-jordanian-public-office/

[50] Iradhati Zahra and Diajeng Wulan Christianti. 'The Beginning of the International Humanitarian Law Application to Cyber Attack: The Status Of Rule 30 Tallinn Manual 1.0.', *Padjadjaran Journal of International Law*, 5.1 (2021), 98–113 https://doi.org/10.23920/pjil.v5i1.366

[51] Wanshu Cong, 'Seeking Customary International Human Rights Law in the Cyberspace: A Critique of the Tallinn Manual 2.0.', *SSRN Electronic Journal*, 1 (2021), 1-20 https://doi.org/10.2139/ssrn.3744924

[52] Iradhati Zahra, Irawati Handayani, and Diajeng Wulan Christianti. 'Cyber-Attack in Estonia: A New Challenge in the Applicability of International Humanitarian Law', *Yustisia Jurnal Hukum*, 10.1 (2021), 48-66 https://doi.org/10.20961/yustisia.v10i1.48336

[53] Chih Hsiang Chang, 'How Does the Tallinn Manual 2.0 Shed Light on the Threat of Cyber Attacks against Taiwan-', *In European Conference on Information Warfare and Security*, 1 (2023), 649–656 https://doi.org/10.34190/eccws.22.1.1294

"interference by cyber means with the functionality of an object" is considered "damage or destruction of objects".[54]

Experts were widely divided on this issue. The majority insisted that it constituted harm only when restoring functionality required replacing physical components. Some people in the majority took a second opinion, saying that this kind of interference could mean that the operating system or some data had to be reinstalled in order for the targeted cyber infrastructure to work again. A third position, taken by a small number of experts, considered that the loss of the usability of the cyber infrastructure constituted harm that could be considered a cyber-attack if the infrastructure in question was the target.[55] The second controversial issue was whether data was considered an "object", on which experts differed widely. Most experts said that data was not something that could be touched, so it wasn't an object in the usual sense of the word. This was different from how the term was interpreted in the 1987 Commentary to the Additional Protocols of the International Committee of the Red Cross. In contrast, a minority of experts believed that some data should be considered an object for the purposes of targeting. The view of this small group is based on Article 52 of Additional Protocol I to the 1949 Geneva Conventions. This section says that "the severity of the consequences of the operation" should be the most important thing, not the type of damage.[56]

In relation to the protections afforded by international humanitarian law in the event of cyber-attacks, it is essential to refer to Common Article 2 of the 1949 Geneva Conventions and the accompanying commentary provided by the International Committee of the Red Cross. This provision establishes that an international armed conflict exists whenever there is recourse to armed force between two States. Conversely, the threshold for determining the existence of a non-international armed conflict is significantly higher. Common Article 3 applies to "a conflict not of an international character occurring in the territory of a High Contracting Party"; however, it does not offer a precise or comprehensive definition of such conflicts.[57] However, the International Criminal Tribunal for the

---

[54] Pauline Charlotte Janssens, and Jan Wouters, 'Informal International Law-Making: *A Way around the Deadlock of International Humanitarian Law?', International* Review of the Red Cross, 104.920–921 (2022), 2111–2130. https://doi.org/10.1017/S1816383122000467

[55] Khalil Akbariavaz, Pardis Moslemzadeh Tehrani, and Johan Shamsuddin bin Haj Sabaruddin. 'Cyberattacks and the Prohibition of the Use of Force under Humanitarian Law with Reference to the Tallinn Manual', *In European Conference on Information Warfare and Security*, 1 (2020), 451–457. https://doi.org/10.34190/EWS.20.508

[56] Helaine Leggat, 'Cyber Warfare: An Enquiry into the Applicability of National Law to Cyberspace', *International Journal of Cyber Warfare and Terrorism*, 10.3 (2020), 28–46 https://doi.org/10.4018/IJCWT.2020070103

[57] Eric A. Heinze, and Rhiannon Neilsen, 'Limited Force and the Return of Reprisals in the Law of Armed Conflict', *Ethics and International Affairs*, 34.2 (2020), 175-188 https://doi.org/10.1017/S0892679420000246

former Yugoslavia has provided a criterion in the Tadić judgment, which requires two conditions: (a) ongoing armed violence between government authorities and organized armed groups, or (b) between such groups within a given state. Regarding cyber operations, the Tallinn Manual 2.0 states that "cyber operations conducted in the context of an armed conflict are subject to the law of armed conflict".[58]

For the law of armed conflict to apply to cyber operations, two conditions must be met: the presence of cyber activities and a clear link between those activities and an armed conflict. The definitions of international and non-international cyber armed conflicts, as outlined in Rules 82 and 83, should align with the principles of the 1949 Geneva Conventions' Common Articles and the standards set by the Tadić judgment.[59] According to the Tallinn Manual 2.0, there is still a divergence of expert opinion on the status of national hackers. While the majority agreed that civilians retain their civilian status even if they directly participate in cyber hostilities, they may become lawful targets. Thus, unless they qualify as collective participants in an attack, they will not enjoy combatant immunity for their actions.[60] In addition, a minority of experts rejected the idea that such individuals could benefit from the protection of the Third or Fourth Geneva Conventions, as they are neither combatants nor civilians.[61]

In the cyber context, a similar problem arises regarding the threshold of non-international armed conflict. The experts in the Tallinn Manual 2.0 noted that "the precise criteria for 'in the context of' are less clear in non-international armed conflict," because "a state retains certain law enforcement obligations and rights in relation to its territory, even in armed conflict".[62] Ongoing uncertainty regarding whether certain cyber operations qualify as cyber-attacks raises important questions about their conformity with the threshold of an armed attack as defined under Article 51 of the United Nations Charter.[63]

---

[58] Sergei Yu Garkusha-Bozhko, 'The Definition of Armed Conflict in Cyberspace' *Vestnik Sankt-Peterburgskogo Universiteta. Pravo*, 14.1 (2023), 194–210 https://doi.org/10.21638/spbu14.2023.112

[59] Johannes Thumfart, 'Public and Private Just Wars: Distributed Cyber Deterrence Based on Vitoria and Grotius', *Internet Policy Review*, 9.3 (2020), 1–26 https://doi.org/10.14763/2020.3.1500

[60] Abdullah Alkhseilat, Naser Al Ali, and Lujain Edweidar, 'Legal Regulation of Impersonation through Websites', *International Journal of Electronic Security and Digital Forensics*, 16.5 (2024), 557–576, https://doi.org/10.1504/ijesdf.2024.140748

[61] Maxron Holder, 'Cyberspace in a State of Flux: Regulating Cyberspace through International Law', *Groningen Journal of International Law*, 9.2 (2022), 266–280 https://doi.org/10.21827/grojil.9.2.266-280

[62] Roberta Arnold, 'The Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations, Edited by Michael N. Schmitt', *International Criminal Law Review*, 20.1 (2020), 155–159 https://doi.org/10.1163/15718123-02001008

[63] Sergei Yu Garkusha-Bozhko, 'The Problem of Cyber Espionage in the International Humanitarian Law', *Moscow Journal of International Law*, 1 (2021), 70–80 https://doi.org/10.24833/0869-0049-2021-1-70-80

The increasing frequency of cyber-attacks perpetrated by states or with their endorsement underscores the necessity for legal attribution to establish international accountability.[64] The Tallinn Manual, which contains authoritative conclusions regarding the application of attribution principles, raises significant concerns about the feasibility of establishing attribution.[65] The primary cause of this issue lies in the characteristics of cyberspace, which include anonymity, spoofing, and targeting from foreign territories.[66] The Tallinn Manual restates the provisions of ARSIWA and does not demonstrate the presence of Lex Specialis for the attribution of cyber-attacks.[67] Accordingly, states bear accountability for the actions of their de facto and de jure organs authorized to perform governmental functions, private entities under their effective control, or for breaches of due diligence obligations.[68]

Therefore, some countries have adopted internal regulations to protect against cyber-attacks. The National Cybersecurity Council in Jordan approved the National Cybersecurity Strategy for 2025-2028, a comprehensive national plan that supports the efforts of the Hashemite Kingdom of Jordan, through the National Cybersecurity Center, to build an effective national cybersecurity system. The National Cybersecurity Center will work in partnership with relevant national authorities to prepare the strategy's executive program and monitor the implementation of all related programs and activities according to specific timeframes and performance indicators. The strategy includes the Hashemite Kingdom of Jordan's vision for building a secure, reliable, and resilient Jordanian cyberspace, relying on national capabilities and enhancing the economy and well-being. This strategy works to achieve this vision through four main strategic objectives and fourteen sub-objectives within clear priorities that adopt programs, projects, and initiatives that achieve the strategic objectives. These objectives are: security and trust through data protection and fortifying digital infrastructure and services; resilience and steadfastness to ensure the continuity of services in the face of cyber threats; capacity building, developing local skills, and supporting scientific research; investing in modern technology to bridge the knowledge gap; and cooperation and partnerships to enhance local and international cooperation and exchange of expertise to address growing cyber challenges. The National

[64] Herbert Lin, 'Cyber Conflict and International Humanitarian Law', *International Review of the Red Cross*, 94.886 (2013), 515–531 https://doi.org/10.1017/S1816383112000811

[65] Colin Sweet, 'Tallinn Manual on the International Law Applicable to Cyber Warfare', *Europe-Asia Studies*, 66.4 (2014), 669–670. https://doi.org/10.1080/09668136.2014.897423

[66] Hazrat Usman, Raja Ishtiaq Ahmed, and Syed Suliman Ali. 'Navigating the Gray Area: A Comprehensive Analysis of Cyber Warfare and Its Relationship to the Law of Armed Conflict', *Global Legal Studies Review*, 7.3 (2022), 32–36 https://doi.org/10.31703/glsr.2022(vii-iii).05

[67] Ian Yuying Liu, 'The Due Diligence Doctrine under Tallinn Manual 2.0.', *Computer Law and Security Review*, 33.3 (2017), 390–395 https://doi.org/10.1016/j.clsr.2017.03.023

[68] Viktoriia Muzyka, 'New Wine in Old Bottles: Applicability of the Rules on Attribution to Cyberattacks Committed against Objects of Critical Infrastructure', *Law Review of Kyiv University of Law*, 3 (2020), 388–391 https://doi.org/10.36695/2219-5521.3.2020.72

Cybersecurity Strategy seeks to position Jordan as a distinguished regional center in the field of cybersecurity. It also seeks to secure Jordanian cyberspace by creating a safe digital environment that encourages innovation and leadership, attracts global companies to invest in cybersecurity, and supports the vision of economic modernization and digital transformation.[69]

In Oman, within the framework of Oman Vision 2040, a spotlight has been placed on the development of start-ups and small enterprises to achieve their goals, which rely on biodiversity, diversity, and innovation. This trend stems from the digital environment's drive for entrepreneurship and contributes to transforming the Sultanate into a hub for technology and innovation. One of the most important digital business programs supporting this is its focus on the cyber environment, emphasizing the importance of developing small startups in the field of cybersecurity.[70]

In Bahrain, the National Cyber Security Centre announced on April 27, 2025, the signing of a cooperation agreement with the British OSP Cyber Academy. This agreement is part of a partnership with "Faalyat" to host the British pavilion at the third edition of the Arab International Cybersecurity Conference and Exhibition, one of the most prominent cybersecurity events in the region. Both parties are keen to invest in the fields of digital transformation, cybersecurity, and e-learning. This cooperation includes the signing of an agreement to develop a comprehensive, interactive e-curriculum targeting all educational levels in the Kingdom of Bahrain. The curriculum will address topics related to cybersecurity and digital citizenship, with the aim of enhancing digital awareness among students and developing their cyber skills in line with the Kingdom of Bahrain's vision to create a digital society and a safe cyberspace. This comes within the framework of a shared commitment to promoting a safe digital environment and expanding public-private partnerships, opening new horizons for educational initiatives and sustainable cyber policies. The agreement seeks to enhance international cooperation in the field of cybersecurity, with a focus on developing the skills of future generations in this vital security field. It also aims to raise awareness of cyber risks and educate young people on how to protect themselves from growing online threats, a step that affirms the Kingdom of Bahrain's commitment to achieving sustainable progress in the field of cybersecurity. This cooperation comes as part of the National Cybersecurity Centre's efforts to provide a distinguished educational and training environment that keeps pace with the latest developments in the field of

[69] National Cybersecurity Center, Approval of the National Cybersecurity Strategy 2025-2028. Amman, Jordan https://ncsc.jo/Ar/NewsDetails/National_CS_Strategy_2025_2028
[70] National Cyber Security Centre, National Cybersecurity Products and Services Guide for 2025, Oman, Muscat. https://cert.gov.om//librarys/publications/servicesGuideline.pdf

digital protection and enhances the ability of individuals and institutions to confront future challenges.[71]

Recently, certain nations have executed global cyber-attacks that not only inflict damage on industrial systems and infrastructure but also serve as information warfare, targeting social networking services and other media, thereby influencing electoral outcomes and democratic processes and posing a significant threat to democracy. Consequently, this action is classified as "disinformation".[72]

The Jurisdiction of the International Criminal Court over Cyber-Attacks

The principle of a state's right to self-defense crystallized within the framework of customary international law after the Caroline incident, and the rules relating to the exercise of this right were set out in Article 51 of the UN Charter.[73] While Article 2(4) categorically prohibits "the threat or use of force in international relations", Article 51 represents one of the rare exceptions that allows a state to lawfully use force. This exception is explicitly invoked when a UN member state is subjected to an "armed attack", which is considered a serious violation of Article 2(4)'s prohibition on the use of force, and was clearly distinguished from the term "use of force" in the International Court of Justice's ruling in the Nicaragua case.[74]

Cyber-attacks yield results akin to conventional assaults, resulting in substantial loss and material destruction, and may be classified as prosecutable offenses before the ICC, including genocide, crimes against humanity, war crimes, and the crime of aggression.[75] Nonetheless, there are restrictions concerning cyber-attack offenses, including the possible challenge of connecting the actions to a specific perpetrator through admissible evidence that meets the standard of proof beyond a reasonable doubt.[76] Technological and technical developments therefore require the world's countries to have a comprehensive legal vision and to adapt laws to suit changing social contexts and new criminal methods, especially in the field of technology,

---

[71] The National Cybersecurity Center. Cybersecurity: Bahraini-UK partnership to enhance international cooperation and build cyber capabilities. Bahrain. https://www.ncsc.gov.bh/ar/media-center/news-details.html?src=

[72] Tomoko Nagasako, 'A Consideration of the Case Study of Disinformation and Its Legal Problems', *In IFIP Advances in Information and Communication Technology*, 590 (2020), 262–276 https://doi.org/10.1007/978-3-030-62803-1_21

[73] Article 51 of the UN Charter. https://www.un.org/en/about-us/un-charter

[74] Steven Wheatley, 'Election Hacking, the Rule of Sovereignty, and Deductive Reasoning in Customary International Law', *Leiden Journal of International Law*, 36.3 (2023), 675–698 https://doi.org/10.1017/S0922156523000092

[75] Abdullah Alkhseilat, Tareq Al Billeh, Mohammed Albazi, and Naser Al Ali, 'The Authenticity of Digital Evidence in Criminal Courts: A Comparative Study', *International Journal of Electronic Security and Digital Forensics*, 16.6 (2024), 720–738 https://doi.org/10.1504/ijesdf.2024.142010

[76] Jennifer Trahan, 'The Criminalization of Cyber-Operations Under the Rome Statute', *Journal of International Criminal Justice*, 19.5 (2021), 1133–1164 https://doi.org/10.1093/jicj/mqab066

including information technology and artificial intelligence.[77] The great advances in modern technologies have led to the emergence of new forms of aggression, targeting not only traditional legal assets but also individuals skilled in advanced technology, so that the term "cyber-attacks" has emerged on the international scene, which raises questions about possible classifications within international legal frameworks.[78]

The role of cyber operations in armed conflict has grown in importance. Therefore, it is important to make clear whether cyber-attacks on data during armed conflict could qualify as war crimes under the International Criminal Court's Statute.[79] There is no legal or doctrinal agreement on whether it is legitimate to include computer data in the Statute's "things" and "property" categories. The Court may, however, take a broad stance on situations in which attacks on or through data have a legally significant impact on tangible items. Whether the Statute will be able to "keep pace" with emerging forms of conflict in the context of the legality principle.[80] In fact, recent global conflicts highlight the possibility of classifying cyber-attacks on critical infrastructure as war crimes or acts of aggression, prompting the International Criminal Court to consider including cybercrimes within its core jurisdiction.[81] Although current agreements lack normative references, the Martens Clause emphasizes the need to consider attacks using technology (cyber-attacks) as equivalent to conventional means.[82]

Article 51 of the UN Charter indicates that cyber weapons can be considered equivalent to conventional weapons under international law. The article emphasizes the importance of advanced education and training for legal personnel skilled in identifying perpetrators of cybercrimes so that the International Criminal Court seeks to train individuals with the legal and technical expertise necessary for effective responses to cybersecurity.[83] This highlights the challenges in

---

[77] Tareq Al-Billeh, Ruba Hmaidan, Ali Al-Hammouri, and Mohammed AL Makhmari, 'The Risks of Using Artificial Intelligence on Privacy and Human Rights: Unifying Global Standards', *Jurnal Media Hukum*, 31.2 (2024), 333–350 https://doi.org/10.18196/jmh.v31i2.23480

[78] Georgia Beatty, 'War Crimes in Cyberspace: Prosecuting Disruptive Cyber Operations under Article 8 of the Rome Statute', *The Military Law and the Law of War Review*, 58.2 (2020), 209–239 https://doi.org/10.4337/mllwr.2020.02.17

[79] Michael Schmitt, 'Classification of Cyber Conflict', *Journal of Conflict and Security Law*, 17.2 (2012), 245–260 https://doi.org/10.1093/jcsl/krs018

[80] Simon McKenzie, 'Cyber Operations against Civilian Data', *Journal of International Criminal Justice*, 19.5 (2022), 1165–1192. https://doi.org/10.1093/jicj/mqab067

[81] Kosmas Pipyros, Christos Thraskias, Lilian Mitrou, Dimitris Gritzalis, and Theodoros Apostolopoulos, 'A New Strategy for Improving Cyber-Attacks Evaluation in the Context of Tallinn Manual', *Computers and Security*, 74 (2018), 371–383. https://doi.org/10.1016/j.cose.2017.04.007

[82] Tainyi LUOR, Jen Fu WANG, and Hsi-Peng LU, 'Trends in and Contributions to Tallinn Manual Research: An Assessment of the Literature from 1998 to November 2022', *Informatica Economica*, 27.3 (2023), 45–60 https://doi.org/10.24818/issn14531305/27.3.2023.04

[83] Article 51 of the UN Charter. https://www.un.org/en/about-us/un-charter

conceptualizing and classifying cybercrimes within existing legal frameworks. From this point of view, the place where law and technology meet needs to have legal and technical experts who can work together without any problems. They need to understand how complicated cyberspace is and how cyber threats can affect the safety and stability of the whole world.[84]

Therefore, the need for a radical shift in the approach to international justice requires recognizing the necessary evolution of the International Criminal Court in confronting cybercrimes. The inclusion of cybercrimes within the jurisdiction of the International Criminal Court must be consistent with the principles of international humanitarian law, while emphasizing that cyber weapons are equivalent to conventional weapons.[85] Collaboration between legal and technical experts is also vital to address the complexities of cybercrimes, ensure accountability, and promote justice in the digital age, in addition to highlighting the proactive role played by the International Criminal Court in shaping the future of global justice in light of the increasing cyber threats.[86]

As for the criminal sanctions imposed by the International Criminal Court on perpetrators of cyber-attacks, the changing nature of cyber threats requires a proactive approach, including anticipating future challenges and adapting legal frameworks, so that the Criminal Court must be able to stay ahead of developments in an environment where technology is evolving at an unprecedented speed by understanding the complexities of cybercrimes, accurately identifying perpetrators, and ensuring accountability within the framework of international law.[87]

Thus, given recent global conflicts, it is evident that prospective cyber-attacks on essential strategic infrastructure and non-military civilian targets may constitute war crimes and/or acts of aggression.[88] Consequently, it is imperative for the ICC to incorporate the analysis and investigation of growing legal concerns pertaining to

---

[84] Cesáreo Gutiérrez Espada, 'The Growing Need for Legislation against Cyber Threats, Sources of Serious Transnational Harm', *Cuadernos de Derecho Transnacional*, 14.2 (2022), 10–14 https://doi.org/10.20318/cdt.2022.7169

[85] Tareq Al-Billeh, Ali Al-Hammouri, Tawfiq Khashashneh, Mohammed AL Makhmari, and Hamad Al Kalbani, 'Digital Evidence in Human Rights Violations and International Criminal Justice', *Journal of Human Rights Culture and Legal System*, 4.3 (2024), 842–871 https://doi.org/10.53955/jhcls.v4i3.446

[86] Jakub Spáčil, 'Cyber Operations against Critical Financial Infrastructure: A Non-Destructive Armed Attack?', *International and Comparative Law Review*, 22.2 (2022), 27–42 https://doi.org/10.2478/iclr-2022-0013

[87] Jasper Schellekens, 'Release the Bots of War: Social Media and Artificial Intelligence as International Cyber Attack', *Przegląd Europejski*, 4 (2021), 163–179 https://doi.org/10.31338/1641-2478pe.4.21.10

[88] Serhii Drobotov, Roman Pertsev, Mariia Hrab, Vasyl Fedytnyk, Svitlana Moroz, and Mariia Kikalishvili, 'Forensic Research of the Computer Tools and Systems in the Fight against Cybercrime', *Journal of Information Technology Management*, 15.1 (2023), 135–62 https://doi.org/10.22059/jitm.2023.90741

"cybercrime" into its fundamental interests and evolving purposes. This method seems to align with the range of offenses under the ICC's jurisdiction, as specified in Article 2/5 of its Statute.[89]

In fact, cybercrimes often transcend national borders, which necessitates international cooperation, so the International Criminal Court relies on coordination with national authorities, law enforcement agencies, and technology experts from different countries.[90] Therefore, providing adequate funding is not only limited to improving equipment and technological infrastructure but is also vital to establishing and maintaining partnerships, facilitating the exchange of information, and coordinating efforts on a global level.[91] Therefore, the International Criminal Court takes into account several factors when determining the appropriate penalty for a convicted person according to the rules of procedure and evidence. Among these factors, the total penalty of imprisonment and a fine must be proportionate to the crime committed.[92] The court must also take into account the nature of the unlawful conduct, the means used to commit the crime, the extent of the convict's participation, the intent and circumstances of time and place, and the convict's age and social status.[93]

Chapter VII of the Statute of the International Criminal Court spells out the punishments that will be given to people who commit international crimes. This clearly aims to deal with the problem of international crime and try to lower it. These penalties include imprisonment for a period of up to thirty years. Life imprisonment. The court may also impose other types of penalties, which include imposing a financial fine in accordance with the rules of procedure and evidence. The court may also confiscate proceeds, property, and funds resulting directly or indirectly from the crime, while preserving the rights of other parties acting in good faith.[94]

However, the International Criminal Court has been called upon to respond to Russia's deployment of offensive cyber activities to support its illegal war against

---

[89] Article 2/5, of the Statute of the International Criminal Court. July 17, 1998. https://www.icc-cpi.int/sites/default/files/2025-02/Rome-Statute-EN-2025.pdf

[90] Dan-Iulian Voitasec, 'Applying International Humanitarian Law to Cyber Attacks', *Lex ET Scientia International Journal*, 22.Xxii (2015), 552–556. http://www.icj-cij.org/docket/files/70/6503.pdf

[91] Yaxuan Leng, 'When Can Cyberattack Constitute Use of Force: A Case Study of Cyberattack in the Russia-Ukraine Conflict', *Lecture Notes in Education Psychology and Public Media*, 17.1 (2023), 201–7 https://doi.org/10.54254/2753-7048/17/20231249

[92] Vanshika Shukla, 'A BRIEF STUDY OF INTERNATIONAL LAW IN THE AGE OF CYBERSECURITY', *EPRA International Journal of Multidisciplinary Research (IJMR)*, 9.11 (2023), 269–273 https://doi.org/10.36713/epra14915

[93] Petro Protas, and Leornard Chimanda Joseph, 'The Law of Armed Conflict in the Era of Cyber Technology: Assessing the Legal Challenges and Response in Tanzania', *Eastern Africa Law Review*, 47.1 (2020), 95–139 https://doi.org/10.56279/ealr.v47i1.4

[94] Chapter VII of the Statute of the International Criminal Court. July 17, 1998. https://www.icc-cpi.int/sites/default/files/2025-02/Rome-Statute-EN-2025.pdf

Ukraine. However, because cyber operations fit awkwardly into the conventional war crimes legal framework, the International Criminal Court is an unsuitable venue for deciding cyber conduct in armed conflict.[95] Furthermore, the types of cyber behavior that could be considered war crimes and against which the Prosecutor of the International Criminal Court could successfully file a case are strictly limited by the Rome Statute's rigorous substantive and procedural characteristics.[96] The Rome Statute's established framework of international humanitarian law does not fully control the particular domain in which cyber operations take place because the majority of cyber conduct does not result in kinetic impacts.[97]

Consequently, the dynamic nature of cyber risks necessitates a proactive strategy, anticipating forthcoming difficulties and adjusting regulatory frameworks accordingly. The International Criminal Court must evolve into a dynamic institution, adept at anticipating developments in a world characterized by rapid technological advancement.[98] Educational and training programs must concentrate on developing a cohort of specialists capable of deciphering the complexities of cybercrimes, pinpointing individual offenders, and enforcing accountability in accordance with international law.[99]

4. Conclusion

The study paper illustrated the enforcement of international humanitarian law on cyber-attack offenders and elucidated the contemporary international ramifications of cyber weapons by defining cyber-attacks and their classifications. It underscored the difficulties in applying international humanitarian law to cyber-attack perpetrators, assessed the appropriateness of existing international humanitarian law regarding cyber-attacks, and illustrated the protections afforded by international humanitarian law in the context of such attacks. It also elucidated the function of international criminal justice in sanctioning perpetrators of cyber-attacks, detailing the jurisdictional scope of the International Criminal Court in

[95] Steven Kleemann, 'Cyber Warfare and the 'Humanization' of International Humanitarian Law', *International Journal of Cyber Warfare and Terrorism*, 11.2 (2021), 1–11. https://doi.org/10.4018/IJCWT.2021040101

[96] Nataliia Mazaraki, and Yulia Goncharova, 'CYBER DIMENSION OF HYBRID WARS: ESCAPING A 'GREY ZONE' OF INTERNATIONAL LAW TO ADRESS ECONOMIC DAMAGES', *Baltic Journal of Economic Studies*, 8.2 (2022), 115–120 https://doi.org/10.30525/2256-0742/2022-8-2-115-120

[97] Zachary R. Orr, 'Redress for Unlawful Cyber-Attacks During Armed Conflict: The Limits of the International Criminal Court and How Human Rights Bodies Can Help Close the Gap', *SSRN Electronic Journal*, 57.359 (2023), 359-410 https://doi.org/10.2139/ssrn.4422358

[98] Mara Tignino, 'The Regulation of Crimes against Water in Armed Conflicts and Other Situations of Violence', *International Review of the Red Cross*, 105.923 (2023), 706–734 https://doi.org/10.1017/S1816383123000061

[99] Ashraful Mozid, and Nelufer Yesmen, 'Term Paper on The Nature of Cyber Crime and Cyber Threats: A Criminological Review', *Journal of Advanced Forensic Sciences*, 1.1 (2020), 1–9 https://doi.org/10.14302/issn.2692-5915.jafs-20-3204

addressing such offences and the punitive measures enforced by the Court against these offenders. In fact, the great boom in Internet networks has led to a significant increase in cyber-attack incidents, which often have dire consequences. Malware is considered a common tool used to carry out these attacks in cyberspace. Cyber attackers either exploit existing vulnerabilities or take advantage of the unique characteristics of modern technologies. The nature of cyber-attacks often requires advanced technological techniques and methods to be able to investigate and prosecute cybercrimes. Therefore, the International Criminal Court needs advanced technical tools and technological infrastructure so that it does not hinder the effectiveness of its work. The cybersecurity community must enhance its knowledge of the types of cyber-attacks and their tools, in addition to the need to take effective security measures to confront these threats. Advanced and effective defense mechanisms must also be developed to combat malware. Finally, a fundamental shift in the approach of international justice is necessary by recognizing the inevitable evolution of the International Criminal Court in addressing cybercrimes. Including cybercrime in the International Criminal Court's jurisdiction is in line with international humanitarian law. It also stresses that cyber weapons are the same as regular weapons by getting legal and technical experts to work together to handle the complexities of cybercrime, make sure people are held accountable, and support justice in the digital age.

Refrences

Abu Issa, Hamzeh, and Abdullah Alkhseilat, 'The Cyber Espionage Crimes in the Jordanian Law', *International Journal of Electronic Security and Digital Forensics*, 14.2 (2022), 111-123. https://doi.org/10.1504/ijesdf.2022.121203

Abu Issa, Hamzeh, Mahmoud Ismail, and Omar Aamar, 'Unauthorized access crime in Jordanian law (comparative study)', *Digital Investigation*, 28 (2019), 104-111. https://doi.org/10.1016/j.diin.2019.01.006

Akbariavaz, Khalil, Pardis Moslemzadeh Tehrani, and Johan Shamsuddin bin Haj Sabaruddin. 'Cyberattacks and the Prohibition of the Use of Force under Humanitarian Law with Reference to the Tallinn Manual', *In European Conference on Information Warfare and Security*, 1 (2020), 451–457. https://doi.org/10.34190/EWS.20.508

Al Makhmari, Mohammed, Ali Al-Hammouri, Tareq Al-Billeh and Abdulaziz Almamari, 'Criminal Liability for Misuse of Social Media in Omani and UAE Legislation', International Journal of Cyber Criminology, 18.2 (2024) 92-106 https://cybercrimejournal.com/menuscript/index.php/cybercrimejournal/article/view/420/121

Al-Billeh, Tareq, Abdullah Alkhseilat, and Lana AL-Khalaileh, 'Scope of Penalties of Offences in Jordanian Public Office', *Pakistan Journal of Criminology*, 15.2 (2023), 341-356 https://www.pjcriminology.com/publications/scope-of-penalties-of-offences-in-jordanian-public-office/

Al-Billeh, Tareq, Ali Al-Hammouri, Tawfiq Khashashneh, Mohammed AL Makhmari, and Hamad Al Kalbani, 'Digital Evidence in Human Rights Violations and International Criminal Justice', *Journal of Human Rights Culture and Legal System*, 4.3 (2024), 842–871 https://doi.org/10.53955/jhcls.v4i3.446

Al-Billeh, Tareq, Ruba Hmaidan, Ali Al-Hammouri, and Mohammed AL Makhmari, 'The Risks of Using Artificial Intelligence on Privacy and Human Rights: Unifying Global Standards', *Jurnal Media Hukum*, 31.2 (2024), 333–350 https://doi.org/10.18196/jmh.v31i2.23480

AL-Hawamleh, Ahmad, 'Predictions of Cybersecurity Experts on Future Cyber-Attacks and Related Cybersecurity Measures', *International Journal of Advanced Computer Science and Applications*, 14.2 (2023), 801–809 https://doi.org/10.14569/IJACSA.2023.0140292

Al-Khawajah, Noor, Tareq Al-Billeh, and Majd Manasra, 'Digital Forensic Challenges in Jordanian Cybercrime Law', *Pakistan Journal of Criminology*, 15.3 (2023), 29-44. https://www.pjcriminology.com/publications/digital-forensic-challenges-in-jordanian-cybercrime-law/

Alkhseilat, Abdullah, Naser Al Ali, and Lujain Edweidar, 'Legal Regulation of Impersonation through Websites', *International Journal of Electronic Security and Digital Forensics*, 16.5 (2024), 557–576, https://doi.org/10.1504/ijesdf.2024.140748

Alkhseilat, Abdullah, Tareq Al Billeh, Mohammed Albazi, and Naser Al Ali, 'The Authenticity of Digital Evidence in Criminal Courts: A Comparative Study', *International Journal of Electronic Security and Digital Forensics*, 16.6 (2024), 720–738 https://doi.org/10.1504/ijesdf.2024.142010

Antonio Carlo and Kim Obergfaell, 'Cyber attacks on critical infrastructures and satellite communications', International Journal of Critical Infrastructure Protection, 46 (2024), 100701 https://doi.org/10.1016/j.ijcip.2024.100701

Arnold, Roberta, 'The Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations, Edited by Michael N. Schmitt', *International Criminal Law Review*, 20.1 (2020), 155–159 https://doi.org/10.1163/15718123-02001008

Beatty, Georgia, 'War Crimes in Cyberspace: Prosecuting Disruptive Cyber Operations under Article 8 of the Rome Statute', *The Military Law and the Law of War Review*, 58.2 (2020), 209–239 https://doi.org/10.4337/mllwr.2020.02.17

Biggio, Giacomo, 'International Humanitarian Law and the Protection of the Civilian Population in Cyberspace: Towards a Human Dignity-Oriented Interpretation of the Notion of Cyber Attack under Article 49 of Additional Protocol I. The Military Law and the Law of War Review', *Edward Elgar Publishing*, 59.1 (2021), 114–140 https://doi.org/10.4337/mllwr.2021.01.06

Brianna Bace, Yasir Gökce, and Unal Tatar, 'Law in Orbit: International Legal Perspectives on Cyberattacks Targeting Space Systems', Telecommunications Policy, 48.4 (2024), 102739–39, https://doi.org/10.1016/j.telpol.2024.102739

Chang, Chih Hsiang, 'How Does the Tallinn Manual 2.0 Shed Light on the Threat of Cyber Attacks against Taiwan-', *In European Conference on Information Warfare and Security*, 1 (2023), 649–656 https://doi.org/10.34190/eccws.22.1.1294

Cong, Wanshu, 'Seeking Customary International Human Rights Law in the Cyberspace: A Critique of the Tallinn Manual 2.0.', *SSRN Electronic Journal*, 1 (2021), 1-20 https://doi.org/10.2139/ssrn.3744924

Daraji, Mohammad Hasan, and Omar Saleh AL-Okour, 'Cyber-Attacks in Accordance With International Humanitarian Law', *Dirasat: Shari'a and Law Sciences*, 51.1 (2024), 1-12 https://doi.org/10.35516/law.v51i1.786

Drobotov, Serhii, Roman Pertsev, Mariia Hrab, Vasyl Fedytnyk, Svitlana Moroz, and Mariia Kikalishvili, 'Forensic Research of the Computer Tools and Systems in the Fight against Cybercrime', *Journal of Information Technology Management*, 15.1 (2023), 135–62 https://doi.org/10.22059/jitm.2023.90741

Efrony, Dan, and Yuval Shany, 'A Rule Book on the Shelf? Tallinn Manual 2.0 on Cyberoperations and Subsequent State Practice', *American Journal of International Law*, 112.4 (2018), 583–657 https://doi.org/10.1017/ajil.2018.86

Eoyang, Mieke, and Chimène Keitner, 'Cybercrime vs. Cyberwar: Paradigms for Addressing Malicious Cyber Activity', *Journal of National Security Law and Policy*, 1 (2020), 1-21 http://dx.doi.org/10.2139/ssrn.3599588

Espada, Cesáreo Gutiérrez, 'The Growing Need for Legislation against Cyber Threats, Sources of Serious Transnational Harm', *Cuadernos de Derecho Transnacional*, 14.2 (2022), 10–14 https://doi.org/10.20318/cdt.2022.7169

Faga, Hemen Philip, 'The Implications of Transnational Cyber Threats in International Humanitarian Law: Analysing the Distinction Between Cybercrime, Cyber Attack, and Cyber Warfare in the 21st Century', *Baltic Journal of Law and Politics*, 10.1 (2017), 1-34 https://doi.org/10.1515/bjlp-2017-0001

Fahey, Elaine, 'The Evolution of EU–US Cybersecurity Law and Policy: On Drivers of Convergence', *Journal of European Integration*, 46.7 (2024), 1073–1088 https://doi.org/10.1080/07036337.2024.2411240

Garkusha-Bozhko, Sergei Yu, 'The Definition of Armed Conflict in Cyberspace' *Vestnik Sankt-Peterburgskogo Universiteta. Pravo*, 14.1 (2023), 194–210 https://doi.org/10.21638/spbu14.2023.112

Garkusha-Bozhko, Sergei Yu, 'The Problem of Cyber Espionage in the International Humanitarian Law', *Moscow Journal of International Law*, 1 (2021), 70–80 https://doi.org/10.24833/0869-0049-2021-1-70-80

Gervais, Michael, 'Cyber Attacks and the Laws of War', *SSRN Electronic Journal*, 1 (2012), 1-45 https://doi.org/10.2139/ssrn.1939615

Heinze, Eric A., and Rhiannon Neilsen, 'Limited Force and the Return of Reprisals in the Law of Armed Conflict', *Ethics and International Affairs*, 34.2 (2020), 175-188 https://doi.org/10.1017/S0892679420000246

Holder, Maxron, 'Cyberspace in a State of Flux: Regulating Cyberspace through International Law', *Groningen Journal of International Law*, 9.2 (2022), 266–280 https://doi.org/10.21827/grojil.9.2.266-280

Hrushko, M. V., 'Attribution of Cyberattacks as a Prerequisite For Ensuring Responsible Behavior in Cyberspace', *Constitutional State*, 43 (2021), 195–201 https://doi.org/10.18524/2411-2054.2021.43.241002

Huang, Ke Zhen, Yi Feng Lian, Deng Guo Feng, Hai Xia Zhang, Di Wu, and Xiang Liang Ma, 'Method of Cyber Attack Attribution Based on Graph Model', *Ruan Jian Xue Bao/Journal of Software*, 33.2, (2022) 683–698. https://doi.org/10.13328/j.cnki.jos.006314

Igakuboon, Adasi Nsanawaji, 'An Appraisal of The Legal Framework for The Protection of Civilians in Cyber-Warfare Under International Humanitarian Law', *International Journal of Research and Scientific Innovation*, 9.7 (2022), 14–26 https://doi.org/10.51244/ijrsi.2022.9702

Janssens, Pauline Charlotte, and Jan Wouters, 'Informal International Law-Making: A Way around the Deadlock of International Humanitarian Law?', *International Review of the Red Cross*, 104.920–921 (2022), 2111–2130. https://doi.org/10.1017/S1816383122000467

Johnson, Craig J., Kimberly J. Ferguson-Walter, Robert S. Gutzwiller, Dakota D. Scott and Nancy Cooke, 'Investigating Cyber Attacker Team Cognition', *Proceedings of the Human Factors and Ergonomics Society Annual Meeting*, 66.1 (2022), 105–109 https://doi.org/10.1177/1071181322661132

Julia E Sullivan and Dmitriy Kamensky, 'Putin's Power Play: Russia's Attacks on Ukraine's Electric Power Infrastructure Violate International Law', The Electricity Journal, 37.2 (2024), 107371–71 https://doi.org/10.1016/j.tej.2024.107371

Kessler, Oliver, and Wouter Werner, 'Expertise, Uncertainty, and International Law: A Study of the Tallinn Manual on Cyberwarfare', *Leiden Journal of International Law*, 26.4 (2013), 793–810 https://doi.org/10.1017/S0922156513000410031

Khashashneh, Tawfiq, Tareq Al-Billeh, Ali Al-Hammouri, and Roua Belghit, 'The Importance of Digital Technology in Extracting Electronic Evidence: How Can Digital Technology be used at Crime Scenes?', *Pakistan Journal of Criminology*, 15.4 (2023), 69-85 https://www.pjcriminology.com/publications/the-importance-of-digital-technology-in-extracting-electronic-evidence-how-can-digital-technology-be-used-at-crime-scenes/

Kleemann, Steven, 'Cyber Warfare and the 'Humanization' of International Humanitarian Law', *International Journal of Cyber Warfare and Terrorism*, 11.2 (2021), 1–11. https://doi.org/10.4018/IJCWT.2021040101

Kotenko, Loger, Elena Fedorchenko, Evgenia Novikova and Ashish Jha, 'Cyber Attacker Profiling for Risk Analysis Based on Machine Learning', Sensors, 23.4, (2023) https://doi.org/10.3390/s23042028

Leggat, Helaine, 'Cyber Warfare: An Enquiry into the Applicability of National Law to Cyberspace', *International Journal of Cyber Warfare and Terrorism*, 10.3 (2020), 28–46 https://doi.org/10.4018/IJCWT.2020070103

Leng, Yaxuan, 'When Can Cyberattack Constitute Use of Force: A Case Study of Cyberattack in the Russia-Ukraine Conflict', *Lecture Notes in Education Psychology and Public Media*, 17.1 (2023), 201–7 https://doi.org/10.54254/2753-7048/17/20231249

Li, Yuchong, and Qinghui Liu, 'A Comprehensive Review Study of Cyber-Attacks and Cyber Security; Emerging Trends and Recent Developments', *Energy Reports*, 7 (2021), 8176–8186 https://doi.org/10.1016/j.egyr.2021.08.126

Lin, Herbert, 'Cyber Conflict and International Humanitarian Law', *International Review of the Red Cross*, 94.886 (2013), 515–531 https://doi.org/10.1017/S1816383112000811

Liu, Ian Yuying, 'The Due Diligence Doctrine under Tallinn Manual 2.0.', *Computer Law and Security Review*, 33.3 (2017), 390–395 https://doi.org/10.1016/j.clsr.2017.03.023

LUOR, Tainyi, Jen Fu WANG, and Hsi-Peng LU, 'Trends in and Contributions to Tallinn Manual Research: An Assessment of the Literature from 1998 to November 2022', *Informatica Economica*, 27.3 (2023), 45–60 https://doi.org/10.24818/issn14531305/27.3.2023.04

M. R, Amal, and Venkadesh P, 'Hybrid H-DOC: A bait for analyzing cyber attacker behavior', *International Journal of Electrical and Computer Engineering Systems*, 14.1, (2023), 37–44 https://doi.org/10.32985/ijeces.14.1.5

Maˇc´ak, Kubo, 'INTERNATIONAL LAW AND PRACTICE From Cyber Norms to Cyber Rules: Re-Engaging States as Law-Makers', *Leiden Journal of International Law*, 30 (2020), 877–899 https://doi.org/10.1017/S0922156517000358

Madubuike-Ekwe, Joseph N., 'Cyberattack and the Use of Force in International Law', *Beijing Law Review*, 12.2 (2021), 631–49 https://doi.org/10.4236/blr.2021.122034

Mazaraki, Nataliia, and Yulia Goncharova, 'Cyber Dimension of Hybrid Wars: Escaping A 'Grey Zone' Of International Law to Adress Economic Damages', *Baltic Journal of Economic Studies*, 8.2 (2022), 115–120 https://doi.org/10.30525/2256-0742/2022-8-2-115-120

McKenzie, Simon, 'Cyber Operations against Civilian Data', *Journal of International Criminal Justice*, 19.5 (2022), 1165–1192. https://doi.org/10.1093/jicj/mqab067

Mozid, Ashraful, and Nelufer Yesmen, 'Term Paper on The Nature of Cyber Crime and Cyber Threats: A Criminological Review', *Journal of Advanced Forensic Sciences*, 1.1 (2020), 1–9 https://doi.org/10.14302/issn.2692-5915.jafs-20-3204

Muzyka, Viktoriia, 'New Wine in Old Bottles: Applicability of the Rules on Attribution to Cyberattacks Committed against Objects of Critical Infrastructure', *Law Review of Kyiv University of Law*, 3 (2020), 388–391 https://doi.org/10.36695/2219-5521.3.2020.72

Nagasako, Tomoko, 'A Consideration of the Case Study of Disinformation and Its Legal Problems', *In IFIP Advances in Information and Communication Technology*, 590 (2020), 262–276 https://doi.org/10.1007/978-3-030-62803-1_21

National Cyber Security Centre, 6th Cybersecurity Forum, Oman, Muscat. https://cert.gov.om/news/270

National Cyber Security Centre, National Cybersecurity Products and Services Guide for 2025, Oman, Muscat. https://cert.gov.om//librarys/publications/servicesGuideline.pdf

National Cybersecurity Center, Approval of the National Cybersecurity Strategy 2025-2028. Amman, Jordan https://ncsc.jo/Ar/NewsDetails/National_CS_Strategy_2025_2028

National Cybersecurity Center, The National Cybersecurity Center Issues its Cybersecurity Posture Report for the First Quarter of 2025. Amman, Jordan https://ncsc.jo/Ar/NewsDetails/Q1_2025_Report_NCSCJO

Nnawulezi, Uche, and Salim Bashir Magashi, 'Evolving Roles of the International Institutions in the Implementation Mechanisms of the Rules of International Humanitarian Law', *Kutafin Law Review*, 9.4 (2022), 684–712 https://doi.org/10.17803/2313-5395.2022.4.22.684-712

Nnawulezi, Uche, Kelechi Onyegbule and Charis Godson Ukanwa, 'Evolving Roles of the United Nations Agencies on the Implementation Mechanisms of the Rules of International Humanitarian Law', *The Nigerian Juridical Review*, 16 (2022), 43–63 https://doi.org/10.56284/tnjr.v16i1.12

Oğurlu, Ebru, 'International Law in Cyberspace: An Evaluation of the Tallinn Manuals', *Annales de La Faculte de Droit d'Istanbul*, 73 (2023), 327–44 https://doi.org/10.26650/annales.2023.73.0010

Orr, Zachary R., 'Redress for Unlawful Cyber-Attacks During Armed Conflict: The Limits of the International Criminal Court and How Human Rights Bodies Can Help Close the Gap', *SSRN Electronic Journal*, 57.359 (2023), 359-410 https://doi.org/10.2139/ssrn.4422358

Pettoello-Mantovani, Clara, 'Cybercrimes: An Emerging Category of Offenses within the Frame of the International Criminal Court Jurisdiction." International Journal of Law and Politics Studies', *Al-Kindi Center for Research and Development*, 6.2 (2024), 6–11 https://doi.org/10.32996/ijlps.2024.6.2.2

Pipyros, Kosmas, Christos Thraskias, Lilian Mitrou, Dimitris Gritzalis, and Theodoros Apostolopoulos, 'A New Strategy for Improving Cyber-Attacks Evaluation in the Context of Tallinn Manual', *Computers and Security*, 74 (2018), 371–383. https://doi.org/10.1016/j.cose.2017.04.007

Pratama, B., and M. Bamatraf, 'Tallinn Manual: Cyber Warfare in Indonesian Regulation', *In IOP Conference Series: Earth and Environmental Science*, 729 (2021), 1-8 https://doi.org/10.1088/1755-1315/729/1/012033

Protas, Petro, and Leornard Chimanda Joseph, 'The Law of Armed Conflict in the Era of Cyber Technology: Assessing the Legal Challenges and Response in Tanzania', *Eastern Africa Law Review*, 47.1 (2020), 95–139 https://doi.org/10.56279/ealr.v47i1.4

Quader, Faisal, and Vandana P. Janeja, 'Insights into Organizational Security Readiness: Lessons Learned from Cyber-Attack Case Studies', *Journal of Cybersecurity and Privacy*, 1.4 (2021), 638-659 https://doi.org/10.3390/jcp1040032

Rendón-Segador, Fernando J., Juan A. Álvarez-García, and Angel Jesús Varela-Vaca, 'Paying Attention to Cyber-Attacks: A Multi-Layer Perceptron with Self-Attention Mechanism', *Computers and Security*, 132 (2023), 103318 https://doi.org/10.1016/j.cose.2023.103318

Richardson, John C, 'Stuxnet as Cyberwarfare: Applying the Law of War to the Virtual Battlefield', *SSRN Electronic Journal*, 1 (2012), 1-38 https://doi.org/10.2139/ssrn.1892888

Samuli Haataja, 'Cyber operations and automatic hack backs under international law on necessity', Computer Law & Security Review, 53 (2024), 105992 https://doi.org/10.1016/j.clsr.2024.105992

Schellekens, Jasper, 'Release the Bots of War: Social Media and Artificial Intelligence as International Cyber Attack', *Przegląd Europejski*, 4 (2021), 163–179 https://doi.org/10.31338/1641-2478pe.4.21.10

Schmitt, Michael, 'Classification of Cyber Conflict', *Journal of Conflict and Security Law*, 17.2 (2012), 245–260 https://doi.org/10.1093/jcsl/krs018

Schmitt, Michael. N, 'Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations', Cambridge University Press, (2017) https://doi.org/10.1017/9781316822524

Shah, Pritik A., and Marcos Roberto Tovani-Palone, 'Surgical Care Services in Inaccessible Zones: Targeted Palliative Care Accessibility Models for Patients in Resource-Limited Settings', *The International Journal of Health Planning and Management*, 37.S1 (2022), 243–49 https://doi.org/10.1002/hpm.3580

Shukla, Vanshika, 'A BRIEF STUDY OF INTERNATIONAL LAW IN THE AGE OF CYBERSECURITY', *EPRA International Journal of Multidisciplinary Research (IJMR)*, 9.11 (2023), 269–273 https://doi.org/10.36713/epra14915

Spáčil, Jakub, 'Cyber Operations against Critical Financial Infrastructure: A Non-Destructive Armed Attack?', *International and Comparative Law Review*, 22.2 (2022), 27–42 https://doi.org/10.2478/iclr-2022-0013

Sweet, Colin, 'Tallinn Manual on the International Law Applicable to Cyber Warfare', *Europe-Asia Studies*, 66.4 (2014), 669–670. https://doi.org/10.1080/09668136.2014.897423

Tanodomdej, Papawadee, 'The Tallinn Manuals and the Making of the International Law on Cyber Operations', *Masaryk University Journal of Law and Technology*, 13.1 (2019), 67–85 https://doi.org/10.5817/MUJLT2019-1-4

The First Additional Protocol to the Geneva Conventions of 1949. https://www.icrc.org/sites/default/files/external/doc/en/assets/files/other/icrc_002_0321.pdf

The National Cybersecurity Center. Cybersecurity: Bahraini-UK partnership to enhance international cooperation and build cyber capabilities. Bahrain. https://www.ncsc.gov.bh/ar/media-center/news-details.html?src=

The National Cybersecurity Center. The National Cybersecurity Center participates in the meetings of the Arab Cybersecurity Ministers Council. Bahrain. https://www.ncsc.gov.bh/en/media-center/news-details

The Statute of the International Criminal Court. July 17, 1998. https://www.icc-cpi.int/sites/default/files/2025-02/Rome-Statute-EN-2025.pdf

The UN Charter. https://www.un.org/en/about-us/un-charter

Thumfart, Johannes, 'Public and Private Just Wars: Distributed Cyber Deterrence Based on Vitoria and Grotius', *Internet Policy Review*, 9.3 (2020), 1–26 https://doi.org/10.14763/2020.3.1500

Tignino, Mara, 'The Regulation of Crimes against Water in Armed Conflicts and Other Situations of Violence', *International Review of the Red Cross*, 105.923 (2023), 706–734 https://doi.org/10.1017/S1816383123000061

Trahan, Jennifer, 'The Criminalization of Cyber-Operations Under the Rome Statute', *Journal of International Criminal Justice*, 19.5 (2021), 1133–1164 https://doi.org/10.1093/jicj/mqab066

Usman, Hazrat, Raja Ishtiaq Ahmed, and Syed Suliman Ali. 'Navigating the Gray Area: A Comprehensive Analysis of Cyber Warfare and Its Relationship to the Law of Armed Conflict', *Global Legal Studies Review*, 7.3 (2022), 32–36 https://doi.org/10.31703/glsr.2022(vii-iii).05

Voitasec, Dan-Iulian, 'Applying International Humanitarian Law to Cyber Attacks', *Lex ET Scientia International Journal*, 22.Xxii (2015), 552–556. http://www.icj-cij.org/docket/files/70/6503.pdf

Werner, Wouter, 'Say That Again, Please: Repetition in the Tallinn Manual', *In Repetition and International Law*, (2022), 95–114 https://doi.org/10.1017/9781009039666.005

Wheatley, Steven, 'Election Hacking, the Rule of Sovereignty, and Deductive Reasoning in Customary International Law', *Leiden Journal of International Law*, 36.3 (2023), 675–698 https://doi.org/10.1017/S0922156523000092

Woods, Daniel W., and Sezaneh Seymour, 'Evidence-Based Cybersecurity Policy? A Meta-Review of Security Control Effectiveness', *Journal of Cyber Policy*, 8.3 (2024), 1–19 https://doi.org/10.1080/23738871.2024.2335461

Yeremyan, Ara, and Lilit Yeremyan, 'International Law Issues of Cyber Defense', *Moscow Journal of International Law*, 2 (2022), 85–100 https://doi.org/10.24833/0869-0049-2022-2-85-100

Yuliya Miadzvetskaya, 'EU sanctions in response to cyber-attacks as crime-based emergency measures', Computer Law & Security Review, 54 (2024), 106010 https://doi.org/10.1016/j.clsr.2024.106010

Zahra, Iradhati, and Diajeng Wulan Christianti. 'The Beginning Of The International Humanitarian Law Application to Cyber Attack: The Status of Rule 30 Tallinn Manual 1.0.', *Padjadjaran Journal of International Law*, 5.1 (2021), 98–113 https://doi.org/10.23920/pjil.v5i1.366

Zahra, Iradhati, Irawati Handayani, and Diajeng Wulan Christianti. 'Cyber-Attack In Estonia: A New Challenge in the Applicability of International Humanitarian Law', *Yustisia Jurnal Hukum*, 10.1 (2021), 48-66 https://doi.org/10.20961/yustisia.v10i1.48336

Zhang, Yan, Degang Zhu, Menglin Wang, Junhan Li, and Jie Zhang, 'A comparative study of cyber security intrusion detection in healthcare systems', *International Journal of Critical Infrastructure Protection*, 44. (2024) https://doi.org/10.1016/j.ijcip.2023.100658