*International Law Discourse in Southeast Asia*
ISSN 2830-0297 (Print) 2829-9655 (Online)
Vol. 5 Issue 1 (2026) 296–329
DOI: https://doi.org/10.15294/ildisea.v5i1.42796
Available online since: July 25, 2026

# Protecting Critical National Infrastructure Against Cyber Operations Under International Humanitarian Law: Lessons for Southeast Asia

Andi Agus Salim [a]✉, Maulidina Sari [b], Nova Bela Dhyta [c], Ahmad Sholihin Muttaqin [d], Try Hardyanthi [e]

[a] Faculty of Law, Universitas Jambi, Jambi, Indonesia
[b] Faculty of Law, Universitas Jambi, Jambi, Indonesia
[c] Faculty of Law, Universitas Jambi, Jambi, Indonesia
[d] Faculty of Law, Universitas Jambi, Jambi, Indonesia
[e] Faculty of Law, University of Pécs, Pécs, Hungary
✉ Corresponding email: andiagus@unja.ac.id

## Abstract

The rapid evolution of digital technology has significantly reshaped the dynamics of modern armed conflict, most notably through the escalating threat of cyberattacks against critical infrastructure. Essential facilities such as power grids, medical centers, water sanitation systems, and communication networks play an indispensable role in ensuring the safety and well-being of the civilian population. When such infrastructure is targeted during armed conflict, whether by State or non-State actors, the resulting humanitarian consequences can be catastrophic and far-reaching. International Humanitarian Law (IHL), which traditionally governs the protection of civilian objects, has yet to explicitly address the unique challenges posed by the digital frontier, particularly regarding the

protection of critical infrastructure from cyber warfare. This research aims to critically examine the extent to which IHL principles can provide adequate protection for critical infrastructure within the context of cyber operations, while identifying the normative gaps that emerge in their implementation. Employing a doctrinal legal research methodology complemented by an interdisciplinary analytical approach integrating international legal analysis with cybersecurity contemporary military studies, and supported by selected contemporary cyber incidents, this study proposes a strengthened normative framework that is more responsive to the exigencies of the digital age. The novelty of this research lies in its specific focus on the protection of vital civilian infrastructure in modern warfare from an IHL perspective, offering legal solutions grounded in state practice and fundamental humanitarian principles. It further highlights the relevance of these normative developments for Southeast Asia by identifying legal and policy lessons that can strengthen regional preparedness for protecting critical infrastructure against cyber operations during armed conflict.

**KEYWORDS** *Critical National Infrastructure (CNI); Cyberattacks; International Humanitarian Law (IHL).*

# Introduction

The gigantic digital transformation has taken place during the last two decades and made the world much more dependent on information and communication technologies. [1] On the one hand, the further development of technology has made life easier and more effective in many public and private spheres. On the other hand, practical advancements have also led to the emergence of new vulnerabilities that can be targeted by adversaries, particularly during modern wars.[2] One of the most evident examples of the mentioned vulnerabilities is the growing number of cyber operations aimed at the most critical national infrastructure such as energy supply systems, water systems, health care

[1] Muh Susila and Andi Salim, "Cyber Espionage Policy and Regulation: A Comparative Analysis of Indonesia and Germany," *Padjadjaran Jurnal Ilmu Hukum (Journal of Law)* 11, no. 1 (2024): 122–44, https://doi.org/10.22304/pjih.v11n1.a6.

[2] Yazid Akbar Alamsyah and Rafi Ilyasa Ibnu Akbar, "Penggunaan Persenjataan Modern Dalam Konflik Bersenjata Ditinjau Dari Prinsip Hukum Humaniter Dan Hukum Islam," *Sanskara Hukum Dan HAM* 3, no. 01 (August 2024): 24–33, https://doi.org/10.58812/shh.v3i01.434.

institutions, and government data centers, as well as transport and communication networks.[3] The operations carried out in peacetime lead already to serious consequences; however, what is more dangerous is that during the war such attacks will cause considerable suffering and damage to civilians.

The significance of critical infrastructure cannot be underestimated, as it provides a foundation for the functioning of societies and the stability of states. Attacks on such infrastructure do not only lead to technical difficulties but also entail serious consequences for people.[4] For instance, widespread blackout caused by any cyber means may lead to problems in hospitals, difficulties with providing safe drinking water and breakdown of the means of communication for humanitarian organizations. In the case of a war, the implications of such attacks can be much worse since they can worsen the already hard living conditions of the civilian population.

Within the framework of international law, International Humanitarian Law (IHL), which is also known as the Armed Conflict Law and the Warfare Law. International Humanitarian Law is defined by several key principles that govern conflict conduct and protect individuals, not directly involved in the conflict. These principles include but are not limited to combatant-civilian distinction principle, proportionality principle, and precautionary principle, which lessen human suffering in wars.[5] However, some questions about principles' relevance, applicability, and efficiency arise in terms of new warfare methods, especially those using cyber technologies.

Moreover, cyber warfare targeting critical infrastructure is not a mere speculation. We see various examples of how the important industries were compromised through cyber operations in the past years. For instance, the Stuxnet attack on the Iranian nuclear facilities in 2010 is the frequently investigated case that shows the power of the malware in the setting of proper integration of IT into physical systems even in the

[3] Renatha Ayu Rossdiana and Titing Reza Fahrisa, "Strategi Cybersecurity Pemerintah India Dari Perspektif Kautilya: Serangan Siber Mumbai 2020," *Indonesian Journal of International Relations* 7, no. 1 (March 2023): 140–64, https://doi.org/10.32787/ijir.v7i1.408.

[4] Adriana Alexandru, Victor Vevera, and Ella Magdalena Ciupercă, "National Security and Critical Infrastructure Protection," *International Conference Knowledge-Based Organization* 25, no. 1 (June 2019): 8–13, https://doi.org/10.2478/kbo-2019-0001.

[5] Indah Sari, "Tinjauan Yuridis Hubungan Kejahatan Perang Dan Hukum Humaniter Internasional," *Jurnal Ilmiah Hukum Dirgantara* 11, no. 2 (2021).

absence of armed conflict.[6] Furthermore, during the armed conflict in Ukraine, many cyber operations aimed at the electricity networks and hospitals were reported to have affected the lives of millions.[7] In these cases, it is not easy to establish whether a certain cyber operation is liable for breaching IHL because there is not a common agreement between different countries and other relevant entities about how to interpret the existing legal norms in relation to the cyberspace.

Up to now, there is existing no international legal framework which clearly outlines the safeguarding of critical infrastructure from cyber attacks during times of war.[8] However, significant scholarly and legal initiatives have begun to bridge this absence of regulation. One of the major publications here is Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations. Even if this document does not create any legal obligations, it still gives valuable indications on how to interpret international law rules, including the international humanitarian law. In addition, it has been stated by the International Committee of the Red Cross that international humanitarian law applies to cyberspace as well. Nonetheless, the implementation of these norms is still considerably debatable among the parties involved in the discussions.[9]

In the field of academia, studies devoted to International Humanitarian Law (IHL) and cyber operations have gained wider acceptance and numerous approaches by different scholars. On the topical research agenda there are studies discussing protection of critical infrastructure. An exemplary study in this regard is written by Andrea Locatelli in the chapter entitled Critical Infrastructure Protection, where critical infrastructure is defined and United States and European Union policies aimed at its protection are examined. Nevertheless, analysis carried out by Locatelli is mainly descriptive and policy-oriented without any normative framework arising from the perspective of armed conflict

---

6 Aryuni Yuliantiningsih, "Analisis Doktrin Perang Yang Adil (Just War) Dalam Kasus Serangan Siber Rusia Terhadap Georgia Tahun 2008," *Kosmik Hukum* 21, no. 3 (October 2021): 175, https://doi.org/10.30595/kosmikhukum.v21i3.10613.

7 Nadia Azzahra and Lina Hastuti, "Analisis Hukum Humaniter Internasional Terhadap Penyerangan Dual Use Object Dalam Konflik Bersenjata Rusia Dan Ukraina," *Jurist-Diction* 8, no. 1 (January 2025): 91–118, https://doi.org/10.20473/jd.v8i1.54375.

8 Maskun Maskun et al., "Cyber-Attack: Its Definition, Regulation, and ASEAN Cooperation to Handle with It," *Jambe Law Journal* 4, no. 2 (November 2021): 131–50, https://doi.org/10.22437/jlj.4.2.131-150.

9 A. Widiada Gunakaya, *Hukum Pidana Internasional* (Takaza Innovatix Labs, 2024).

law.[10] A new piece of research is represented by the article written by Markopoulou and Papakonstantinou entitled The Regulatory Framework for the Protection of Critical Infrastructures Against Cyberthreats: Identifying Shortcomings and Addressing Future Challenges: A Case Study from the Health Sector. It is more focused than the aforementioned research piece and examines healthcare critical infrastructure using the EU regulatory framework.[11]

While both works relate to critical infrastructure protection, they are unique from this study in terms of their scope and perspective. In the present research, critical national infrastructure comes under scrutiny in terms of protection from cyber operations, as per International Humanitarian Law. This legal concept is central to the study since it aims to regulate human behavior in armed conflict. Therefore, the main goal of the study is to analyze how international humanitarian law can provide effective protection to critical infrastructure from cyber threats during wars. In addition, the research tries to identify certain gaps in the present international legislation, and suggest changes which can help overcome the problems posed.

The study has been conducted using the doctrinal legal research method along with its interdisciplinary research approach. The research is mainly based on international legal sources like the Geneva Conventions of 1949, the Additional Protocols of 1977, customary international humanitarian law, international case law, soft-law documents including the Tallinn Manual 2.0, and modern literature on cyber warfare within international law. In this research, it is acknowledged that cyber operations have legal and technical aspects, therefore insights from the cybersecurity studies, the protection of critical infrastructure, digital governance, and modern military strategy issues are also used. These interdisciplinary insights have not been used for particular research purposes, but rather to provide a more comprehensive analysis of the technicalities of cyber operations.

In order to illustrate what currently International Humanitarian Law really looks like in practice, this research employs selected

[10] Andrea Locatelli, "Critical Infrastructure Protection," in *Technology and International Relations*, ed. Giampiero Giacomello, Francesco N. Moro, and Marco Valigi (Edward Elgar Publishing, 2021), https://doi.org/10.4337/9781788976077.00016.

[11] Dimitra Markopoulou and Vagelis Papakonstantinou, "The Regulatory Framework for The Protection of Critical Infrastructures Against Cyberthreats: Identifying Shortcomings and Addressing Future Challenges: The Case of The Health Sector in Particular," *Computer Law & Security Review* 41 (July 2021): 105502, https://doi.org/10.1016/j.clsr.2020.105502.

contemporary cyber events associated with key infrastructure, taking these events not as empirical case studies but as analytical ones. Those examples serve not only to showcase the implementation of legal principles, but also to establish normative gaps and evaluate the degree of efficiency of the current legal policies concerning cyber operations with critical civilian infrastructure in an armed conflict. Thus, the case studies serve as legal illustrative evidence used in the doctrinal analysis.

## Characteristics and Vulnerabilities of Critical Infrastructure in the Cyber Era

Critical National Infrastructure (CNI) serves as the basic system of the administration, delivery of public services, ensuring economic stability, and meeting the basic needs of citizens. In the terms of international law and security studies, it can be noted that CNI covers many strategic sectors such as energy, health services, transportation, telecommunications, water supply, finance, defense, and e-government services. In the conditions of constant digitalization, with automated processes and interconnected systems, several components of CNI rely heavily on cyber technologies and information networks. This situation has caused the appearance of vulnerabilities that were unavailable in the framework of conventional warfare.[12]

Changes in the global security landscape suggest that cyber operations are no longer restricted to espionage and limited sabotage, but now serve as strategic tool to incapacitate national infrastructure without the need for military mobilization.[13] Since 2019, the NATO CCDCOE, ENISA, and Microsoft Digital Defence have reported a significant rise in computer operations aimed at civil and military infrastructure, especially in the energy and health industries.[14] The WannaCry attack in 2017 was a

[12] Moritz Weiss and Felix Biermann, "Cyberspace and the Protection of Critical National Infrastructure," *Journal of Economic Policy Reform* 26, no. 3 (July 2023): 250–67, https://doi.org/10.1080/17487870.2021.1905530.

[13] Martti Lehto, "Cyber-Attacks Against Critical Infrastructure," in *Cyber Security*, vol. 56, ed. Martti Lehto and Pekka Neittaanmäki, Computational Methods in Applied Sciences (Cham: Springer International Publishing, 2022), 3–42, https://doi.org/10.1007/978-3-030-91293-2_1.

[14] Roberto Di Pietro et al., "Critical Infrastructure," in *New Dimensions of Information Warfare*, vol. 84, by Roberto Di Pietro et al., Advances in Information Security (Cham:

signal of the growing digital threats.[15] Now, in five years since that incident, cyber operations are predominantly aimed at key players whose disruption causes immediate and significant impact on civilian populations.[16]

The growing reliance of critical infrastructure on Supervisory Control and Data Acquisition (SCADA) systems, Industrial Control Systems (ICS), and the Internet of Things (IoT) has further amplified these risks. Within electricity networks, for example, the exploitation of vulnerabilities in distribution systems may trigger large scale power outages that directly affect hospitals, clean water services, emergency communication systems, and even defensive military operations.[17] The cyber operation targeting the Colonial Pipeline in 2021 demonstrated that cyber attacks against energy infrastructure are capable of disrupting fuel distribution, generating public panic, and causing significant economic losses across national borders.[18]

Vulnerability is further intensified by the increasing interdependence among critical infrastructures. Whereas disruptions were previously confined to individual sectors, a single cyber operation is now capable of generating cascading effects across multiple systems. For example, when telecommunications systems are compromised, emergency services, hospitals, transportation networks, and logistics distribution are simultaneously affected.[19] Consequently, the concept of interconnected vulnerabilities has attracted heightened attention since 2020, particularly within digital security studies conducted by the United Nations Office for Disarmament Affairs, the Interpol Cybercrime Directorate, and the Organisation for Economic Cooperation and Development.

---

Springer International Publishing, 2021), 157–96, https://doi.org/10.1007/978-3-030-60618-3_5.

15 Sebastian W. Schuetz et al., "Does Ransomware Make Investors 'WannaCry'? On Investors' Divergent Reactions to Ransomware Hits and Near Misses," *MIS Quarterly* 49, no. 3 (September 2025): 1153–68, https://doi.org/10.25300/MISQ/2024/18509.

16 Tawfiq M. Aljohani, "Cyberattacks on Energy Infrastructures as Modern War Weapons - Part I: Analysis and Motives," *IEEE Technology and Society Magazine* 43, no. 2 (June 2024): 59–69, https://doi.org/10.1109/MTS.2024.3395688.

17 Dr. A.Shaji George, Dr. T.Baskar, and Dr. P.Balaji Srikaanth, *Cyber Threats to Critical Infrastructure: Assessing Vulnerabilities Across Key Sectors*, February 25, 2024, https://doi.org/10.5281/ZENODO.10639463.

18 Shadrach Owusu, "The Rising Threat - Cybersecurity Risks in Critical Energy Infrastructure," preprint, SSRN, 2025, https://doi.org/10.2139/ssrn.5370813.

19 James McCarthy et al., *Energy Sector Asset Management For Electric Utilities, Oil & Gas Industry* (National Institute of Standards and Technology, 2020), https://doi.org/10.6028/NIST.SP.1800-23.

Beyond technical risks, the complexity of relevant actors has also increased. Both State actors and non-State actors, including non-state armed groups, hacktivists, cyber mercenaries, and organized cybercrime networks, play a significant role in cyber contestation targeting civilian infrastructure. In the context of armed conflict, non-state armed groups are no longer limited to the use of conventional weapons, but increasingly operate digital units capable of penetrating critical information systems. Groups such as Lazarus Group, commonly associated with North Korea, Sandworm, linked to Russia, Charming Kitten, associated with Iran, and several actors attributed to China are frequently connected with operations against government networks and public facilities.[20]

Weak governance in cyber security has made many countries more vulnerable. Scarcity of financial, human, and technology resources has made these nations vulnerable to cyber operations and activities. Reports by the World Economic Forum issued during the last five years have indicated that numerous countries do not have proper infrastructure protection strategies during peacetime and war.[21]

Critical infrastructure is considered as a civilian object and requires protection in accordance with the International Humanitarian Law (IHL). However, a question arises whether a data center or another form of critical infrastructure can be seen only as a civilian object or as an object that possesses features of a military target and therefore can be attacked.

There are numerous recent incidents demonstrating how complicated this issue is. In the framework of the Russia–Ukraine conflict which has been going on since 2022, reports by Microsoft Threat Intelligence published in 2023 indicated that more than 200 cyber operations targeted Ukrainian energy and government sectors. While some of these operations were related to spying, others aimed at interrupting vital public operations. What is even more worrying is that many of these cyber operations were executed along with military attacks.[22] From the point of view of International Human Law, such

[20] Hugo Riggs et al., "Impact, Vulnerabilities, and Mitigation Strategies for Cyber-Secure Critical Infrastructure," *Sensors* 23, no. 8 (April 2023): 4060, https://doi.org/10.3390/s23084060.

[21] Miklós BöRöCZ, "Critical Infrastructure Protection Policy in the EU," *Strategic Impact* 80, no. 3 (February 2022): 46–61, https://doi.org/10.53477/1841-5784-21-15.

[22] Microsoft Threat Intelligence, *Microsoft Digital Defense Report 2023: Building and Improving Cyber Resilience* (2023), https://www.microsoft.com/en-us/search/explore?q=Microsoft+Digital+Defense+Report+2023#:~:text=featuring%20expert%20guidance.-,Microsoft%20Digital%20Defense%20Report,-https%3A//www.microsoft.

attacks raise serious questions regarding their legality and proportionality, particularly when it comes to their consequences for civilians.

Cyber threats aimed at the health sector are one of the worst trends we can see today. According to what the WHO announced in 2020, cyber attacks against hospitals have increased by 500 percent during the COVID 19 pandemic.[23] Cyber incidents involving systems of hospitals in Czechia in 2020[24] and the Irish health system in 2021[25] prove that cybercriminals tend to attack systems whose failure could greatly affect human lives. Since these incidents took place in peacetime, cyber operations against hospitals in armed conflict may actually constitute a serious breach of the principles of International Humanitarian Law (IHL).

Besides the external threats, internal vulnerabilities such as the absence of a proper digital infrastructure, improper use of encryption, use of outdated unpatched software, and poor capacity to react to incidents play a crucial role in weakening these threats. An IBM report of 2023 stated that 61 percent of successful cyber attacks on government and critical infrastructure organizations are due to human errors or poor segmentation of networks.[26]

Another issue that further amplifies vulnerability is the difficulty of attribution, commonly referred to as the attribution problem. Unlike conventional armed attacks, the traces of cyber operations can be easily concealed, obfuscated, or rerouted through proxy attacks. This condition significantly undermines the enforcement of international law, delays the response of victim States, and obscures questions of responsibility and accountability.

Overall, these findings indicate that the protection of critical infrastructure cannot be assessed solely from a technical perspective, but must also be examined through an International Humanitarian Law

---

[23] World Health Organization, *WHO Reports Fivefold Increase in Cyber Attacks, Urges Vigilance* (Geneva, 2020), https://www.who.int/news/item/23-04-2020-who-reports-fivefold-increase-in-cyber-attacks-urges-vigilance?utm_source=chatgpt.com.

[24] Ying He et al., "Health Care Cybersecurity Challenges and Solutions Under the Climate of COVID-19: Scoping Review," *Journal of Medical Internet Research* 23, no. 4 (April 2021): e21747, https://doi.org/10.2196/21747.

[25] Gemma Moore et al., "A Resilient Workforce: Patient Safety and the Workforce Response to A Cyber-Attack on the ICT Systems of the National Health Service in Ireland," *BMC Health Services Research* 23, no. 1 (October 2023): 1112, https://doi.org/10.1186/s12913-023-10076-8.

[26] IBM Security X-Force, *X-Force Threat Intelligence Index 2023* (n.d.), https://secure-iss.com/wp-content/uploads/2023/02/IBM-Security-X-Force-Threat-Intelligence-Index-2023.pdf?utm_source=chatgpt.com.

framework that is capable of adapting to digital realities. Over the past five years, discussions on cybersecurity and the law of armed conflict have increasingly taken place within international fora, including the United Nations Group of Governmental Experts, the Open Ended Working Group, the Organization for Security and Co operation in Europe, the Association of Southeast Asian Nations, and the North Atlantic Treaty Organization. Nevertheless, these deliberations have largely remained at a general normative level and have yet to address in a specific manner the protection of critical infrastructure as civilian objects with profound humanitarian significance.

## Application of International Humanitarian Law Principles to Cyber Operations

International Humanitarian Law is designed to regulate the conduct of armed conflict and to afford protection to persons who do not take part in hostilities. Fundamental principles such as distinction, proportionality, and precaution have traditionally been applied within the context of kinetic warfare. However, the escalation of cyber threats targeting critical infrastructure presents novel challenges to the application of these principles, particularly given that the characteristics of cyber operations differ significantly from those of conventional physical attacks.

### *A. Distinction Principle*

According to the principle of distinction, combatants must distinguish between military personnel and civilians, as well as between military targets and civilian objects. Non-combatant objects may not be attacked, unless they are used for the purposes of military activity.[27] The main problem in cyber warfare is that vital infrastructures are often double-purpose. For example, electrical systems could be supplying power to military facilities and hospitals at the same time.

Tallinn Manual 2.0 published in 2017 states that cyber systems which support military operations may be perceived as military targets due to their contribution to hostilities and because their destruction will provide definite military advantage.[28] Nevertheless, identifying whether

[27] Talitha Ramphal, "The Principle of Distinction in an International Armed Conflict: Organized Armed Groups Not Belonging to a State Party to the Conflict," *International Journal of Law and Society* 4, no. 4 (2021): 275, https://doi.org/10.11648/j.ijls.20210404.15.

[28] Michael N Schmitt, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (Cambridge University Press, 2017).

the above-mentioned criteria are met is challenging. For instance, a state communication center may be used for the military purpose while simultaneously rendering services relevant for various state authorities, such as local administration, information health systems, and taxation. Cyber activity against such systems may thus cause the indirect impact on civilians.

A report of the International Committee of the Red Cross (ICRC) published in 2023 states that the majority of hacking incidents aimed at energy sector, transport systems, and governmental networks do not clearly differentiate between military and civilian tasks.[29] This situation provides evidence of how complicated it is to implement the principle of distinction in cyber warfare when it comes to critical infrastructure which is usually designed in a way that makes it hard to separate military and civilian tasks.

Moreover, another difficulty is present in cyber warfare due to cyber operations being diffuse and transboundary, which is known as spillover effect. For example, malware aimed at military targets can accidentally enter civilian networks. This has been demonstrated by the NotPetya attack of 2017 carried out against Ukraine but eventually having much wider impact as the attack affected various organizations in other countries.[30]

From the point of view of International Humanitarian Law, these unintended consequences create a lot of questions since it is not completely clear whether the cybercriminal can be held responsible for any damage inflicted on the civilian infrastructure through carrying out of his original plan of attacking only military targets.

The legal and operational challenges manifest themselves during the interactions between Russia and Ukraine, given the difficulty in implementing the principle of distinction established by International Humanitarian Law in matters of cyber operations aimed at critical infrastructure. The Russia-Ukraine crisis has shown itself to be a landmark occasion in the development of cyber warfare as an integral part of hostilities in regard to fighting wars since its initiation in 2014 and intensification in 2022. Such attacks have not only been executed through

---

[29] International Committee of the Red Cross (ICRC), *Cyber and Information Operations and International Humanitarian Law* (n.d.), https://www.icrc.org/en/law-and-policy/cyber-and-information-operations.

[30] Mourad Benmalek, "Ransomware on Cyber-Physical Systems: Taxonomies, Case Studies, Security Gaps, and Open Challenges," *Internet of Things and Cyber-Physical Systems* 4 (2024): 186–202, https://doi.org/10.1016/j.iotcps.2023.12.001.

physical attacks such as missiles and artillery, but also via digital campaigns.[31]

Before February 2022, both Microsoft in its 2023 report and NATO CCDCOE reported on the occurrence of large-scale cyberattacks against the infrastructures, connected with energy, military logistics, and governmental activities in Ukraine. Some of the major cyber operations were those against the electric grid in 2015 and 2016, which resulted in large-scale blackouts for thousands of victims. This was achieved through the use of malware, for instance, the BlackEnergy and Industroyer targeting Supervisory Control and Data Acquisition systems.[32]

The onset of the year 2022 saw the emergence of a new breed of malware - wiper malware that includes HermeticWiper and WhisperGate, which targeted the governmental infrastructures as well as civilian data centers. While the concern with regard to physical destruction was not part of the scenario, it still led to major impacts on the humanitarian aid mechanisms, hospitals, and public administration issues.[33] Now, the International Humanitarian Law perspective on such operations leads to the inquiry whether the operation of the digital systems that are the basis of supporting civilian governance is essentially classified as a valid military target.

It is worth noting that Ukraine, in coordination with its allies, has hardly used International Humanitarian Law in the context of the response to the digital operations, but instead, it has adopted a more political and diplomatic reaction to everything that took place, including the execution of sanctions and the reports provided by the Council of Europe as well as the international attribution campaigns.[34]

Moreover, the existence of volunteer hacktivist organizations such as the IT Army of Ukraine, in addition to other pro-Russian hacktivist organizations, complicates the legal position of non-state actors. There have already been cases of cyber attacks against hospitals, public transport,

---

[31] Khoirunnisa Khoirunnisa and Cristy Sugiati, "Cyber Warfare Strategies in the Russia-Ukraine Conflict (2021-2022): Implications for National Security and Modern Warfare," *Jurnal Public Policy* 10, no. 2 (April 2024): 138, https://doi.org/10.35308/jpp.v10i2.9026.

[32] Doney Abraham, Siv Hilde Houmb, and Laszlo Erdodi, "Cyber-Attacks on Energy Infrastructure - A Literature Overview and Perspectives on the Current Situation," *Applied Sciences* 15, no. 17 (August 2025): 9233, https://doi.org/10.3390/app15179233.

[33] America's Cyber Defense Agency, *Update: Destructive Malware Targeting Organizations in Ukraine*, n.d., https://www.cisa.gov/news-events/alerts/2022/02/26/update-destructive-malware-targeting-organizations-ukraine.

[34] European Council, *Sanctions Against Cyber-Attacks*, May 12, 2025, https://www.consilium.europa.eu/en/policies/sanctions-against-cyber-attacks/.

and civilian information systems carried out by non-state actors. Such circumstances create problems regarding attribution, combatant status, and international legal liability.

The case of Ukraine illustrates that the distinction principle becomes harder to apply when it comes to cyber operations against dual-use objects, such as power systems, which enable activities not only of civilians but also of military logistics. While article 52 of Additional Protocol I protects civilian objects, it does not provide any clarification as to how to classify digital objects that serve for both civilian and military purposes.

## *B. Proportionality Principle*

The principle of proportionality prohibits operations which are expected to inflict excessive damage to civilians in relation to the particular military advantage to be obtained. With cyber warfare, it becomes increasingly difficult to evaluate the principle of proportionality, as its impact tends to be indirect, delayed, or difficult to predict. For example, a cyber attack on an electricity network may aim at disrupting military activities but result in a blackout that affects hospitals, public transport, and water supply systems as well. This uncertainty connected with humanitarian implications makes the application of proportionality in cyber warfare very complicated. Various authors including Marco Roscini in 2021 point out that the lack of strict technical and legal standards for estimating damage in the cyber sphere has made the use of the principle of proportionality highly speculative.[35]

Additionally, civilian casualties from cyber operations do not always involve any physical damage. For example, losing access to medical services, hindering food supplies, or disrupting emergency communications may lead to significant humanitarian harm even without any physical damage to the infrastructure. Still, many states choose to interpret the principle of proportionality in a narrow sense, focusing almost entirely on the physical impact.[36]

---

[35] Marco Roscini, "Cyber Operations as a Use of Force," in *Research Handbook on International Law and Cyberspace*, ed. Nicholas Tsagourias and Russell Buchan (Edward Elgar Publishing, 2021), https://doi.org/10.4337/9781789904253.00025.

[36] Giacomo Biggio, "Regulating Non-Kinetic Effects of Cyber Operations: The 'Loss Of Functionality' Approach and The Military Necessity-Humanity Balance Under International Humanitarian Law," *Journal of Conflict and Security Law* 30, no. 2 (July 2025): 241–63, https://doi.org/10.1093/jcsl/kraf008.

One more consequence of this is the issue of the time gap between the initial action and its secondary effects. For example, a cyber operation disrupting the supply chain at hospitals may not lead to loss of lives at once, but if the system for treating patients is disrupted for a long time, the humanitarian outcomes may be devastating. International humanitarian law does not yet have a clear position on how the absence of physical impact or damage to the data should be perceived in the framework of the principle of proportionality.

The problems are especially visible in cases of cyber operations that target medical infrastructures as well and show the insufficiency of proportionate assessments concerning humanitarian harm that is not physical. The health sector has become a target for cyber-attacks in the last five years during both peace and war. Incidents like WannaCry that took place in 2017 can still serve as examples in discussions on cybersecurity that take place in 2024.[37] Nevertheless, from 2020 to 2023, there was a rise in both the number and seriousness of cyber-attacks on medical systems directly affecting human safety.

The World Health Organization's 2021 report, CyberPeace Institute's report in 2022,[38] and ENISA's 2023[39] report confirmed an uptick in hacking activities against hospitals in Europe, North America, Canada, India, and Australia during the COVID 19 crisis. University Hospital Brno in Czech Republic suffered a cyber attack which affected its surgical services and intensive care activities. Likewise, the ransomware attack on the Irish Health Service Executive occurred in May 2021 resulting in the paralysis of almost the entire healthcare system of Ireland for weeks.[40]

Even though these events happened outside of any war surroundings, the impact of the same kinds of events will be worse in a conflict. Under the laws of war, hospitals earn special protection per the Geneva Conventions and the Protocol I and II. However, it must be noted that specific constitutional developments concerning the protection of hospitals digitally do not exist. The Red Cross has stressed that cyber

[37] Budi Hartono, "Ransomware: Memahami Ancaman Keamanan Digital," *Bincang Sains Dan Teknologi* 2, no. 02 (May 2023): 55–62, https://doi.org/10.56741/bst.v2i02.353.

[38] Brm Yehizkia Y. Kristalia and Indra Wisnu Wibisono, "Ancaman Siber Dan Penguatan Kedaulatan Digital Indonesia Dari Perspektif Geopolitik Digital," *Jurnal Ilmiah Multidisiplin* 3, no. 02 (March 2024): 83–93, https://doi.org/10.56127/jukim.v3i02.1584.

[39] Kristalia and Wibisono, "Ancaman Siber".

[40] Kristalia and Wibisono, "Ancaman Siber".

attacks against hospitals can represent serious international humanitarian law violations.[41]

These occurrences show that cyber actions can result in dire humanitarian outcomes without causing any human devastation. The definition of proportionality under International Humanitarian Law is usually limited to physical damage, while the technological impairment of medical services, the slowdown of medical treatments, and the interruption of rescue operations are given far less attention. Therefore, current evaluations of proportionality do not reflect the actual humanitarian effects of cyber activities.

## *C. Precaution Principle*

The principle of precaution requires parties conducting attacks to take all feasible measures to minimize risks to civilians and civilian objects. In digital warfare, the implementation of this principle encounters significant technical and structural obstacles. Not all parties to a conflict possess sufficient intelligence capabilities or technical capacity to identify the interdependencies between targeted systems and the essential public services that rely upon them.[42]

For instance, a cyber operation directed against military fuel supply systems may weaken military logistics. However, where such networks are also integrated with energy supplies for hospitals or clean water systems, harm to civilians may be unavoidable. In such circumstances, the application of the principle of precaution necessitates a comprehensive assessment of the digital networks being targeted. In practice, however, most States lack transparency mechanisms concerning the structure of their digital infrastructure. As a result, attackers may not have adequate information to prevent civilian harm, even where there is an intention to do so.

The Tallinn Manual 2.0 affirms that attackers are required to assess the foreseeable effects of an operation and to suspend or cancel an attack

[41] International Committee of the Red Cross, *Protection of Medical Personnel, Units and Transports During Armed Conflict* (2025), https://www.icrc.org/sites/default/files/2025-02/06_Medical_facilities.pdf.

[42] Takdir Mattanete et al., "Paradoks Hukum Humaniter Di Era Perang Siber Dan Drone: Antara Kepatuhan Normatif Dan Realitas Operasional," *Jurnal Ilmu Hukum, Humaniora Dan Politik* 5, no. 5 (June 2025): 4278–83, https://doi.org/10.38035/jihhp.v5i5.4919.

where it is likely to cause disproportionate civilian harm.[43] Nonetheless, given its non-binding nature, the Manual does not impose legally enforceable obligations upon States.

The contemporary cyber incidents reveal the interpretive and operational considerations related to humanitarian issues associated with the disruption of vital infrastructure. For instance, the Colonial Pipeline incident in the USA in 2021 proved to be one of the most frequently discussed cases concerning the impact of cyberattacks on the energy sector. Although the incident was caused by the crime group named DarkSide rather than the state actor in the framework of military activity, it had serious consequences for global security. The disruption of fuel supply led to the public's panic and price surge, besides serious disruptions in logistical distribution networks.[44]

In the framework of military conflicts, cyber attacks on the energy sector can cause lots of humanitarian consequences. If a similar incident was to take place during the war, its effects would be a clear breach of proportionality and civilian object protection principles set forth by International Humanitarian Law. Moreover, strikes on energy distribution systems cause negative consequences for the functioning of hospitals, the food distribution systems, and the transport systems, which may amplify humanitarian impacts on the civilian population.

The Colonial Pipeline case shows that the preventive mandates of Article 57 of Additional Protocol I were mostly created for traditional attacks, thus giving little direction on implementing preventive measures in cyberspace. The modern conflicts require precautionary measures that cover such aspects as cyber resilience, segmentation, redundancy measures, and digital contingency planning.

## *D. Classification of Civilian Objects vs. Military Objectives*

[43] Michael N Schmitt, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*.

[44] Manav Mittal, "Colonial Pipeline Cyberattack Drives Urgent Reforms in Cybersecurity and Critical Infrastructure Resilience," *International Journal of Oil, Gas and Coal Engineering* 12, no. 5 (December 2024): 106–19, https://doi.org/10.11648/j.ogce.20241205.11.

In traditional warfare, military targets must be determined by their potential contributions to warfare,[45] but in cyberspace it is much less clear-cut. Many important legal questions arise: Are computer servers, data centers, or civilian lines of communication which are also used for military purposes legitimate military targets? And if the answer is affirmative, to what extent is civilian immunity still guaranteed?

In effect, numerous countries combine civilian and military infrastructure into a new technological network. The national Internet, governmental servers, and satellite communications for civilians may at the same time assist military operations. The presence of the above-mentioned factors will eliminate the civilian character of such objects.

The report from the ICRC published in 2022 underlined that the combination of civilian systems with military ones increases the level of the attacks on civilian population and undermines the very essence of international humanitarian law, which is to protect civilians.[46]

Further debate concerns the status of data as an object of attack. Traditional humanitarian law has historically focused on physical objects as the primary reference point. In the digital environment, however, data and information systems may constitute the principal targets of cyber operations without causing physical destruction.[47] Academic discussions over the past five years, including analyses by Kubo Mačák in 2021[48] and Liis Vihul in 2020,[49] have argued that the destruction or manipulation of data may qualify as an attack where it significantly disrupts the functioning of civilian infrastructure.

These legal uncertainties are clearly illustrated by the prolonged cyber confrontation between Israel and Iran over the past decade. Over

---

[45] Art. 52(2), Additional Protocol I, Geneva Conventions of 1949, https://www.icrc.org/sites/default/files/external/doc/en/assets/files/publications/icrc-002-0173.pdf.

[46] International Committee of the Red Cross (ICRC), *International Humanitarian Law Imposes Essential Limits on the Conduct of Cyber Operations*, n.d., https://www.icrc.org/en/document/international-humanitarian-law-limits-cyber-operations?utm_source=chatgpt.com.

[47] Biggio, "Regulating Non-Kinetic Effects of Cyber Operations."

[48] Kubo Mačák, "Unblurring the Lines: Military Cyber Operations and International Law," *Journal of Cyber Policy* 6, no. 3 (September 2021): 411–28, https://doi.org/10.1080/23738871.2021.2014919.

[49] Liis Vihul et al., "International Legal Regulation of Autonomous Technologies," in *Modern Conflict and Artificial Intelligence* (Centre for International Governance Innovation, 2020), https://www.cigionline.org/sites/default/files/documents/Modern%20Conflict%20and%20AI_web_0.pdf.

the past decade, Israel and Iran have been engaged in a low intensity cyber conflict targeting water facilities, ports, military systems, and civilian networks. In 2020, Iran was allegedly responsible for a cyber operation against Israel's water management system, which, if successful, could have contaminated drinking water supplies. In response, Israel was widely believed to have conducted a cyber operation against Iran's Shahid Rajaee port, resulting in significant disruption to civilian logistics and international trade.[50]

From the perspective of International Humanitarian Law, these incidents raise critical legal questions. First, can public water systems and civilian ports be classified as lawful military objectives? Second, can non physical cyber operations that cause serious disruption to civilian life be considered violations of humanitarian law? To date, no international enforcement mechanism has been applied in relation to either incident.

Moreover, since the Israel-Iran conflict has not been recognized officially as a military conflict, many experts argue that cyber operations in this context can be characterized as hostile actions.[51] Nonetheless, the reality of these operations' consequences on civilian life makes it important to rethink existing regulations. This is vital to make sure that cyber operations that affect humanitarian protections still belong to the scope of International Humanitarian Law even if they take place outside recognized military conflict.

Cyberattacks on water facilities or ports make it evident that many forms of digital infrastructure can be used for military and civilian purposes at the same time. Still, existing International Humanitarian Law does not provide sufficiently clear criteria regarding when such dual purpose infrastructure loses civilian protection.

## *E. Synthesis of Interpretative Challenges Revealed by Contemporary Cyber Operations*

The foregoing analysis demonstrates that contemporary cyber operations against Critical National Infrastructure expose a series of

[50] Laila Rizky Amaliya, "A Cyber War of Iran-Israel: A Geopolitical Rivalry," in *Proceedings of the International Conference on Strategic and Global Studies (ICSGS 2024)*, vol. 33, ed. Ibrahim Kholilul Rohman et al., Atlantis Highlights in Social Sciences, Education and Humanities (Dordrecht: Atlantis Press International BV, 2025), 45–56, https://doi.org/10.2991/978-94-6463-646-8_4.

[51] Stuart Casey-Maslen et al., "Towards a Definition of Hybrid Warfare," in *Maritime Security Law in Hybrid Warfare*, ed. Alexander Lott (Brill | Nijhoff, 2024), 7–27, https://doi.org/10.1163/9789004707993_003.

interconnected interpretative challenges that substantially limit the effectiveness of International Humanitarian Law. Instead of being considered isolated cases, the events of the Russia–Ukraine war, attacks against the medical establishment, Israel–Iran cyber war, and the Colonial Pipeline case show patterns showing that existing international standards are unable to regulate responsible cyber attacks against key infrastructure. The presented cases show that complications are of the issue of applicability of IHL in cyberspace rather than the new way of interpreting it.

The first challenge pertains to applying the principle of distinction within the context of dual-use and digitized infrastructure. Evidence from cyber attacks on Ukraine's electricity grid and attacks on water utilities in the Israel-Iran war shows that a large portion of today's critical infrastructure serves both military and civilian purposes.[52] Electricity networks, means of communication, cloud computing governmental services, and satellite systems are widely used both by humans and militaries.[53] Although Article 52 of the Additional Protocol I states that the civilian objects are protected unless they become military objectives, it is not clear when dual-use digital infrastructure loses its protected status. As a result, the line between legal military objectives and protected civilian objects becomes less clear in cyberspace.

Another problem comes from the need to interpret the principle of proportionality in terms of non-physical humanitarian harm. The attacks on healthcare systems and the Colonial Pipeline show that cyber operations can have humanitarian effects without inflicting visible damage.[54] Interruptions to electricity, hospital services, transport systems, food delivery, and emergency communications can cause civilian populations to face life-threatening situations even without physical

[52] Amaliya, "A Cyber War of Iran-Israel."

[53] Holger Lueschow and Roberto Pelaez, "Satellite Communication for Security and Defense," in *Handbook of Space Security*, ed. Kai-Uwe Schrogl (Cham: Springer International Publishing, 2020), 779–96, https://doi.org/10.1007/978-3-030-23210-8_107; see also Elizabeth Seebode Waldrop, "Integration of Military and Civilian Space Assets : Legal and National Security Implications" (McGill University, 2003), https://doi.org/10.82308/5745.

[54] Ana Maria Costea, "The Possibility of a Cyberwar: Accountability, Ever-Evolving Threats, No Ultimate Weapon, Threshold, Armed Attack," in *Cyber Deterrence and State Response in the Age of Technology*, by Ana Maria Costea, Contributions to International Relations (Cham: Springer Nature Switzerland, 2026), 167–207, https://doi.org/10.1007/978-3-032-13450-9_5.

damage.[55] However, proportionality assessments under conventional international humanitarian law have been based mainly on measurable physical destruction and civilian casualties. The existing interpretation of law fails to allow for an assessment of humanitarian harm from the malfunctioning of digital systems, disruptions of service, and the failure of interdependent systems. This gap excludes some of the most serious humanitarian effects of cyber operations from comprehensive legal analysis.

The third issue is related to applying the precautionary principle in cyberspace. Cyberattacks differ from conventional military operations because they can occur instantly and in several jurisdictions without sending troops to perform them, thus making it impossible to apply the most precautionary measures described in Article 57 of Additional Protocol I.[56] In addition, the interconnectedness of the cyber infrastructure makes the obligations to prevent cyberattacks even more difficult to fulfill since a cyberattack targeted at a particular object can also affect other connected civilian objects.[57] Therefore, the existing precautionary framework must be changed to include cybersecurity measures such as segmentation of the networks, duplication of important systems, preparation of response plans in case of incidents, cyber resilience, and many others.

In sum, the cases studied illustrate the ongoing challenges of attribution and accountability. The presence of state-sponsored groups, proxy actors, amateur hackers, and global criminal networks makes the identification of accountable individuals complex. The Russia-Ukraine war exemplifies how cyberspace operations are increasingly executed through decentralized systems that hide the actual involvement of states, though still achieving strategic military results. Absent the principle of attribution, the application of state responsibility and implementation of international humanitarian law is bound to remain limited, resulting in lack of

[55] Jonathan Matusitz and Elizabeth Minei, "Cyberterrorism: Its Effects on Health-Related Infrastructures," *Journal of Digital Forensic Practice* 2, no. 4 (September 2009): 161–71, https://doi.org/10.1080/15567280802678657.

[56] Kosmas Pipyros et al., "Cyberoperations and International Humanitarian Law: A Review of Obstacles in Applying International Law Rules in Cyber Warfare," *Information & Computer Security* 24, no. 1 (March 2016): 38–52, https://doi.org/10.1108/ICS-12-2014-0081.

[57] Martti Lehto, "Cyber-Attacks Against Critical Infrastructure," in *Cyber Security*, vol. 56, ed. Martti Lehto and Pekka Neittaanmäki, Computational Methods in Applied Sciences (Cham: Springer International Publishing, 2022), 3–42, https://doi.org/10.1007/978-3-030-91293-2_1.

accountability for such major cyber incidents affecting civilian infrastructure.[58]

These various challenges show that the main flaw of modern International Humanitarian Law is not that there are legal rules and regulations but rather that their current interpretation is inadequate for cyber attacks against Critical National Infrastructure. The case studies carried out provides the same conclusions: rules made for the purposes of traditional warfare are unable to manage non-physical influence, digital connectivity, multifunctionality of infrastructure along with the anonymity of cyberspace. Hence, this section will present the idea that the improvement of protection of Critical National Infrastructure is additionally about the expansion of applicability of International Humanitarian Law to cyberspace along with the advancement of new legal standards suitable for technological warfare.

# Strengthening International Humanitarian Law Protection for Critical National Infrastructure

## *A. Recognizing Digital Critical Infrastructure as Protected Civilian Objects*

The first and most urgent reform concerns the explicit recognition of digital critical infrastructure as protected civilian objects under International Humanitarian Law. Contemporary armed conflicts increasingly depend on digital systems that sustain electricity distribution, healthcare services, water management, transportation, banking, and public administration.[59] Although these systems are indispensable to civilian survival, existing treaty law remains largely focused on physical objects and provides only limited guidance regarding the legal status of the

[58] Fadhli Muhaimin Ishaq, "Forced Displacement and Blockade Reviewed From International Humanitarian Law: A Case Study of the Humanitarian Attacks in Rafah," *Uti Possidetis: Journal of International Law* 5, no. 3 (October 2024): 420–54, https://doi.org/10.22437/up.v5i3.36281.

[59] François Delerue, *Cyber Operations and International Law*, Cambridge Studies in International and Comparative Law 146 (Cambridge, United Kingdom ; New York, NY, USA: Cambridge University Press, 2020).

digital infrastructure that enables such services.[60] To strengthen civilian protection, states and international organizations should adopt a functional approach that treats digital infrastructure supporting essential civilian services as civilian objects unless it makes a direct and substantial contribution to military operations. Such recognition would reduce interpretative ambiguity and reinforce the humanitarian purpose underlying Articles 48 and 52 of Additional Protocol I.

## *B. Expanding Proportionality Assessments to Include Non-Physical Harm*

International Humanitarian Law should also adapt its provisions so as to include the idea that civilian damage related to cyber attacks is not only related to material destruction. Even if no buildings are damaged, the disruption of hospital systems, power grid, water supply, food supply chain, and emergency communication may cause significant humanitarian damage as well. Proportionality assessments should therefore explicitly include foreseeable humanitarian implications related to the interruption of vital services, disruption of medical treatment, chain of failures, and all consequences which can be detrimental to the safety of civilians.

## *C. Developing Precautionary Obligations for Cyber Operations*

In addition to proportionality considerations, precautionary obligations must be modified for the cyber context. The traditional precautionary measures were created primarily with classic military operations in mind, and thus they do not deal with the interrelated character of the digital infrastructure.[61] As a result, the conflicting parties should be obliged before engaging in any actions against the systems implicated in providing crucial services for civilians to make a thorough risk assessment concerning cybersecurity. This risk assessment should encompass the assessment of dependencies between different networks and identifying the likelihood of overwhelm effects and feasible technical measures, which include network segregation and redundancy and

[60] Michael N. Schmitt, ed., *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, 2nd ed. (Cambridge University Press, 2017), https://doi.org/10.1017/9781316822524.

[61] Nehaluddin Ahmad and Ahmad Masum, "Cyber Operations and the Redefinition of Modern Warfare," *Journal of Information Assurance & Cybersecurity*, March 3, 2026, 1–12, https://doi.org/10.5171/2026.300029.

emergency-recovery procedures. Integrating these measures for cyber resilience into the general understanding of the Article 57 of Additional Protocol I would significantly strengthen the protection of civilians against highly avoidable harm resulting from the cyberspace activities.

### *D. Strengthening Attribution and International Accountability*

To promote effective Critical National Infrastructure protection, it is necessary to adopt new methods to attribute activities in cyberspace and to hold parties responsible for these actions. The rise of involvement of proxy entities, amateur hackers, cyber mercenaries, and state-sponsored organization [62] has made it extremely challenging to locate those responsible for such actions in the context of law. Consequently, countries should facilitate the formation of independent international attribution mechanisms that will guarantee technological investigation and make unbiased conclusions about major cyber activities concerning civilian infrastructure. It is also essential to enhance cooperation in cyber investigation and information sharing efforts in order to increase the amount of evidence for state responsibility and application of International Humanitarian Law in cyberspace.

## Lessons for Southeast Asia: Strengthening Critical National Infrastructure Protection Against Cyber Operations

The transformation of public management, energy systems, finance, healthcare, transport, telecommunications industry is increasing the susceptibility of Southeast Asia to the threat of cyber operations involving Critical National Infrastructure (CNI).[63] Although this region has not been subject to cyber attacks of the magnitude that took place during the Russia–Ukraine war, the fact that vital public services depend on interconnected digital systems suggests the possibility of similar human costs should inter-state relations deteriorate and war breaks out.

[62] Johan Sigholm, "Non-State Actors in Cyberspace Operations," *Journal of Military Studies* 4, no. 1 (December 2013): 1–37, https://doi.org/10.1515/jms-2016-0184.

[63] Michael Raska and Benjamin Ang, "Cybersecurity in Southeast Asia," *Paris: Asia Centre & DGRIS*, 2018, 1–9.

Therefore, the experiences gained from the legal aspects concerned with contemporary cyber war must be viewed not in a confined geographical context but as an important factor contributing to legal preparedness of Southeast Asia.

Indonesia serves as an example of how Critical National Infrastructure can be both secured and jeopardized in a world that is becoming increasingly digitalized. The creation of the National Cyber and Crypto Agency (BSSN) [64] together with the formulation of national strategies in the area of cybersecurity and outlining of Critical Information Infrastructure demonstrates more and more awareness of the importance of cyber resilience for national security. [65] However, the existing regulations of Indonesia's law when it comes to cybersecurity revolve around national resilience, prevention of cybercrime, and digital governance. Thus, the IHL provisions concerning potential responsibilities arising from cyber operations carried out in the course of an international armed conflict, remain unregulated. In particular, Indonesian law does not provide for using humanitarian principles that govern the protection of civilian digital infrastructure ensuring provision of essential public services.[66]

The model of critical infrastructure protection that Singapore has is rather institutionalized in nature. The government of Singapore issues the Cybersecurity Act, and at the same time, the government's Cyber Security Agency oversees the operators of Critical Information Infrastructure that have relevant obligations regarding cybersecurity, reporting obligations concerning incidents, and security assessments. The experience and practices that Singapore implements show that it is possible to improve cyber resilience significantly by employing binding regulation in peacetime conditions. [67] However, similarly to Indonesia, Singapore's legislative

---

[64] Muhammad Prakoso Aji, Gumilar Rusliwa Somantri, and Muhammad Syaroni Rofii, "The Strategic Role of the National Cyber and Crypto Agency (BSSN) in Maintaining State Sovereignty in Cyberspace," *Journal of Law, Politic and Humanities* 5, no. 5 (July 2025): 3916–24, https://doi.org/10.38035/jlph.v5i5.1973.

[65] Agus Haryanto and Satya Muhammad Sutra, "Upaya Peningkatan Keamanan Siber Indonesia Oleh Badan Siber Dan Sandi Negara (BSSN) Tahun 2017-2020," *Global Political Studies Journal* 7, no. 1 (April 2023): 56–69, https://doi.org/10.34010/gpsjournal.v7i1.8141.

[66] Ahmad M. Ramli et al., "The Urgency of Regulating Artificial Intelligence in Relation to Cybersecurity and Cyber Resilience," *Cogent Social Sciences* 12, no. 1 (December 2026): 2632977, https://doi.org/10.1080/23311886.2026.2632977.

[67] Benjamin Ang, "Cybersecurity and Legislation: The Case Study of Singapore," in *Cybersecurity and Legal-Regulatory Aspects*, by Gabi Siboni and Limor Ezioni (World Scientific, 2021), 89–102, https://doi.org/10.1142/9789811219160_0004.

framework is aimed mainly at their peacetime needs, and there is very little guidance concerning how IHL regulations can be applied during armed conflicts.[68]

The examination of Indonesia with Singapore illustrates that Southeast Asia countries have achieved genuine reforms in cybersecurity regulation. Nevertheless, humanitarian aspects of cyber warfare have not been comprehensively integrated into the legal systems of the Southeast Asian states. This phenomenon is indicative of a peculiar tendency observed in the region whereby cyber threats are commonly viewed as phenomena of either national security, economic stability, or cyber crime instead of as aspects of danger for civilians in instances of armed conflicts.

At the regional level, ASEAN has a chance to make the most of the unique opportunity to close the normativity gap by adding concepts of humanitarian law to its existing cooperation in the field of cybersecurity. Though the ASEAN Cybersecurity Cooperation Strategy and various related programs provide for building capacity, sharing information, as well as establishing measures to build confidence, any of the aforementioned initiatives can be classified mainly as preventive and technical measures.[69] Therefore, further regional collaboration can be related to the establishment of principles, which would result in extending cybersecurity regulation to the policies concerning critical national infrastructure protection. This can involve various initiatives, which can include developing regional rules for civilian digital infrastructure protection during times of war, facilitating separation of civilian and military digital systems, conducting joint exercises of response to cyber-incidents under the humanitarian scenarios and developing the cooperation of the countries of the region in the sphere of attribution and technical investigations.

The different incidents analyzed within the current research, including cyber actions against the electric grid of Ukraine, strikes on medical facilities, disturbances relating to energy infrastructures, and cyber attacks targeting the water supply systems, are valuable for ASEAN countries in terms of possible implications and lessons. Instead of waiting until similar episodes take place in the region, they need to implement

[68] Ron Matthews and Fitriani Bintang Timur, "Singapore's 'Total Defence' Strategy," *Defence and Peace Economics* 35, no. 5 (July 2024): 638–58, https://doi.org/10.1080/10242694.2023.2187924.

[69] Candice Tran Dai and Miguel Alberto Gomez, "Challenges and Opportunities for Cyber Norms in ASEAN," *Journal of Cyber Policy* 3, no. 2 (May 2018): 217–35, https://doi.org/10.1080/23738871.2018.1487987.

proactive legal and regulatory measures that treat digital critical infrastructure as an important humanitarian issue. The introduction of International Humanitarian Law into the regional cybersecurity regulations would promote the legal readiness for future armed conflicts and improve the dedication of ASEAN to regional stability, protection of civilians, and democratic principles.

# Conclusion

The protection of vital infrastructure against cyber attacks under International Humanitarian Law faces profound challenges due to the absence of explicit positive legal rules recognizing digital systems as civilian objects, despite the growing dependence of essential public services such as electricity, water, health care, and communications on digital infrastructure whose disruption may generate humanitarian consequences comparable to or even exceeding those of kinetic attacks. Although cyber operations can paralyze critical services without causing immediate physical destruction, the principles of distinction and proportionality remain predominantly anchored in assessments of material damage and civilian casualties, rendering them ill-equipped to address the destructive potential of non-kinetic harm. The ambiguous status of multifunctional or dual-use infrastructure, the lack of coherent and robust global protection standards, and the prevalence of unilateral state interpretations further exacerbate civilian vulnerability when hostilities extend into the digital domain. At the same time, persistent attribution difficulties and the absence of effective accountability mechanisms expand the space for impunity for both state and non-state actors, enabling forms of concealed warfare that inflict severe yet often invisible harm on civilian life. Unless binding normative developments are pursued and International Humanitarian Law principles are meaningfully integrated into national cyber policies, the law risks losing its practical relevance and failing in its foundational purpose of safeguarding humanity in armed conflict; consequently, normative reformulation, progressive reinterpretation of existing principles, and the creation of credible enforcement and accountability frameworks are imperative to ensure sustained civilian protection in the era of digital warfare.

# References

Abraham, Doney, Siv Hilde Houmb, and Laszlo Erdodi. “Cyber-Attacks on Energy Infrastructure - A Literature Overview and Perspectives

on the Current Situation." *Applied Sciences* 15, no. 17 (August 2025): 9233. https://doi.org/10.3390/app15179233.

Ahmad, Nehaluddin, and Ahmad Masum. "Cyber Operations and the Redefinition of Modern Warfare." *Journal of Information Assurance & Cybersecurity*, March 3, 2026, 1–12. https://doi.org/10.5171/2026.300029.

Aji, Muhammad Prakoso, Gumilar Rusliwa Somantri, and Muhammad Syaroni Rofii. "The Strategic Role of the National Cyber and Crypto Agency (BSSN) in Maintaining State Sovereignty in Cyberspace." *Journal of Law, Politic and Humanities* 5, no. 5 (July 2025): 3916–24. https://doi.org/10.38035/jlph.v5i5.1973.

Alamsyah, Yazid Akbar, and Rafi Ilyasa Ibnu Akbar. "Penggunaan Persenjataan Modern Dalam Konflik Bersenjata Ditinjau Dari Prinsip Hukum Humaniter Dan Hukum Islam." *Sanskara Hukum Dan HAM* 3, no. 01 (August 2024): 24–33. https://doi.org/10.58812/shh.v3i01.434.

Alexandru, Adriana, Victor Vevera, and Ella Magdalena Ciupercă. "National Security and Critical Infrastructure Protection." *International Conference Knowledge-Based Organization* 25, no. 1 (June 2019): 8–13. https://doi.org/10.2478/kbo-2019-0001.

Aljohani, Tawfiq M. "Cyberattacks on Energy Infrastructures as Modern War Weapons - Part I: Analysis and Motives." *IEEE Technology and Society Magazine* 43, no. 2 (June 2024): 59–69. https://doi.org/10.1109/MTS.2024.3395688.

Amaliya, Laila Rizky. "A Cyber War of Iran-Israel: A Geopolitical Rivalry." In *Proceedings of the International Conference on Strategic and Global Studies (ICSGS 2024)*, vol. 33, edited by Ibrahim Kholilul Rohman, Wu Zhaoyang, Mohammad Izdiyan Muttaqin, Ismail Suardi Wekke, and Irene Sondang Fitrinitia, 45–56. Atlantis Highlights in Social Sciences, Education and Humanities. Dordrecht: Atlantis Press International BV, 2025. https://doi.org/10.2991/978-94-6463-646-8_4.

America's Cyber Defense Agency. *Update: Destructive Malware Targeting Organizations in Ukraine*. n.d. https://www.cisa.gov/news-events/alerts/2022/02/26/update-destructive-malware-targeting-organizations-ukraine.

Ang, Benjamin. "Cybersecurity and Legislation: The Case Study of Singapore." In *Cybersecurity and Legal-Regulatory Aspects*, by Gabi Siboni and Limor Ezioni, 89–102. World Scientific, 2021. https://doi.org/10.1142/9789811219160_0004.

Azzahra, Nadia, and Lina Hastuti. "Analisis Hukum Humaniter Internasional Terhadap Penyerangan Dual Use Object Dalam Konflik Bersenjata Rusia Dan Ukraina." *Jurist-Diction* 8, no. 1 (January 2025): 91–118. https://doi.org/10.20473/jd.v8i1.54375.

Benmalek, Mourad. "Ransomware on Cyber-Physical Systems: Taxonomies, Case Studies, Security Gaps, and Open Challenges." *Internet of Things and Cyber-Physical Systems* 4 (2024): 186–202. https://doi.org/10.1016/j.iotcps.2023.12.001.

Biggio, Giacomo. "Regulating Non-Kinetic Effects of Cyber Operations: The 'Loss Of Functionality' Approach and The Military Necessity-Humanity Balance Under International Humanitarian Law." *Journal of Conflict and Security Law* 30, no. 2 (July 2025): 241–63. https://doi.org/10.1093/jcsl/kraf008.

BöRöCZ, Miklós. "Critical Infrastructure Protection Policy in the EU." *Strategic Impact* 80, no. 3 (February 2022): 46–61. https://doi.org/10.53477/1841-5784-21-15.

Casey-Maslen, Stuart, Arne Willy Dahl, Sofia Galani, and Alexander Lott. "Towards a Definition of Hybrid Warfare." In *Maritime Security Law in Hybrid Warfare*, edited by Alexander Lott, 7–27. Brill | Nijhoff, 2024. https://doi.org/10.1163/9789004707993_003.

Costea, Ana Maria. "The Possibility of a Cyberwar: Accountability, Ever-Evolving Threats, No Ultimate Weapon, Threshold, Armed Attack." In *Cyber Deterrence and State Response in the Age of Technology*, by Ana Maria Costea, 167–207. Contributions to International Relations. Cham: Springer Nature Switzerland, 2026. https://doi.org/10.1007/978-3-032-13450-9_5.

Delerue, François. *Cyber Operations and International Law*. Cambridge Studies in International and Comparative Law 146. Cambridge, United Kingdom ; New York, NY, USA: Cambridge University Press, 2020.

Di Pietro, Roberto, Simone Raponi, Maurantonio Caprolu, and Stefano Cresci. "Critical Infrastructure." In *New Dimensions of Information Warfare*, vol. 84, by Roberto Di Pietro, Simone Raponi, Maurantonio Caprolu, and Stefano Cresci, 157–96. Advances in Information Security. Cham: Springer International Publishing, 2021. https://doi.org/10.1007/978-3-030-60618-3_5.

Dr. A.Shaji George, Dr. T.Baskar, and Dr. P.Balaji Srikaanth. *Cyber Threats to Critical Infrastructure: Assessing Vulnerabilities Across Key Sectors*. February 25, 2024. https://doi.org/10.5281/ZENODO.10639463.

European Council. *Sanctions Against Cyber-Attacks*. May 12, 2025. https://www.consilium.europa.eu/en/policies/sanctions-against-cyber-attacks/.

Geneva Conventions of 1949. https://www.icrc.org/sites/default/files/external/doc/en/assets/files/publications/icrc-002-0173.pdf.

Gunakaya, A. Widiada. *Hukum Pidana Internasional*. Takaza Innovatix Labs, 2024.

Hartono, Budi. "Ransomware: Memahami Ancaman Keamanan Digital." *Bincang Sains Dan Teknologi* 2, no. 02 (May 2023): 55–62. https://doi.org/10.56741/bst.v2i02.353.

Haryanto, Agus, and Satya Muhammad Sutra. "Upaya Peningkatan Keamanan Siber Indonesia Oleh Badan Siber Dan Sandi Negara (BSSN) Tahun 2017-2020." *Global Political Studies Journal* 7, no. 1 (April 2023): 56–69. https://doi.org/10.34010/gpsjournal.v7i1.8141.

He, Ying, Aliyu Aliyu, Mark Evans, and Cunjin Luo. "Health Care Cybersecurity Challenges and Solutions Under the Climate of COVID-19: Scoping Review." *Journal of Medical Internet Research* 23, no. 4 (April 2021): e21747. https://doi.org/10.2196/21747.

IBM Security X-Force. *X-Force Threat Intelligence Index 2023*. n.d. https://secure-iss.com/wp-content/uploads/2023/02/IBM-Security-X-Force-Threat-Intelligence-Index-2023.pdf?utm_source=chatgpt.com.

International Committee of the Red Cross. *Protection of Medical Personnel, Units and Transports During Armed Conflict*. 2025. https://www.icrc.org/sites/default/files/2025-02/06_Medical_facilities.pdf.

International Committee of the Red Cross (ICRC). *Cyber and Information Operations and International Humanitarian Law*. n.d. https://www.icrc.org/en/law-and-policy/cyber-and-information-operations.

———. *International Humanitarian Law Imposes Essential Limits on the Conduct of Cyber Operations*. n.d. https://www.icrc.org/en/document/international-humanitarian-law-limits-cyber-operations?utm_source=chatgpt.com.

Ishaq, Fadhli Muhaimin. "Forced Displacement and Blockade Reviewed From International Humanitarian Law: A Case Study of the Humanitarian Attacks in Rafah." *Uti Possidetis: Journal of International*

*Law* 5, no. 3 (October 2024): 420–54. https://doi.org/10.22437/up.v5i3.36281.

Khoirunnisa, Khoirunnisa, and Cristy Sugiati. "Cyber Warfare Strategies in the Russia-Ukraine Conflict (2021-2022): Implications for National Security and Modern Warfare." *Jurnal Public Policy* 10, no. 2 (April 2024): 138. https://doi.org/10.35308/jpp.v10i2.9026.

Kristalia, Brm Yehizkia Y., and Indra Wisnu Wibisono. "Ancaman Siber Dan Penguatan Kedaulatan Digital Indonesia Dari Perspektif Geopolitik Digital." *Jurnal Ilmiah Multidisiplin* 3, no. 02 (March 2024): 83–93. https://doi.org/10.56127/jukim.v3i02.1584.

Lehto, Martti. "Cyber-Attacks Against Critical Infrastructure." In *Cyber Security*, vol. 56, edited by Martti Lehto and Pekka Neittaanmäki, 3–42. Computational Methods in Applied Sciences. Cham: Springer International Publishing, 2022. https://doi.org/10.1007/978-3-030-91293-2_1.

———. "Cyber-Attacks Against Critical Infrastructure." In *Cyber Security*, vol. 56, edited by Martti Lehto and Pekka Neittaanmäki, 3–42. Computational Methods in Applied Sciences. Cham: Springer International Publishing, 2022. https://doi.org/10.1007/978-3-030-91293-2_1.

Locatelli, Andrea. "Critical Infrastructure Protection." In *Technology and International Relations*, edited by Giampiero Giacomello, Francesco N. Moro, and Marco Valigi. Edward Elgar Publishing, 2021. https://doi.org/10.4337/9781788976077.00016.

Lueschow, Holger, and Roberto Pelaez. "Satellite Communication for Security and Defense." In *Handbook of Space Security*, edited by Kai-Uwe Schrogl, 779–96. Cham: Springer International Publishing, 2020. https://doi.org/10.1007/978-3-030-23210-8_107.

Mačák, Kubo. "Unblurring the Lines: Military Cyber Operations and International Law." *Journal of Cyber Policy* 6, no. 3 (September 2021): 411–28. https://doi.org/10.1080/23738871.2021.2014919.

Markopoulou, Dimitra, and Vagelis Papakonstantinou. "The Regulatory Framework for The Protection of Critical Infrastructures Against Cyberthreats: Identifying Shortcomings and Addressing Future Challenges: The Case of The Health Sector in Particular." *Computer Law & Security Review* 41 (July 2021): 105502. https://doi.org/10.1016/j.clsr.2020.105502.

Maskun, Maskun, Irwansyah Irwansyah, Ahsan Yunus, Armelia Safira, and Siti Nurhalima Lubis. "Cyber-Attack: Its Definition, Regulation, and ASEAN Cooperation to Handle with It." *Jambe Law Journal* 4,

no. 2 (November 2021): 131–50. https://doi.org/10.22437/jlj.4.2.131-150.

Mattanete, Takdir, Joko Wahyudi, Tarsisius Susilo, Dinand Tumpak Sirait, and Wahyu Rs Wahyu Rs. "Paradoks Hukum Humaniter Di Era Perang Siber Dan Drone: Antara Kepatuhan Normatif Dan Realitas Operasional." *Jurnal Ilmu Hukum, Humaniora Dan Politik* 5, no. 5 (June 2025): 4278–83. https://doi.org/10.38035/jihhp.v5i5.4919.

Matthews, Ron, and Fitriani Bintang Timur. "Singapore's 'Total Defence' Strategy." *Defence and Peace Economics* 35, no. 5 (July 2024): 638–58. https://doi.org/10.1080/10242694.2023.2187924.

Matusitz, Jonathan, and Elizabeth Minei. "Cyberterrorism: Its Effects on Health-Related Infrastructures." *Journal of Digital Forensic Practice* 2, no. 4 (September 2009): 161–71. https://doi.org/10.1080/15567280802678657.

McCarthy, James, Lauren Acierto, Glen Joy, Jason Kuruvilla, Titilayo Ogunyale, Nikolas Urlaub, John Wiltberger, and Devin Wynne. *Energy Sector Asset Management for Electric Utilities, Oil & Gas Industry*. National Institute of Standards and Technology, 2020. https://doi.org/10.6028/NIST.SP.1800-23.

Microsoft Threat Intelligence. *Microsoft Digital Defense Report 2023: Building and Improving Cyber Resilience*. 2023. https://www.microsoft.com/en-us/search/explore?q=Microsoft+Digital+Defense+Report+2023#:~:text=featuring%20expert%20guidance.-,Microsoft%20Digital%20Defense%20Report,-https%3A//www.microsoft.

Mittal, Manav. "Colonial Pipeline Cyberattack Drives Urgent Reforms in Cybersecurity and Critical Infrastructure Resilience." *International Journal of Oil, Gas and Coal Engineering* 12, no. 5 (December 2024): 106–19. https://doi.org/10.11648/j.ogce.20241205.11.

Moore, Gemma, Zuneera Khurshid, Thérèse McDonnell, Lisa Rogers, and Orla Healy. "A Resilient Workforce: Patient Safety and the Workforce Response to A Cyber-Attack on the ICT Systems of the National Health Service in Ireland." *BMC Health Services Research* 23, no. 1 (October 2023): 1112. https://doi.org/10.1186/s12913-023-10076-8.

Owusu, Shadrach. "The Rising Threat - Cybersecurity Risks in Critical Energy Infrastructure." Preprint, SSRN, 2025. https://doi.org/10.2139/ssrn.5370813.

Pipyros, Kosmas, Lilian Mitrou, Dimitris Gritzalis, and Theodoros Apostolopoulos. "Cyberoperations and International Humanitarian Law: A Review of Obstacles in Applying International Law Rules in Cyber Warfare." *Information & Computer Security* 24, no. 1 (March 2016): 38–52. https://doi.org/10.1108/ICS-12-2014-0081.

Ramli, Ahmad M., Sigid Suseno, Ranti Fauza Mayana, Ramalinggam Rajamanickam, and Rubben Denova Rohmana. "The Urgency of Regulating Artificial Intelligence in Relation to Cybersecurity and Cyber Resilience." *Cogent Social Sciences* 12, no. 1 (December 2026): 2632977. https://doi.org/10.1080/23311886.2026.2632977.

Ramphal, Talitha. "The Principle of Distinction in an International Armed Conflict: Organized Armed Groups Not Belonging to a State Party to the Conflict." *International Journal of Law and Society* 4, no. 4 (2021): 275. https://doi.org/10.11648/j.ijls.20210404.15.

Raska, Michael, and Benjamin Ang. "Cybersecurity in Southeast Asia." *Paris: Asia Centre & DGRIS*, 2018, 1–9.

Riggs, Hugo, Shahid Tufail, Imtiaz Parvez, Mohd Tariq, Mohammed Aquib Khan, Asham Amir, Kedari Vineetha Vuda, and Arif I. Sarwat. "Impact, Vulnerabilities, and Mitigation Strategies for Cyber-Secure Critical Infrastructure." *Sensors* 23, no. 8 (April 2023): 4060. https://doi.org/10.3390/s23084060.

Roscini, Marco. "Cyber Operations as a Use of Force." In *Research Handbook on International Law and Cyberspace*, edited by Nicholas Tsagourias and Russell Buchan. Edward Elgar Publishing, 2021. https://doi.org/10.4337/9781789904253.00025.

Rossdiana, Renatha Ayu, and Titing Reza Fahrisa. "Strategi Cybersecurity Pemerintah India Dari Perspektif Kautilya: Serangan Siber Mumbai 2020." *Indonesian Journal of International Relations* 7, no. 1 (March 2023): 140–64. https://doi.org/10.32787/ijir.v7i1.408.

Sari, Indah. "Tinjauan Yuridis Hubungan Kejahatan Perang Dan Hukum Humaniter Internasional." *Jurnal Ilmiah Hukum Dirgantara* 11, no. 2 (2021).

Schmitt, Michael N. *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*. Cambridge University Press, 2017.

Schmitt, Michael N., ed. *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*. 2nd ed. Cambridge University Press, 2017. https://doi.org/10.1017/9781316822524.

Schuetz, Sebastian W., Yan Chen, Jens Forderer, and Yusi Ma. "Does Ransomware Make Investors 'WannaCry'? On Investors'

Divergent Reactions to Ransomware Hits and Near Misses." *MIS Quarterly* 49, no. 3 (September 2025): 1153–68. https://doi.org/10.25300/MISQ/2024/18509.

Sigholm, Johan. "Non-State Actors in Cyberspace Operations." *Journal of Military Studies* 4, no. 1 (December 2013): 1–37. https://doi.org/10.1515/jms-2016-0184.

Susila, Muh, and Andi Salim. "Cyber Espionage Policy and Regulation: A Comparative Analysis of Indonesia and Germany." *Padjadjaran Jurnal Ilmu Hukum (Journal of Law)* 11, no. 1 (2024): 122–44. https://doi.org/10.22304/pjih.v11n1.a6.

Tran Dai, Candice, and Miguel Alberto Gomez. "Challenges and Opportunities for Cyber Norms in ASEAN." *Journal of Cyber Policy* 3, no. 2 (May 2018): 217–35. https://doi.org/10.1080/23738871.2018.1487987.

Vihul, Liis, Aaron Shull, Daniel Araya, Samantha Bradshaw, Amandeep Singh Gill, Michael C. Horowitz, Meg King, Robert Mazzolin, Maya Medeiros, and Rodrigo Nieto-Gómez. "International Legal Regulation of Autonomous Technologies." In *Modern Conflict and Artificial Intelligence*. Centre for International Governance Innovation, 2020. https://www.cigionline.org/sites/default/files/documents/Modern%20Conflict%20and%20AI_web_0.pdf.

Waldrop, Elizabeth Seebode. "Integration of Military and Civilian Space Assets : Legal and National Security Implications." McGill University, 2003. https://doi.org/10.82308/5745.

Weiss, Moritz, and Felix Biermann. "Cyberspace and the Protection of Critical National Infrastructure." *Journal of Economic Policy Reform* 26, no. 3 (July 2023): 250–67. https://doi.org/10.1080/17487870.2021.1905530.

World Health Organization. *WHO Reports Fivefold Increase in Cyber Attacks, Urges Vigilance*. Geneva, 2020. https://www.who.int/news/item/23-04-2020-who-reports-fivefold-increase-in-cyber-attacks-urges-vigilance?utm_source=chatgpt.com.

Yuliantiningsih, Aryuni. "Analisis Doktrin Perang Yang Adil (Just War) Dalam Kasus Serangan Siber Rusia Terhadap Georgia Tahun 2008." *Kosmik Hukum* 21, no. 3 (October 2021): 175. https://doi.org/10.30595/kosmikhukum.v21i3.10613.

***

## DECLARATION OF CONFLICTING INTERESTS

The authors state that there is no conflict of interest in the publication of this article.

## FUNDING INFORMATION

This research received no specific grant from any funding agency in the public, commercial, or not-for-profit sectors.

## ACKNOWLEDGMENT

The author would like to express sincere gratitude to the anonymous reviewers and the editorial team for their valuable comments and constructive suggestions, which significantly improved the quality of this manuscript. The author also appreciates the support of colleagues and the academic environment that contributed to the completion of this study.

## GENERATIVE AI STATEMENT

During the preparation of this manuscript, the authors used Gemini AI and ChatGPT (OpenAI, GPT-5.5) to refine the language, improve readability, enhance the academic writing style, and assist in restructuring sections of the manuscript. All legal analysis, interpretation, arguments, and conclusions were developed and verified by the authors, who take full responsibility for the content of this manuscript.