

<https://doi.org/10.5281/zenodo.18601198>

Environmental Warfare in Cyberspace: Can Cyber Operations Causing Climate Harm Constitute Prohibited Environmental Damage Under International Law?

Muhammed Islahuddin Assistant Professor Law & Shariah University of Swat
Swatiadvocate@gmail.com

Abstract: *This study examines whether cyber operations causing climate or environmental harm constitute prohibited environmental damage under international law. Using doctrinal legal analysis, it assesses humanitarian, environmental, and responsibility frameworks, finding that existing principles may extend to cyber-induced harm despite significant regulatory gaps globally. Cyber operations increasingly target physical infrastructure and environmental systems, blurring the lines between cybersecurity, environmental protection, and armed conflict law. This research critically examines whether cyber operations that cause climate harm such as disrupting energy grids, water systems, or industrial controls leading to emissions increases can fall under the umbrella of environmental warfare prohibited by international law. By analysing existing legal frameworks, state practice, and emerging cyber threats with environmental impact, the article argues that although current international law does not explicitly regulate climate harm via cyber operations, core principles of environmental protection, humanitarian law, and state responsibility can and should be interpreted to encompass such harm.*

Keywords: Cyber operations; Environmental harm; Climate change impacts; International humanitarian law; State responsibility; Due diligence; Transboundary damage; Critical infrastructure; Emerging warfare norms

1. Introduction

The rapid integration of digital technologies into critical infrastructure has transformed cyberspace into a domain capable of producing tangible physical and environmental consequences. Cyber operations that interfere with energy systems, industrial control mechanisms, water treatment facilities, and environmental monitoring platforms now possess the potential to cause pollution, increase greenhouse gas emissions, and undermine climate mitigation and adaptation efforts. Despite this evolving risk landscape, international law has yet to clearly articulate whether such cyber-induced environmental and climate harm may amount to prohibited environmental damage or environmental warfare. The purpose of this article is to examine whether cyber operations causing climate-related or environmental harm can be regulated under existing international legal frameworks (Ghani et al., 2025). The study is situated at the intersection of international humanitarian law, international environmental law, and the law of state responsibility, addressing a growing normative gap in the governance of cyber activities with environmental consequences. The significance of this inquiry lies in the increasing reliance of states on digital systems to manage environmentally sensitive infrastructure, coupled with the escalating frequency of malicious cyber operations targeting such systems (Norouzi & Abolghasemi, 2024; Malik & Gul, 2024).

The central hypothesis of this research is that, although international law does not expressly prohibit cyber operations causing climate harm, established legal principles particularly those relating to environmental protection during armed conflict, due diligence, and the prevention of transboundary harm are sufficiently flexible to encompass such conduct. Accordingly, the study seeks to answer whether cyber operations can meet the threshold of prohibited environmental damage and what legal standards may apply in attributing responsibility. Methodologically, the article adopts a doctrinal and analytical approach, examining treaties, customary international law, scholarly commentary, and selected cyber incidents with environmental implications (Mathlouthi et al., 2025). The findings suggest that while existing norms can be interpreted to address environmental harm in cyberspace, their application remains fragmented and uncertain. The article proceeds by outlining the nature of cyber-induced environmental harm, analysing relevant legal frameworks, identifying existing gaps, and proposing avenues for normative development. Technological advancement has transformed cyber operations from a purely digital domain into a force capable of triggering significant physical and environmental harm. Incidents like the Stuxnet attack and the 2021 Colonial Pipeline ransomware seizure demonstrate how cyber interference can affect industrial processes and essential systems (Nuredin & İnan, 2024; Gul, & Malik, 2024).

2. Research Methodology

This study employs analytical research methodology, focusing on the systematic examination of international legal instruments, treaties, customary law, judicial decisions, and scholarly commentary to investigate the regulatory scope of cyber operations causing environmental and climate harm. Primary sources, including the Geneva Conventions, Additional Protocols, the UNFCCC, the Paris Agreement, and the Articles on State Responsibility, were analysed to identify applicable legal obligations, thresholds, and principles. Secondary sources, such as journal articles, legal reports, and case studies—including Stuxnet and the Colonial Pipeline incident—were reviewed to contextualize cyber operations within real-world environmental impacts. The rationale for this approach lies in its ability to synthesize doctrinal interpretation with practical examples, allowing for a comprehensive assessment of how existing legal frameworks can be applied or adapted to emerging forms of environmental harm in cyberspace. This methodology facilitates critical evaluation, comparative analysis, and identification of normative gaps, providing a solid foundation for recommendations and future directions (Khan et al., 2025).

3. Cyber Operations & Environmental Harm: Defining the Problem

Cyber operations are no longer confined to the virtual manipulation of data or information systems; they increasingly produce physical effects by targeting digitally controlled infrastructure. Modern energy networks, industrial facilities, water treatment plants, and climate-monitoring systems rely heavily on supervisory control and data acquisition SCADA and industrial control systems ICS, making them vulnerable to cyber interference with direct environmental consequences. When such systems are compromised, the resulting malfunctions can lead to pollution, excessive emissions, resource depletion, or long-term ecological degradation. Environmental harm arising from cyber operations may be direct **or** indirect. Direct harm occurs when cyber interference causes physical damage to facilities handling hazardous materials, resulting in chemical spills, fires, or uncontrolled emissions. Indirect harm arises when cyber disruptions alter operational behaviour, such as forcing reliance on carbon-intensive backup energy sources, delaying environmental protection measures, or impairing climate data collection and environmental governance. Although the environmental damage may not be the primary objective of a cyber operation, its foreseeable consequences can nonetheless be severe (Khan & Ullah, 2024; Lin & Song, 2024). A key difficulty in defining the problem lies in the cumulative and diffuse nature of climate harm. Unlike conventional kinetic attacks, cyber operations may trigger incremental increases in emissions or gradual ecosystem stress that only manifest over time. This challenges traditional legal thresholds for environmental damage, which are often designed to capture immediate and visible

destruction. Consequently, cyber-induced environmental harm occupies a grey area in international law, demanding a reassessment of how environmental damage is identified, measured, and legally classified in the digital age (Chatinakrob, 2024; Gul et al., 2022).

4. International Legal Frameworks Relevant to Environmental Harm

4.1 International Humanitarian Law IHL

International Humanitarian Law provides the primary legal framework governing the conduct of hostilities during armed conflict and contains specific provisions aimed at protecting the natural environment from the effects of warfare. Although developed in the context of conventional kinetic warfare, these rules are increasingly relevant to cyber operations that produce physical or environmental effects. Key protections are found in Additional Protocol I to the Geneva Conventions. Article 35(3) prohibits methods or means of warfare that are intended, or may be expected, to cause *widespread, long-term and severe* damage to the natural environment. Complementing this provision, Article 55 obliges parties to a conflict to protect the natural environment against such damage and to avoid actions that may prejudice the health or survival of the civilian population (Khan, 2024). These provisions reflect the recognition that environmental destruction can have enduring humanitarian consequences extending beyond the immediate battlefield. The applicability of IHL to cyber operations depends on whether such operations are conducted in the context of an armed conflict and whether they amount to an “attack” producing physical effects. Cyber operations that disable or manipulate infrastructure such as power grids, oil refineries, or industrial plants can cause environmental harm comparable to kinetic attacks and may therefore fall within the scope of IHL. If the foreseeable consequences of a cyber operation include large-scale pollution or long-term ecological damage, it may meet the high threshold required under Articles 35(3) and 55. However, significant interpretative challenges remain. The cumulative nature of climate harm complicates the assessment of what constitutes *widespread, long-term, and severe* damage, and proving intent or expectation in cyber contexts is particularly difficult. Nevertheless, the underlying principles of distinction, proportionality, and military necessity continue to apply, suggesting that cyber operations with foreseeable environmental consequences may be constrained by IHL even in the absence of explicit cyber-specific provisions (De Baets, 2022; Khan, 2024).

4.2 International Environmental Law IEL

International Environmental Law governs state obligations to protect the environment during both peacetime and, to a limited extent, situations of conflict. While IEL was not designed with cyber operations in mind, its foundational principles are increasingly relevant where digital activities result in environmental or climate-related harm. Unlike IHL, IEL does not require the existence of an armed conflict and therefore offers a broader normative framework for assessing cyber operations that cause environmental damage outside traditional warfare. Central to IEL is the no-harm principle, which obliges states to ensure that activities within their jurisdiction or control do not cause significant environmental damage to other states or areas beyond national jurisdiction. Closely linked to this is the duty of due diligence, requiring states to take reasonable measures to prevent, reduce, and control environmental harm. Applied to cyberspace, these principles suggest that states have an obligation to prevent cyber operations emanating from their territory that foreseeably cause transboundary environmental or climate harm (Khan & Jiliani, 2023). Climate-specific regimes, particularly the United Nations Framework Convention on Climate Change UNFCCC and the Paris Agreement, impose obligations on states to mitigate greenhouse gas emissions and protect the climate system. Although these instruments do not expressly address cyber-induced harm, cyber operations that disrupt emissions-reduction mechanisms, renewable energy infrastructure, or climate monitoring systems may undermine treaty objectives and violate broader commitments of good faith and cooperation. Nevertheless, IEL faces notable limitations in this context. Establishing causation between a cyber operation and diffuse

climate harm is complex, and enforcement mechanisms remain weak. Despite these challenges, IEL provides important normative guidance, reinforcing the argument that cyber operations contributing to environmental degradation or climate harm should not exist in a legal vacuum but be assessed within established environmental protection obligations (Van Steenberghe, 2022; Usman et al., 2023).

4.3 State Responsibility and Customary International Law

The law of state responsibility provides a crucial framework for addressing cyber operations that cause environmental or climate-related harm, particularly where neither international humanitarian law nor international environmental treaties offer explicit cyber-specific rules. Under the Articles on Responsibility of States for Internationally Wrongful Acts ARSIWA, a state incurs responsibility when conduct attributable to it constitutes a breach of an international obligation. This framework is especially relevant in cyberspace, where harmful actions may occur outside formally declared armed conflicts. Attribution is the first legal hurdle. Cyber operations causing environmental harm must be linked to a state through its organs, agents, or entities acting under its effective control (Khan & Usman, 2023). While technical attribution remains complex, international law does not require absolute certainty; rather, it relies on a reasonable evidentiary standard based on available facts and circumstances. Once attribution is established, the focus shifts to whether the conduct breached an international obligation, such as the duty to exercise due diligence or the customary obligation to prevent transboundary environmental harm. Customary international law reinforces these obligations. The no-harm rule, affirmed in cases such as *Trail Smelter* and subsequent jurisprudence, requires states to prevent activities within their control from causing serious environmental damage to other states. Applied to cyber operations, this principle suggests that states may bear responsibility not only for direct cyber attacks but also for failing to prevent non-state actors from launching cyber operations that result in foreseeable environmental or climate harm. Where a breach is established, international law requires cessation, assurances of non-repetition, and reparation, which may include restitution, compensation, or satisfaction. Although practical enforcement remains difficult, the law of state responsibility offers a flexible and evolving basis for holding states accountable for environmentally harmful cyber conduct and for integrating climate protection into emerging norms of cyber governance (Hemmati, et al., 2024; Hussain et al., 2023).

5. Cyber Operations with Environmental Impact: Case Studies

5.1 Stuxnet and Industrial Sabotage

The Stuxnet operation, uncovered in 2010, represents one of the earliest and most significant examples of a cyber operation producing tangible physical effects. Designed to infiltrate and manipulate industrial control systems, Stuxnet targeted uranium enrichment centrifuges by altering their operational speeds while concealing the malfunction from monitoring systems. Although the operation was narrowly focused on nuclear infrastructure and did not directly result in environmental damage, it demonstrated the capacity of cyber tools to cause physical destruction within highly sensitive industrial environments. From an environmental law perspective, Stuxnet is significant not for its immediate outcomes but for the precedent it sets (Khan & Ximei, 2022). The same techniques used to manipulate centrifuges could, if directed at chemical plants, oil refineries, dams, or waste treatment facilities, cause large-scale pollution, toxic releases, or long-term ecological harm. Such scenarios highlight how cyber operations can function as a form of industrial sabotage with potentially severe environmental consequences, even in the absence of kinetic force. Legally, Stuxnet underscores the challenges of attribution, intent, and classification under international law. If a similar cyber operation were to cause environmental damage, questions would arise as to whether it constitutes an unlawful attack under international humanitarian law, a breach of environmental obligations, or an internationally wrongful act under the law of state responsibility. Stuxnet thus serves as a cautionary case study, illustrating how cyber operations can easily cross the threshold from strategic disruption to environmentally destructive conduct, exposing significant gaps in existing legal regulation (Lindsay, 2025; Amjad et al., 2022).

5.2 Colonial Pipeline Ransomware (2021)

The 2021 ransomware attack on the Colonial Pipeline in the United States illustrates how cyber operations targeting critical infrastructure can indirectly produce environmental and societal consequences. The attack forced the temporary shutdown of a major fuel pipeline, disrupting the supply of gasoline, diesel, and jet fuel across the Eastern United States. While the operation did not directly damage the physical environment, its cascading effects such as increased reliance on alternative, less efficient energy sources, emergency fuel transport, and operational adjustments highlight the potential for cyber incidents to affect energy consumption patterns and, by extension, greenhouse gas emissions. This case emphasizes the broader concept of indirect environmental harm in cyberspace (Amjad et al., 2022). Unlike kinetic attacks, which may produce immediate and visible destruction, ransomware attacks can have delayed or diffuse ecological consequences. Disruptions to energy infrastructure, industrial supply chains, or environmental monitoring systems may unintentionally exacerbate climate risks, reduce efficiency in emissions control, and undermine sustainable energy transitions. Legally, the Colonial Pipeline incident raises critical questions regarding state responsibility, due diligence, and the applicability of international environmental law in non-conflict contexts. While the attack was carried out by a non-state actor, the state hosting the perpetrators may bear obligations under customary international law to prevent transboundary environmental harm. The case underscores the evolving nature of cyber threats and the need for legal frameworks that recognize and regulate both direct and indirect environmental consequences of cyber operations (Beerman, et al., 2023; Khan et al., 2020).

5.3 Hypothetical Climate Data Manipulation

A particularly concerning future scenario involves cyber operations targeting climate and environmental data systems rather than physical infrastructure. Governments and international organizations rely heavily on digital climate models, satellite data, emissions inventories, and early-warning systems to design mitigation strategies, allocate resources, and respond to environmental disasters. Manipulation, deletion, or distortion of such data through cyber means could significantly undermine climate governance without causing immediate physical damage. The environmental harm in this scenario is indirect but systemic. Altered climate data may lead to flawed policy decisions, delayed adaptation measures, misallocation of funding, or underestimation of environmental risks. Over time, such interference could contribute to increased emissions, greater vulnerability to climate disasters, and long-term ecological degradation. Unlike industrial sabotage, the damage here lies in compromised decision-making processes, making causation and harm assessment particularly difficult. From a legal perspective, climate data manipulation challenges traditional notions of environmental damage, which often rely on observable physical effects. While such conduct may fall outside the classic scope of “attacks” under international humanitarian law, it may still violate obligations under international environmental law, including duties of cooperation, good faith, and due diligence. Moreover, if attributable to a state, such actions could engage state responsibility for undermining global efforts to protect the climate system, highlighting the urgent need to reconceptualize environmental harm in the digital age (Fallah & Rostami, 2024).

6. Can Climate Harm from Cyber Operations Be Prohibited Environmental Damage?

6.1 Interpretation of “Environmental Warfare” in IHL

International Humanitarian Law IHL recognizes environmental protection as a fundamental aspect of lawful conduct during armed conflict, particularly through the concept of “environmental warfare,” which prohibits acts intended or expected to cause widespread, long-term, and severe damage to the natural environment. Originally developed for conventional kinetic warfare, these provisions are increasingly relevant for cyber operations capable of producing physical or ecological effects. Cyber attacks targeting critical infrastructure, industrial facilities, or energy systems can trigger consequences comparable to traditional warfare, potentially meeting the threshold for prohibited environmental

damage. The criteria under Articles 35(3) and 55 of Additional Protocol I *widespread, long-term, and severe* serve as the primary benchmark for evaluating environmental harm. Widespread damage refers to large geographic impact, long-term denotes persistent effects on ecosystems or climate systems, and severe indicates significant threats to human health or biodiversity. Many cyber operations, however, produce indirect, delayed, or diffuse environmental effects, making it difficult to assess whether these thresholds are met. Additionally, determining whether harm was intended or merely foreseeable poses a challenge in the cyber context. Despite these interpretive difficulties, the general principles of distinction, proportionality, and military necessity remain applicable. Cyber operations that foreseeably disrupt energy infrastructure, industrial processes, or environmental monitoring systems, resulting in large-scale ecological or climate harm, can reasonably be considered prohibited under IHL's environmental protection provisions. This evolving interpretation underscores the need for IHL to adapt to the digital age, integrating emerging forms of cyber-enabled environmental harm into the legal framework (Szpak, et al., 2024).

6.2 IEL and the Paris Framework

International Environmental Law IEL provides a broader framework for environmental protection that applies in both peacetime and situations of conflict, emphasizing state obligations to prevent harm and promote sustainability. Central to IEL is the principle of due diligence, which requires states to take reasonable measures to ensure that activities within their jurisdiction or control do not cause significant environmental damage to other states or areas beyond national jurisdiction. This includes preventing cyber operations emanating from their territory that could disrupt ecosystems, energy systems, or climate-related infrastructure, leading to environmental degradation or climate harm. The Paris Agreement and the broader UNFCCC establish specific obligations for states to mitigate greenhouse gas emissions and protect the climate system. While these instruments do not explicitly address cyber operations, disruptions to renewable energy infrastructure, emissions monitoring systems, or climate data management can undermine treaty objectives. Consequently, cyber operations that interfere with climate mitigation or adaptation efforts may be interpreted as contravening states' obligations under these frameworks. Despite these principles, IEL faces limitations in addressing cyber-induced environmental harm. Establishing causation between a cyber operation and long-term climate effects is complex, and enforcement mechanisms for transboundary harm remain weak. Nevertheless, IEL reinforces the idea that states have legal obligations to prevent environmental harm, including that arising from cyber operations, highlighting the need for legal adaptation to address emerging threats to climate and ecological security (Kramer, 2025).

7. Conclusion

Cyber operations capable of causing environmental or climate harm represent an emerging frontier in both international law and security studies. This research demonstrates that, although existing frameworks like International Humanitarian Law, International Environmental Law, and state responsibility principles can be interpreted to address such harm, there is no explicit legal regime governing cyber-induced environmental damage. Key findings indicate that cyber operations may produce direct and indirect environmental effects, challenge traditional thresholds of "widespread, long-term, and severe" damage, and complicate issues of attribution, intent, and enforcement. Given these gaps, there is a pressing need for legal and policy innovation. Future directions include developing treaty or customary norms specifically addressing cyber operations with environmental consequences, establishing clear criteria for measuring cyber-induced environmental harm, and creating international mechanisms for rapid attribution and accountability. Further research could also explore the intersection of climate governance, cybersecurity, and liability, particularly regarding non-state actors and transboundary impacts. Ultimately, understanding and regulating environmental warfare in cyberspace is crucial not only for protecting ecosystems and climate stability but also for ensuring that technological advancement does not outpace the legal and ethical safeguards needed to prevent global harm.

Addressing this challenge will require interdisciplinary collaboration between legal scholars, policymakers, technologists, and environmental scientists to build a resilient and accountable framework for the digital age. Cyber operations with environmental consequences particularly those contributing to climate harm challenge existing legal frameworks. While no treaty currently prohibits climate harm from cyber operations explicitly, fundamental principles in IHL, IEL, and state responsibility can be interpreted to encompass such harm. As cyber warfare evolves, international law must adapt to integrate environmental protection, ensuring accountability for operations that threaten the climate and future generations.

References

- Amjad, S. O. H. A. I. L., Khan, A. S. I. F., & Usman, M. U. H. A. M. M. A. D. (2022). Analyzing International Environmental Law in Addressing Air Pollution. *Asian Social Studies and Applied Research (ASSAR)*, 3(01), 272-283.
- Amjad, S., Usman, M., & Khan, A. (2022). Environmental Jurisprudence in Pakistan: A Comprehensive Analysis of National Laws, Judicial Role, and Legislative Instruments Impacting Air Quality and Public Health.
- Beerman, J., Berent, D., Falter, Z., & Bhunia, S. (2023, May). A review of colonial pipeline ransomware attack. In *2023 IEEE/ACM 23rd International Symposium on Cluster, Cloud and Internet Computing Workshops (CCGridW)* (pp. 8-15). IEEE.
- Chatinakrob, T. (2024). Interplay of International Law and Cyberspace: State Sovereignty Violation, Extraterritorial Effects, and the Paradigm of Cyber Sovereignty. *Chinese Journal of International Law*, 23(1), 25-72.
- De Baets, A. (2022). The view of the past in international humanitarian law (1860–2020). *International review of the Red Cross*, 104(920-921), 1586-1620.
- Fallah, B., & Rostami, M. (2024). Exploring the impact of the recent global warming on extreme weather events in Central Asia using the counterfactual climate data ATTRICI v1. 1. *Climatic Change*, 177(5), 80.
- Ghani, H. U., Gong, X., Haider, A., & Khan, A. (2025). The Indian concern on China-Pakistan Economic Corridor (CPEC) and justification from the perspective of international law. *China and WTO Review*, 11(2), 25-39.
- Gul, S., & Malik, W. (2024). Cyber Conflict and International Security: Legal Challenges and Strategic Solutions in Cyberspace. *The Journal of Research Review*, 1(04), 305-314.
- Gul, S., Ullah, Q., Qasim, M., & Sheringal, D. U. P. (2022). Bio-waste management legislation regulations and policies: A case study of Pakistan. *Pakistan Journal of International Affairs*, 5(3).
- Hemmati, F., Raei, M., & Arashpour, A. (2024). States Responsibility in Mitigating Climate Change under Customary International Law. *Journal of Legal Research*.
- Hussain, N., Khan, A., & Wassan, R. (2023). UNCLOS 1982: Comparative analysis of marine pollution prevention by ships. *Annals of Human and Social Sciences*, 4(2), 295-308.
- Khan, A. (2024). The Emergence of the Fourth Industrial Revolution and its Impact on International Trade. *ASR: CMU Journal of Social Sciences and Humanities (2024) Vol, 11*.
- Khan, A. (2024). The intersection of artificial intelligence and international trade laws: Challenges and opportunities. *IIUMLJ*, 32, 103.
- Khan, A., & Jiliani, M. A. H. S. (2023). Expanding The Boundaries Of Jurisprudence In The Era Of Technological Advancements. *IIUMLJ*, 31, 393.
- Khan, A., & Ullah, M. (2024). The Pakistan-China FTA: legal challenges and solutions for marine environmental protection. *Frontiers in Marine Science*, 11, 1478669.
- Khan, A., & Usman, M. (2023). The effectiveness of international law: a comparative analysis.

- Khan, A., & Ximei, W. (2022). Digital economy and environmental sustainability: do information communication and technology (ICT) and economic complexity matter?. *International journal of environmental research and public health*, 19(19), 12301.
- Khan, A., Amjad, S., & Usman, M. (2020). The Role of Customary International Law in Contemporary International Relations. *International Review of Social Sciences*, 8(08), 259-265.
- Khan, A., Jillani, M. A. H. S., Ullah, M., & Khan, M. (2025). Regulatory strategies for combatting money laundering in the era of digital trade. *Journal of Money Laundering Control*, 28(2), 408-423.
- Kramer, A. (2025). a critical ecofeminist review of the paris agreement: potential for enhanced effectiveness and inclusivity.
- Lin, S., & Song, Y. (2024). Upholding human rights in mega sports: A study of governance practices within the IOC and FIFA through the lens of the Ruggie Principle. *Heliyon*, 10(16).
- Lindsay, J. R. (2025). Stuxnet revisited: From cyber warfare to secret statecraft. *Journal of Strategic Studies*, 1-40.
- Malik, W., & Gul, S. (2024). Bridging the Gap: Exploring the Intersection of Cybersecurity and Human Security in the Digital Age. *Competitive Research Journal Archive*, 2(04), 195-202.
- Mathlouthi, N., Haider, A., Khan, A., & Ahmad, N. (2025). The role of Hainan Free Trade Port in shaping China's WTO commitments and international trade policies. *China and WTO Review*, 11(1), 71-82.
- Norouzi, M., & Abolghasemi, S. (2024). Environmental damage: Interfaces between international criminal law and international humanitarian law. *CIFILE Journal of International Law*, 5(9), 50-66.
- Nuredin, A., & İnan, T. C. (2024). Cyber warfare and international criminal law: State responsibility for cyber attacks. In *International Scientific Conference on AI, Human Rights, Migration, Democracy, and Public Impact* (pp. 188-200).
- Szpak, A., Bar, M., & Kemp, E. (2024). PROTECTION OF THE ENVIRONMENT–INTERNATIONAL HUMAN RIGHTS AND INTERNATIONAL HUMANITARIAN LAW PERSPECTIVES. *Torun International Studies*, 1(19), 33-52.
- Usman, M., Amjad, S., & Khan, A. (2023). Clearing the air: Legal strategies for combating smog and pollution. *Journal of Strategic Policy and Global Affairs*, 4(01), 15-21.
- Van Steenberghe, R. (2022). The interplay between international humanitarian law and international environmental Law: Towards a comprehensive framework for a better protection of the environment in armed conflict. *Journal of International Criminal Justice*, 20(5), 1123-1154.