International Journal for Multidisciplinary Research (IJFMR)
E-ISSN: 2582-2160 ● Website: www.ijfmr.com ● Email: editor@ijfmr.com

Digital Battlefronts: Rethinking Legal Frontiers in Cyberwarfare and AI Conflicts

Pasupathieswaran M[1], Kapilan Bharathi G[2]

[1,2]Law Student, Sastra Deemed University

ABSTRACT:
Cyberspace and artificial intelligence (AI) have been increasingly used in international conflicts without sufficient regulations, raising concerns over their unchecked impact. Although authoritative texts like the Tallinn Manual provide guidance for governing cyberspace, the absence of explicit International Humanitarian Law (IHL) rules tailored to cyber operations remains a significant concern.The current legal frameworks are insufficient to effectively regulate armed conflicts in cyberspace.The article discusses how cyber-attacks are regulated by the existing body of laws such as the United Nations Charter, International humanitarian Law (IHL), international treaties. The UN General Assembly global Conference on Cyberspace was organised to address, Whether the human moderators and commanders can be held responsible for AI-driven violations under the current IHL framework?. This paper explores the cyber attacks that are global in nature using various cyber case studies that are state sponsored or not state sponsored. This paper concludes that there is a need for new international conventions or legislations to effectively deal with cyberwarfare in international space.

KEYWORDS: Cyberwarfare, International Humanitarian Law, International Treaties, Cyber Attacks, Artificial Intelligence.

BACKGROUND OF THE STUDY:
"Cyber Space" was formed over the course of the last three decades by the confluence of information and communication technologies (ICTs) and different governance frameworks. Cyberspace is a living reality today, impacting every facet of human conduct. It is therefore crucial to establish a universal and open worldwide framework to guarantee the efficient use and protection of cyberspace "for the economic and social advancement of all peoples."
When the United Nations General Assembly (UNGA) passed its first resolution on ICTs, governments began to confront this issue more than 20 years ago. Businesses, academic institutions, and civil society organisations are among the other players who have become more vocal in their quest for an international framework that supports their online operations. Despite the genuinely unpredictable consequences of the COVID-19 p[1]andemic, The time has come to start a broad-based, multi-stakeholder process that could lead to the adoption of an international convention on cyberspace, especially as the UN celebrates its 75th anniversary this year.
Within a few short years, the Internet of Things (IoT), artificial intelligence (AI), and robotics are predicted to take over cyberspace and reshape the role of humans in this field. Cyber infrastructure and technology

[1] https://jindalforinteconlaws.in/

are at the centre of these connections.

"Cyberwarfare," is also defined as fighting using cyberspace and cybertools. A purposeful act of destruction results from an armed attack (i.e., property destruction, physical harm to living things, and/or death). Cyberwarfare is restricted to governments, state organs, and individuals or groups under state direction or sponsorship. Cyberwarfare targets can also include people whose lives, or the functioning of items, depend on computer systems, such as people tied to various medical, military, or professional life-support systems, transportation systems, or power plants. The nature of cyberattacks: For instance, a variety of assets can be targeted by computer viruses. Cyberattacks have the potential to take down websites and networks, stop nuclear power plants, or steal intellectual property. When a computer virus compromises a business's property and takes down the electrical grid, it becomes illegal.

Along with certain principles of customary international law, IHL, or jus in bello, is largely established in the 1949 Geneva Conventions and their Additional Protocols of 1977 and 2005. Like all other new forms of warfare, experts agree that cyberwarfare that takes place during a "international armed conflict" will be governed by IHL. The UN General Assembly resolutions on cyberlaw, the ICRC Report 2020, the UN GGE reports, and the final UN OEWG 2021 report all support this consensus by stating that international law, including the UN Charter, applies to cyberwarfare. However, because there is no shared comprehension of cyber activities in international law, the application of IHL to cyberwarfare is complicated and ambiguous.These in turn have detrimental impacts on civilians.

LITERATURE REVIEW:

In this article, “Why the World Needs an International Cyberwar Convention”, the research gap identified is the lack of established international rules or norms governing cyber warfare, despite the increasing prevalence of cyberattacks. Additionally, there is insufficient exploration of effective mechanisms for reliable attribution of cyberattacks, which is crucial for enforcing compliance with any potential international treaty. The article argues that existing objections to an international cyber convention are often based on misconceptions, highlighting the need for further investigation into the feasibility and necessity of such a framework.

In the article, “Issues in cyber Warfare in international Law”, the research gap identified is insufficient analysis of how existing international laws can be effectively adapted to address the unique challenges posed by cyber warfare, particularly regarding attribution and the right to self-defense. Finally, the evolving nature of cyber threats and the involvement of non-state actors further complicate the legal landscape, indicating a need fo[2]r more comprehensive studies on these dynamics.

In the article, “Applying International Humanitarian Law to Cyber Warfare”, the research gap identified lies in the lack of established international rules or norms governing cyber conflict, as well as the challenges related to effective attribution of cyberattacks. While the article discusses the obstacles to creating an international cyberwar convention, it highlights the need for further exploration of mechanisms for reliable attribution and enforcement of compliance. Additionally, it suggests that historical experiences from other areas of international arms control could inform the development of cyber norms, which remains under-researched.

The article addresses the challenges of applying International Humanitarian Law (IHL) to cyber operations due to a lack of transparency, insufficient information about the nature of cyber attacks, and difficulties in

[2] https://jindalforinteconlaws.in/2023/10/15/international-humanitarian-law-is-cyber-warfare-fair-part-ii-smriti-jaiswal/

interpreting key concepts like "control" in cyberspace. It highlights the need to determine how existing legal frameworks can effectively regulate cyber warfare while preserving human dignity and preventing unnecessary suffering. The overarching problem is the ambiguity surrounding the legal status and implications of cyber operations in armed conflict.

In the article,"Hacking into International Humanitarian Law: The Principles of Distinction and Neutrality in the Age of Cyber Warfare", the research gap identified in the article is the lack of consensus within the international community on how existing International Humanitarian Law (IHL) applies to cyber warfare. While there is agreement that legal restrictions should exist, the current frameworks are deemed inadequate to address the unique challenges posed by cyber conflicts, necessitating the evolution of new norms and practices rather than the creation of new treaties. Additionally, the article highlights the difficulty in enforcing existing laws due to the complexities of attribution and accountability in cyber attacks.

In the article"Corresponding Evolution: International Law and the Emergence of Cyber Warfare", The research gap identified in the article is the inadequacy of current international laws to address key issues of cyber warfare, specifically regarding attribution, jurisdiction, and the definition of "use of force." There is a lack of consensus on fundamental aspects of cyber warfare, which creates legal uncertainty and hinders the development of effective international regulations. Additionally, the article highlights the need for a completely new legal paradigm tailored to the unique challenges posed by cyber warfare, as existing frameworks are insufficient.

In the article, " Cyber warfare and International Law", concludes that cyberwarfare is not legally unregulated but is subject to established international law principles, though applying these to cyberspace presents challenges. It emphasizes the need for states to recognize their legal and moral responsibilities regarding cyber operations, particularly concerning critical infrastructure and potential humanitarian impacts. The article advocates for a clearer interpretation of existing laws to address the complexities of cyber warfare effectively.

RESEARCH PROBLEM

Cyber Warfare involves state-sponsored hacking and cyberattacks targeting another nation's infrastructure, data, or systems to disrupt, damage, or steal. While typically state-sponsored, non-state actors can also engage in such activities for various motives. It's a cyber platform on which cyber attacks happen. Many people have argued that since it's not particularly a state it cannot be specifically governed under any international law that is existing. There is a lack of clarity in applying the IHL to the cyber attacks.

In recent times what all international conventions are introduced and how international conventions are used to govern the cyberwarfare in international space, and how it affects civilians.

RESEARCH OBJECTIVE:

Impact on Civilians and Need for Protection: The article examines how cyber warfare has impacted civilian populations, particularly through disruptions to critical infrastructure, and underscore the necessity of enhanced protections for civilians in cyberspace.

Application of Existing International Humanitarian Law (IHL): Assesses the current applicability of IHL to cyberattacks, identifying the lack of clarity in how these legal frameworks address attacks on cyber platforms and critical infrastructure.

Evolving International Conventions and Governance: Explores the development of new international conventions and agreements aimed at governing cyber warfare, with a focus on the role of the UN Charter and the evolving legal framework for cyberspace.

RESEARCH QUESTIONS:

Whether the cyber-attacks on critical infrastructure, as seen in case studies like Stuxnet and the Russia-Ukraine conflict, can be definitively categorized as state-sponsored or non-state-sponsored?

Whether the current international conventions address the protection of civilians in cyberwarfare, especially in cases involving attacks on civilian cyber infrastructure?

Whether the existing international laws, such as the United Nations Charter and International Humanitarian Law (IHL), are sufficient to regulate cyberwarfare effectively in international conflicts?

Whether or not evolving cyber threats demand the creation of specialized international conventions and a legal body to address cyber conflicts within the scope of international law?

RESEARCH METHODOLOGY:

In this study, we have used a qualitative method of research to support and justify our research questions. We gathered secondary data from several articles to provide a possible answer for the challenges that are pointed out in the article.

SCOPE AND LIMITATION:

This research focuses, using case studies such as Stuxnet and cyber operations in the Russia-Ukraine conflict, aims to differentiate between state-sponsored and non-state-sponsored cyber-attacks, highlighting the challenges in determining their origins.

The scope extends to an in-depth examination of international conferences, such as the UN General Assembly's global Conference on Cyberspace, and efforts to develop multi-stakeholder frameworks for regulating cyberwarfare. Furthermore, the study explores the moral and legal responsibilities of states under IHL and evaluates whether current laws adequately protect civilian infrastructure in the context of cyber conflicts. The research ultimately concludes that there is a pressing need for new international conventions or legislation that can more effectively govern cyberwarfare in the evolving global landscape, ensuring the protection of civilians and maintaining international peace and security in cyberspace.

Attribution in cyberwarfare—the ability to definitively identify whether an attack is state-sponsored or non-state-sponsored remains a significant challenge. Despite examining various case studies, the clandestine nature of cyber-attacks complicates efforts to draw firm conclusions about their origins, limiting the ability to propose definitive legal solutions.

Moreover, the research focuses primarily on legal and theoretical aspects, and lacks empirical analysis of how effective current regulations are in preventing cyber-attacks in real-world scenarios. Finally, the study may not fully encompass regional perspectives or the interests of smaller states, which could result in a bias towards dominant international actors in cyberspace.

Overview of International Humanitarian Law and Cyberwarafare: Cyberwarfare has been subjected to existing legal regulations and standards pertaining to warfare (see Tallinn Manual 2.0 International Law Applicable to Cyber Operations, 2017 and Tallinn Manual on the International Law Applicable to Cyber Warfare, 2013). The establishment of jus ad bellum, or the right to employ force, is necessary prior to participating in cyberwarfare. Any use of force in this situation needs to be justified and authorized by the

law. The legitimate justification for this is self-defense.[3] Under Article 51 of the UN Charter of 1945, nations are permitted to use force to defend themselves.

The UN Charter is the primary source of jus ad bellum. Some of that law's specifics, including the procedures governing the use of force in self-defense, are not controlled by the UN Charter and instead have to be inferred from customary law, which is recognized by international jurisprudence and is reflected in state practice and opinio juris. Examining whether cyber operations can be considered (1) an internationally wrongful threat or use of "force," (2) a "armed attack" that justifies the use of appropriate force in self-defense, or (3) a "threat to the peace," "breach of the peace," or "act of aggression" that warrants intervention by the UN Security Council, is necessary.

"Jus ad bellum," or the law governing the justification for war, plays a crucial role in the context of cyber warfare, as it dictates when a state may resort to armed conflict. The principles of jus ad bellum include just cause, legitimate authority, proportionality, and last resort, all of which become complex in the realm of cyber operations. Establishing a just cause for a cyber attack can be challenging, especially since many cyber incidents involve non-state actors or may not lead to immediate physical harm. This ambiguity complicates the determination of when a state can lawfully respond to a cyber attack with military force. Additionally, the principle of legitimate authority raises questions about who has the right to initiate cyber warfare; non-state actors and rogue entities can perpetrate attacks, blurring the lines of accountability. Proportionality must also be carefully assessed, as a cyber response could lead to unintended consequences that escalate conflict or harm civilians.

"Jus in bello," or the law governing conduct in war, faces unique challenges in the context of cyber warfare. Key principles such as distinction, proportionality, and necessity must be carefully applied. The principle of distinction requires combatants to differentiate between military targets and civilians; however, in cyber warfare, this can be complex due to the interconnectedness of civilian and military networks. Proportionality mandates that any military action should not cause excessive civilian harm compared to the anticipated military advantage, but the unpredictable nature of cyber attacks can lead to unintended consequences, such as disruptions to critical infrastructure like hospitals. The principle of necessity emphasizes that force should only be used to achieve legitimate military objectives, which is increasingly complicated in cyber operations due to the potential for widespread disruption. Attribution also poses a significant challenge; identifying the perpetrator of a cyber attack can be difficult, complicating the response while adhering to "jus in bello" principles. This lack of clear frameworks for accountability further complicates the enforcement of international humanitarian law in the cyber realm. Efforts like the Tallinn Manual aim to clarify how existing international law applies to cyber warfare, highlighting the need for legal frameworks that adequately address the complexities of modern conflict in cyberspace. As cyber warfare continues to evolve, the application of "jus in bello" remains a critical area for ongoing study and debate.

According to Question No. 1 of Research :- Responsibility of state and non- state actors in cyber attacks: States have a responsibility under international law to prevent, control, or prosecute cyberattacks launched from their territories, even when such actions are carried out by non-state actors or private organizations. This duty stems from the principle of state sovereignty and the obligation to ensure that their territory is not used in ways that harm other states. According to norms in international law, including

[3] https://www.cirsd.org/en/horizons/horizons-spring-2020-issue-no-16/the-need-for-an-international-convention-on-cyberspace
https://www.stimson.org/2024/strengthening-global-cyber-resilience-through-un-security-council-initiatives/

the UN Charter, states must take reasonable measures to prevent cyber operations that could violate the rights of other states. If a cyberattack originates from non-state actors or private entities within their jurisdiction, states are expected to investigate and, where appropriate, prosecute the perpetrators or otherwise mitigate the damage. This may involve coordination with international law enforcement bodies like INTERPOL or cooperation with affected states to hold perpetrators accountable. Failure to act against such activities may lead to state responsibility for allowing harmful cyber activities, potentially leading to diplomatic consequences or countermeasures by affected states.

In cyber warfare, it states that non – state actors can be held accountable for cyberattacks, holding them responsible requires proving a clear link between their actions and a state. This makes it difficult to enforce accountability under current international Law. Recently, the United Nations and other international efforts have tried to push for clearer rules regarding non- state actors in cyberwarfare, but no binding agreements have yet been established.

States may use cyber proxies or third-party actors, such as private hackers, criminal groups, or mercenaries, to carry out cyber operations covertly. This strategy allows states to maintain a degree of plausible deniability, making it difficult to trace the attack directly to the government. By outsourcing cyber operations to non-state actors, states can evade responsibility under international law or obscure their involvement, complicating retaliation by the targeted state.[4]

Cases Reported on cyber attacks by state sponsored agency:

A. Stuxnet Case: (Iran and USA conflict)

The Stuxnet case involved a sophisticated cyber weapon developed by the US and Israel, targeting Iran's nuclear facilities, particularly the Natanz uranium enrichment plant. The attack unfolded in several phases, beginning in 2002 with the discovery of Iran's nuclear program, followed by diplomatic efforts and sanctions from 2006 to 2010. In 2010, Stuxnet infiltrated the facility's programmable logic controllers, causing centrifuges to malfunction while employing rootkits to conceal its presence, ultimately leading to a significant reduction in uranium enrichment and contributing to international sanctions. This case is a landmark example of cyber warfare, showcasing the potential of digital attacks to disrupt critical infrastructure. The Stuxnet attack raised serious concerns about the potential for cyber warfare to be used as a tool of state-sponsored aggression. It also highlighted the vulnerability of critical infrastructure to cyberattacks.

B. Russia and Ukraine War:

The Russia-Ukraine war case study examines the intricate historical ties between Russia and Ukraine, rooted in their shared origins in Kievan Rus and further complicated by their time as part of the Soviet Union. The conflict intensified in 2014 when Russia annexed Crimea, a move widely condemned by the international community, and began supporting separatist movements in eastern Ukraine, leading to a protracted military confrontation.[5]

Key phases of the conflict include the initial annexation of Crimea, which marked a significant escalation in hostilities, followed by ongoing military engagements in the Donbas region, where Russian-backed separatists clashed with Ukrainian forces. Additionally, the war has seen a significant component of cyber warfare, with Russia launching cyber attacks aimed at destabilizing Ukraine's infrastructure, disrupting communications, and undermining public trust in the government. This case study illustrates the broader

[4] https://cams.mit.edu/wp-content/uploads/2017-10.pdf
https://guides.ll.georgetown.edu/cyberspace/cyber-warfare

[5] https://scholarlycommons.law.wlu.edu/cgi/viewcontent.cgi?article=1512&context=wlufac

geopolitical tensions in Eastern Europe and the struggle for influence, sovereignty, and national identity in the face of aggression.

C. Ukraine Power Grid Case:

The Ukrainian Power Grid case study details a significant cyber attack that occurred in December 2015, targeting Ukraine's electricity distribution networks. The attack began with a spear-phishing campaign that compromised the IT staff of multiple energy companies, allowing hackers to gain access to critical systems and deploy malware, including KillDisk, which rendered operator stations inoperable. Although the power outage lasted only one to six hours for affected areas, the attack highlighted vulnerabilities in critical infrastructure and the potential for cyber warfare to disrupt essential services, with control centers remaining partially non-operational for months afterward.

D. Russia and Georgia War:

The Russia-Georgia war case study focuses on the complex historical and political relationship between Georgia and Russia, marked by tensions stemming from Russia's support for separatist regions in Georgia and Georgia's aspirations to join NATO. The conflict escalated in August 2008, beginning with cyber attacks against Georgian infrastructure, including Distributed Denial of Service (DDoS) attacks that targeted government websites, coinciding with military hostilities. The war culminated in a brief but intense military engagement, leading to a cease-fire agreement brokered by French President Nicolas Sarkozy, and resulted in the recognition of the separatist regions of South Ossetia and Abkhazia as independent by Russia, further straining relations between the two countries and impacting regional stability.

According to Question No.2 of the research: - Civil Protection under IHL in Cyber Space: Indiscriminate assaults that can be "anticipated" to injure non-targeted civilians without making a distinction between military units or infrastructure are forbidden, according to Article 51(4)(b) and (c). Because of the disparity in computer security between military and civilian cyberspace, the interconnectedness of cyberspace, and the inexperience of armed forces in conducting such operations, it can be difficult to determine which cyberattack is capable of causing indiscriminate harm. In general, civilian cyberspaces offer less protection than military cyberspaces. To prevent enemy attacks, military cyberspace may be equipped with features like kill switches, system fencing, and geo-fencing that are absent from civilian cyberspace. Thus, an enemy's cyberattack intended for military objectives could have unanticipated effects on infrastructure used by the general public.[6]

Cyber attacks targeting critical infrastructure, such as healthcare systems, power grids, and financial networks, can have profound and often devastating impacts on civilians. These attacks can disrupt essential services, leading to loss of life, injury, and significant societal disruption. For instance, a cyber attack on a healthcare facility might incapacitate medical equipment, delay patient care, or compromise sensitive medical data, directly threatening the health and safety of individuals. Similarly, a cyber assault on power grids can result in widespread blackouts, affecting everything from homes to emergency services, while disruptions in financial systems can hinder access to funds and economic stability for civilians.

Current international humanitarian law (IHL) protections face challenges in adequately addressing these scenarios. While IHL principles such as distinction, proportionality, and necessity are designed to limit civilian harm during armed conflict, their application to cyber warfare is not always straightforward. The

[6] https://cams.mit.edu/wp-content/uploads/2017-10.pdf
https://www.un.org/counterterrorism/cybersecurity

interconnected nature of modern infrastructure makes it difficult to distinguish between military and civilian targets, as many critical services overlap. Additionally, the potential for collateral damage from cyber attacks is significant, yet the unpredictability of these attacks complicates assessments of proportionality.

According to the Question No.4 of the Research: - Fairly New International Conventions made for cyber attacks Regulations:

A. CT Tech Initiative:

The goal of the UNOCT/UNCCT Cybersecurity and New Technologies program is to strengthen Member States' and commercial organizations' ability to stop terrorist groups from using cyberattacks against vital infrastructure. In the event of a cyberattack, the program also aims to recover and restore the targeted systems and lessen the damage of the attack.

The CT TECH initiative was started in 2022 by UNOCT/UNCCT and INTERPOL with the goal of assisting Member States in using new and emerging technologies to combat terrorism and enhancing the ability of law enforcement and criminal justice authorities in a few partner nations to prevent the use of these technologies for terrorist purposes. Under the UNCCT Global Counter-Terrorism Programme on Cybersecurity and New Technologies, CT TECH is carried out with funding from the European Union.

Additionally, international and regional cooperation, the implementation of the biennial reviews of the United Nations Global Counter-Terrorism Strategies, pertinent Security Council resolutions, and consideration of the UN Human Rights Due Diligence Policy on Support for Non-United Nations Security Forces (HRDDP) will be used to ensure human rights and civilian protection from cyber attacks.

The 2019 Recommendation on **Digital Security of Critical Activities** by the Economic Co-operation and Development (OECD) focused on "economic and social activities the interruption or disruption of which would have serious consequences" on specific targets, like the well-being of citizens or the efficient operation of the government. The specific infrastructure or services that are covered by the obligations of any new treaty could be determined by each state under this framework.

The German Council for Foreign Relations' more constrained 2023 plan, known as the "**Digital Geneva Convention,**" called on nations to sign bilateral agreements prohibiting the use of cyberspace to target specific key infrastructure.

To create a worldwide accountability system in cyberspace and to declare vital infrastructure a cyberattack-free zone. Additionally, it would expand on previous discussions in UN Security Council sessions regarding cyberattacks on vital infrastructure and the obligations of governments.[7]

RECOMMENDATIONS:

The attacks on vital infrastructure are getting more frequent, but the reaction cannot continue as usual. To safeguard vital infrastructure, the international community should think about ratifying a global cyber pact. A treaty might supplement current regulations and help raise the bar for cybersecurity globally in an area where numerous states are already actively committed.

Governments may oppose binding, prohibitive measures, and states' compliance with them will ultimately determine how much of an influence they have on the quantity and scope of cyberattacks. Positive

[7] https://unidir.org/files/publication/pdfs/cyberwarfare-and-international-law-382.pdf
https://www.scirp.org/journal/paperinformation?paperid=109997
https://www.unodc.org/unodc/en/frontpage/2024/August/united-nations_-member-states-finalize-a-new-cybercrime-convention.html

responsibilities centered on cybersecurity and the security of operators of Critical infrastructure, however, have the potential to revolutionize the worldwide strengthening of cyber resilience, this also leads to protecting the civilians from danger.

CONCLUSION:

In conclusion, the escalating frequency of cyberattacks on vital infrastructure demands a proactive and unified global response. The proposal for a global cyber pact, aimed at establishing international cybersecurity standards, holds significant promise in reinforcing cyber resilience. By fostering cooperation and raising cybersecurity standards worldwide, such a treaty could mitigate the risks posed by both state-sponsored and non-state-sponsored cyberattacks, ultimately protecting civilians and enhancing global stability. The international community must act decisively to safeguard against these growing threats.