Humanizing Cyber War: A Geneva Conventions-Based Framework for Cyber Warfare

Shreyas Kumar[1], Maitreya Niranjan[1], Gourav Nagar[2], Sateesh Peddoju[3] and Komal Tripathi[3]

[1]Texas A&M University, College Station, USA
[2]Independent Researcher
[3]Indian Institute of Technology, Roorkee, India

shreyas.kumar@tamu.edu
maitreya.niranjan@tamu.edu
gouravnagar@ieee.org
sateesh@cs.iitr.ac.in
komal.tripathi@ch.iitr.ac.in

Abstract: Cyber warfare has emerged as a defining threat of the 21st century, presenting unique challenges that existing international humanitarian laws, such as the Geneva Conventions, are ill-equipped to address. This paper proposes a framework equivalent to the Geneva Conventions to regulate cyber warfare, ensuring the protection of civilian life, critical infrastructure, and digital systems during armed conflicts. By adapting the principles of distinction, proportionality, necessity, and humanity to the cyber domain, this proposal outlines protocols for safeguarding critical infrastructure, civilian data, maritime and satellite networks, and prohibiting indiscriminate cyber weapons and cyber hostage-taking. Drawing from case studies, such as the Russia-Ukraine conflict and the 2024 Israel-Hezbollah pager attack, the paper demonstrates how cyber warfare blurs the lines between combatants and civilians, amplifying the risk of collateral damage. Building on existing frameworks and academic proposals, this paper advocates for international cooperation, clear accountability mechanisms, and the establishment of humanitarian principles to govern cyber operations.

Keywords: Cyber warfare, Geneva Conventions, International Humanitarian Law (IHL), Civilian protection, Critical infrastructure, Cyber hostage-taking

1. Introduction

As cyber threats continue to grow in scale and sophistication, the traditional frameworks of international humanitarian law (IHL), such as the Geneva Conventions(International Committee of the Red Cross, 2023), face increasing challenges in addressing the unique nature of modern warfare. The Geneva Conventions have long provided vital protections for civilians, prisoners of war, and critical infrastructure in times of conflict, but they were developed in an era before the rise of digital warfare. Today, cyberattacks can disrupt essential services, target civilian infrastructure, and blur the lines between combatants and non-combatants. This paper explores the need to adapt the core principles of the Geneva Conventions—distinction, proportionality, and necessity—to the realm of cyber warfare. By proposing the Cyber Geneva Conventions, this framework aims to safeguard critical digital infrastructure, protect civilian data, and regulate cyber warfare tactics to minimize harm to non-combatants. The paper also advocates for international cooperation and clearer accountability mechanisms to ensure ethical conduct in the digital age.

2. Research Questions

What humanitarian principles should be included to protect critical infrastructure and civilian populations from cyber-attacks?

What are the potential Cyber Regulations to uphold the non cruelty principles that govern the Geneva Conventions?

3. Background

The Geneva Conventions established norms for warfare, ensuring humane treatment of individuals and the protection of civilians and non-combatants. However, the principles governing traditional warfare have not yet fully extended to cyberspace. Cyber warfare targets are often civilian and critical infrastructure, amplifying the risks and potential consequences. For example, a cyber attack on a chemical plant could trigger toxic releases, leading to mass casualties. As such, the need for international cyber-warfare regulations has become increasingly urgent to prevent these outcomes.

4. Salient Features of Geneva Conventions

The Geneva Conventions, established in 1949 and supplemented with protocols in 1977 and 2005, are a cornerstone of international humanitarian law, aiming to protect human rights and minimize suffering during armed conflicts. These conventions consist of four main treaties that cover the protection of the wounded, sick, and prisoners of war, as well as the safeguarding of civilians in conflict zones. The First Convention mandates the humane treatment of wounded and sick military personnel, while the Second extends this protection to those affected by naval warfare. The Third Convention focuses on prisoners of war, ensuring they receive basic rights like food, shelter, medical care, and protection from coercion. The Fourth Convention prohibits violence and intimidation against civilians and requires occupying powers to ensure the welfare of occupied populations. Further, the Geneva Conventions prohibit the taking of hostages, the use of excessively harmful weapons like chemical and biological arms, and emphasizes the importance of humanitarian organizations, such as the Red Cross, in monitoring and assisting in conflict zones. These treaties also introduce the principles of distinction and proportionality, ensuring that military force is used appropriately, minimizing harm to civilians and infrastructure. In essence, the Geneva Conventions provide a framework that seeks to balance military necessity with humanitarian concerns, ensuring that even in the chaos of war, fundamental human dignity is preserved.

5. Related Work

Cyber Warfare and the Application of International Humanitarian Law: Several studies have examined how International Humanitarian Law (IHL), specifically the Geneva Conventions, might be extended to cover the unique challenges of cyber warfare. Sutherland et al. (2015) explore how traditional IHL protections for civilians during kinetic warfare can be adapted to the digital domain, emphasizing the need to safeguard non-combatants from cyber attacks. Waugh (2020) highlights the pressing need for a comprehensive international framework to govern cyber warfare, similar to the Geneva Conventions' role in traditional conflicts. Gervais (2012) argues that existing laws of war are inadequate for cyber conflicts and advocates for the creation of new legal standards tailored to the digital battlefield. Eilstrup-Sangiovanni (2018) supports this view by critiquing the shortcomings of current frameworks like the Convention on Cybercrime(Council of Europe, (2001)) and the Tallinn Manual by Schmitt, M. N (2017), underscoring the need for an International Cyberwar Convention (ICWC) to address key legal ambiguities. A study by Hughes (2009) addresses the aftermath of the 2007 cyber conflict between Estonia and Russia, highlighting the lack of a cohesive global framework for cyber warfare and the potential risks of a new digital arms race, calling for NATO and the Euro-Atlantic Community to take a leading role in establishing international cooperation. Biller's (2018) research specifically focuses on naval warfare, discussing how cyber vulnerabilities in modern naval operations challenge the protections provided by the Second Geneva Convention. Wallace and Visger (2018) counter the argument of a legal void in cyberspace by illustrating how customary international norms are already evolving, despite enforcement difficulties. Collectively, these papers highlight the ongoing discourse around adapting and expanding the Geneva Conventions to address cyber threats.

Challenges of Regulating Cyber Warfare: Cyber warfare presents unique obstacles in applying traditional legal principles such as distinction, proportionality, and accountability. Kalshoven, Zegveld, and the International Committee of the Red Cross (2001) discuss the complexities of maintaining the principle of distinction in cyberspace, where it can be difficult to differentiate between military and civilian targets. Fleck (2021) underscores the historical struggle of legal frameworks to keep up with rapid technological advancements, a challenge that cyber conflicts exemplify. Rauscher (2013) elaborates on the complexities of creating global norms for cyber warfare, noting the covert nature of cyber operations and the diverse actors involved. Forsythe (2005) suggests that traditional humanitarian principles could serve as a baseline for cyber regulations, while Stewart (2011) highlights the increased difficulty of enforcing accountability when dealing with anonymous or state-sponsored cyber attackers. These discussions point to the need for a new or revised international convention that can specifically address the challenges posed by cyber warfare.

Cyber and Chemical Catastrophes: Industrial disasters involving chemical facilities have demonstrated the catastrophic potential of safety lapses. In 2019, the Xiangshui Chemical Plant explosion in China resulted in 78 deaths and severe economic losses due to ignored safety regulations and previous warnings as mentioned by Yang et al. (2020). Similarly, the 2020 Beirut explosion according to Sivaraman and Varadharajan (2021) , triggered by improperly stored ammonium nitrate, caused over 200 deaths and massive economic damage, including the destruction of critical infrastructure. Earlier, in 2003, as covered by The New York Times (2003), the PetroChina Chuandongbei natural gas field explosion in Chongqing killed more than 233 people, showcasing the lethal risks when safety systems fail. These incidents highlight the devastating impact of chemical accidents

on lives, economies, and infrastructure. In 2017, the Triton malware attack on a Saudi petrochemical plant exposed the vulnerabilities of digital safety systems, as highlighted by the Federal Bureau of Investigation (FBI) (2022). Had the hackers succeeded in disabling safety controls, the consequences could have been disastrous, underscoring the urgent need for cybersecurity measures in industrial contexts.

Broader Perspectives on Modern Warfare Regulations: In addition to direct discussions on cyber warfare, other studies provide context for the adaptation of international law in response to modern conflicts. Bothe et al.(1982) and Dinstein (2016) delve into the ethical challenges of applying the Geneva Conventions in evolving warfare contexts, particularly where the line between combatants and non-combatants is increasingly blurred. Research by Wilson (2007) and Akande (2012) into conflicts involving non-state actors adds a layer of complexity relevant to cyber warfare, where both state and non-state entities engage in digital conflicts. These insights suggest that the principles of international law must evolve to keep pace with the changing landscape of conflict, whether through direct amendments to existing conventions or the creation of new, specialized treaties.

6. Methodology

The proposed framework was developed using a multifaceted approach aligned with the Geneva Conventions' principles of distinction, proportionality, necessity, and humanity, adapted to cyber warfare. Key cyber incidents, such as Russia-Ukraine operations (European Parliament, 2023) and Hezbollah Pager attack(CNN (2024)), were analyzed to assess challenges like blurred military-civilian lines and infrastructure risks. Expert input from cybersecurity professionals and legal scholars refined the framework's practicality and addressed regulatory gaps. Cyber targets were systematically classified—covering critical infrastructure, civilian data, and maritime/satellite networks—to establish clear protections and permissible operations. Finally, the framework applied the Geneva Conventions' principle across cyber domains, safeguarding civilians, essential systems, and humanitarian networks while introducing accountability mechanisms for violations.

6.1 Core Principles of Geneva Conventions

The Geneva Conventions' key principles—distinction, proportionality, necessity, and humanity—are essential for protecting civilians and limiting suffering during armed conflicts, but they face unique challenges in the cyber warfare era. The principle of distinction requires differentiating between military and civilian targets, yet cyberattacks often affect dual-use systems like power grids and hospitals, as seen in the Russia-Ukraine conflict. Proportionality limits harm relative to military gain, but cascading effects of cyber operations, such as the 2024 Israel-Hezbollah attack, complicate this assessment. The principle of necessity ensures actions are taken only for legitimate military purposes, yet operations like Stuxnet(Baezner, M. and Robin, P, (2017)) raise concerns about unintended consequences impacting neutral parties. The principle of humanity prohibits causing unnecessary suffering, which becomes critical when cyberattacks disrupt essential services like healthcare, water, or energy, leading to immense indirect harm. Lastly, protection of those hors de combat extends to safeguarding civilians, the wounded, and humanitarian networks from cyber operations that could endanger their safety. Adapting these principles to cyber warfare is imperative to ensure civilian systems are protected and ethical boundaries in digital conflicts are upheld.

6.2 Case Studies

6.2.1 Case study 1: Russia-Ukraine War – cyber operations in conventional conflict

The ongoing conflict between Russia and Ukraine offers a modern and evolving example of how cyber operations can complement traditional military tactics (European Parliament, 2023). Since the annexation of Crimea in 2014, and even more intensely during the full-scale invasion in 2022, Russia has deployed numerous cyberattacks against Ukrainian critical infrastructure, including power grids, financial systems, and government websites. These cyber operations have been integrated with kinetic strikes, often to create confusion, weaken defenses, and disrupt communications. The Russia-Ukraine conflict highlights hybrid warfare, where cyber operations amplify conventional military actions, blurring the lines between cybercrime, espionage, and acts of war. Attacks on Ukrainian power grids in 2015 and 2016 (Pollard, Miles, 2024) exposed the severe civilian impact of cyberattacks, underscoring the need for updated laws to protect non-combatants. Online agents called Sandworm, which is associated with Russia, targeted the Ukrainian power grid by disabling the substations responsible for providing electricity to localities. While Ukraine is a special case given their use of old Soviet equipment, these cyber-attacks conducted against Ukraine exemplify the nascent domain of cyber warfare and the need for stronger protections in international law. This conflict has intensified international debates on

interpreting laws of armed conflict in cyberspace, emphasizing the urgent need for a comprehensive international cyber convention to establish clear wartime standards.

6.2.2 Case study 2: Israel-Hezbollah Conflict – The 2024 pager attack

On September 17, 2024, Israel executed a technologically advanced attack against Hezbollah by embedding explosives within the batteries of pagers used by the group (CNN (2024)). When activated, these weaponized devices caused devastating explosions, resulting in the deaths of at least 37 individuals, including children, and injuring nearly 3,000, many of whom were civilian bystanders. This unprecedented operation highlighted the potential for leveraging everyday technology for strategic military purposes, raising significant ethical and legal questions under international law. The attack on pagers blurred the lines between combatants and civilians, impacting not only Hezbollah operatives but also nearby civilians, including children, highlighting challenges in controlling collateral damage when using cyber-physical weapons. This operation, which fused cyber and kinetic strategies by triggering explosives through digital means, raises concerns about regulating such weapons under international law, especially when personal communication devices are exploited as targets. The implications extend further in scenarios where soldiers work remotely, as targeting their devices could endanger entire families and uninvolved civilians. This underscores the urgent need for international cyber norms to protect non-combatants, even in indirect theaters of war.

The case studies highlight the inadequacy of the Geneva Conventions in addressing the evolving nature of warfare in the cyber age. As cyber operations merge with traditional military strategies, the lines between combatants and civilians blur, increasing risks to non-combatants. To protect civilians and uphold humanitarian principles, it is crucial to update international legal frameworks, extending Geneva protections to cyberspace and cyber-physical conflicts.

7. A Geneva Convention based Framework for Cyber Warfare

7.1 Clause 1: Protection of Critical Digital Infrastructure (Analogous to Protection of the Wounded and Sick)

In traditional armed conflict, the Geneva Conventions mandate the protection of medical facilities and personnel to ensure that civilians and combatants alike receive necessary care. Similarly, in the realm of cyber warfare, critical infrastructure—such as hospitals, power grids, and water systems—must be safeguarded from cyberattacks. Cyber operations targeting these systems can result in cascading consequences, such as delays in medical care, widespread power outages, and disruptions in water supply, leading to indirect casualties and immense suffering.

7.1.1 Alignment of clause 1 with existing frameworks and research

Shinkaretskaya and Lyalina's work highlights the evolving landscape of safeguarding critical digital infrastructures at national and international levels. Their analysis emphasizes that existing provisions of international law can apply to the security of digital infrastructure, provided they are interpreted with an understanding of modern digitization and supported by additional measures. They argue that while "soft law" norms—such as guidelines, best practices, and informal agreements—are increasingly common, the need for binding international frameworks remains essential for consistent protection. (Shinkaretskaya and Lyalina, 2019)

The Executive Order issued by the U.S. in 2013 underscores the importance of collaboration between governments and the private sector to enhance the security of critical infrastructure. This framework proposes risk-based methodologies, improved information sharing, and voluntary adoption of cybersecurity practices, which could serve as a model for broader international efforts. For instance, the development of a Cybersecurity Framework by NIST has been instrumental in setting cross-sector security standards and could inform international cybersecurity norms. (The White House (2013))

7.1.2 Proposed application in cyber warfare context

Drawing from these sources, the cyber Geneva Conventions must include explicit provisions to protect critical infrastructure from cyberattacks during armed conflicts. This should involve establishing clear definitions and guidelines for what constitutes "critical infrastructure" in the digital age, ensuring that there is no ambiguity about which systems require protection. Additionally, enhancing international cooperation is essential to develop shared standards for safeguarding such infrastructure, similar to the NIST Cybersecurity Framework, to create a cohesive global approach. Finally, the Convention should establish enforcement mechanisms to hold both state and non-state actors accountable for cyber operations that compromise essential services, ensuring that violators face appropriate consequences.

7.2 Clause 2: Protection of Maritime and Satellite Networks (Analogous to Protection of Shipwrecked at Sea)

The Geneva Conventions establish the right to care and protection for individuals stranded at sea, emphasizing the need to protect human life in precarious maritime circumstances. Extending this principle to the cyber domain, maritime and satellite networks must be safeguarded from cyberattacks during conflicts, as they form critical lifelines for navigation, communication, and trade.

7.2.1 Alignment of clause 2 with existing frameworks and research

The Maritime Security Centre of Excellence (MARSEC COE) underscores the global reliance on maritime critical infrastructure (CI), which includes shipping lanes, ports, offshore energy installations, and underwater communication cables. These infrastructures are essential for international trade and energy security, carrying over 80% of global trade and facilitating 99% of international data traffic. MARSEC COE highlights that the protection of maritime CI is a cornerstone of global security, advocating for improved cybersecurity measures, intelligence sharing, and resilience strategies(Maritime Security Centre of Excellence (MARSEC COE) (2023)).

Tedeschi, Sciancalepore, and Di Pietro (2022) identify satellite-based communication (SATCOM) systems as pivotal to navigation, communication, and defense operations. Their survey highlights the growing risks posed by jamming, spoofing, and eavesdropping attacks, exacerbated by the rapid advancements in adversarial technologies. The authors propose solutions such as anti-jamming mechanisms, quantum-based cryptography, and enhanced physical-layer security as essential measures to safeguard these systems. These recommendations align with the principles of non-interference and the protection of critical lifelines in conflict scenarios.

International organizations, including NATO, have incorporated maritime CI protection into strategic priorities. MARSEC COE emphasizes the importance of international cooperation and the adoption of multi-faceted approaches to address emerging threats. Similarly, the frameworks outlined by Tedeschi et al. call for greater collaboration between academia, industry, and governments to enhance the security of satellite networks.

7.2.2 Proposed application in cyber warfare context

The cyber Geneva Conventions would mandate the protection of these vital networks to prevent harm to civilian and economic interests. Drawing on insights from MARSEC COE and Tedeschi et al., this convention could strengthen cybersecurity measures for ports and shipping operations to prevent attacks that could disrupt global trade and endanger maritime workers. It would also develop and enforce standards for SATCOM security, addressing threats at both the physical and cryptographic layers. Additionally, the convention could incorporate advanced solutions, such as quantum-based key distribution and anti-jamming technologies, to enhance resilience against cyberattacks.

7.3 Clause 3: Safeguarding Civilian Data and Networks (Analogous to Protection of Civilians)

In a similar vein to civilian protection under the Fourth Geneva Convention, a cyber warfare framework could restrict cyber attacks on civilian data, such as personal identities or medical histories stored in government databases. For instance, in 2021, a cyber attack on Ireland's Health Service Executive(Hutton, B., and Bray, J., (2021)) caused widespread disruption in healthcare services. Ensuring that civilian data and essential systems are protected in times of cyber conflict prevents significant harm to non-combatants.

7.3.1 Alignment of clause 3 with existing frameworks and research

Hutchins (2021) highlights the growing prevalence of internet shutdowns during violent uprisings and armed conflicts, which disrupt civilian life and raise legal and ethical questions. The author emphasizes the inadequacy of existing international humanitarian law (IHL) in safeguarding civilian internet access and infrastructure during conflicts. Hutchins proposes a new legal framework that includes special protections for physical internet infrastructure and the recognition of civilian internet access as a vital humanitarian need. This framework also suggests the adoption of digital emblems, akin to the Red Cross, to mark protected civilian communications.

Pauwels (2022) discusses how the rise of AI technologies exacerbates risks to civilian data during cyber conflicts. Threats such as adversarial data manipulation and AI-augmented malware targeting critical civilian databases underscore the vulnerability of sensitive information like medical records and biometric data. Pauwels also identifies ambiguities in IHL regarding whether data sets should be classified as protected objects and stresses the importance of strengthening legal and technical frameworks. Collaborative efforts among states, private actors, and civil society are proposed as a means to ensure data integrity and mitigate cyber risks.

7.3.2 Proposed application in cyber warfare context

The principle of safeguarding civilian data and networks in cyber warfare directly parallels the Fourth Geneva Conventions' emphasis on civilian protection. Applying the insights from Hutchins (2021) and Pauwels (2022), civilian databases, such as those containing medical histories, personal identities, or critical urban infrastructure data, should be explicitly recognized as protected under the cyber Geneva Conventions. This would align with the broader principle of safeguarding non-combatants and their resources in armed conflicts. Additionally, governments and combatants should be prohibited from deliberately disrupting civilian internet access during conflicts. Adopting digital emblems, as proposed by Hutchins, could mark and protect networks essential to civilian communication and humanitarian activities. Drawing on Pauwels' recommendations, states should collaborate with private sector entities and international bodies to enhance cybersecurity measures for civilian data, including the use of encryption, secure data sharing protocols, and anticipatory strategies to identify and address vulnerabilities in civilian networks.

7.4 Clause 4: Distinction and Proportionality in Cyber Attacks

The principle of distinction mandates that attacks target only military objectives, not civilian infrastructure. In cyber warfare, this would translate to restricting attacks on non-military targets and ensuring that any cyber operations avoid excessive harm to civilian systems. For instance, in the 2008 Russia-Georgia conflict(Gorman, S., (2008)), cyber attacks targeted both government and civilian networks, disrupting essential services. The cyber Geneva Conventions would establish protocols ensuring that attacks are proportional and limited to legitimate military targets to prevent excessive collateral damage.

7.4.1 Alignment of clause 4 with existing frameworks and research

Pascucci (2017) highlights that while international humanitarian law (IHL) principles like distinction and proportionality are foundational, they face significant challenges in cyberspace. The Tallinn Manual, an expert-driven interpretation of IHL, attempts to guide these principles in cyber contexts, but it falls short in critical areas. Key issues include ambiguity in distinguishing civilian and military cyber objectives, particularly with regard to data and dual-use systems. There are also unclear definitions of "attack" and "damage," which lead to inconsistent proportionality assessments. Furthermore, there is a lack of guidelines for accounting for indirect effects, or "knock-on" impacts, in proportionality analysis. Pascucci argues for a targeted Additional Protocol IV to clarify these ambiguities and ensure consistent application of IHL in cyber conflicts.

Fenton (2019) emphasizes the strategic importance of cyber strikes and the challenges of applying *jus in bello*(law in war) proportionality in this domain. He notes that existing IHL struggles to regulate cyber actions due to issues like the dual-use nature of systems (e.g., civilian and military infrastructure interdependence) and the difficulty of predicting reverberating effects of cyber attacks. Fenton proposes developing a unified definition of cyberattacks to address their unique threats and establishing an international cyberwarfare agreement to codify proportionality standards, preventing unregulated and lethal cyber aggressions.

7.4.2 Proposed application in cyber warfare context

The principles of distinction and proportionality, foundational in traditional armed conflict, must be adapted for cyber warfare to prevent undue harm to civilian infrastructure and lives. Drawing on Pascucci (2017) and Fenton (2019), we propose that cyberattacks must adhere to a standardized proportionality analysis, considering not only direct effects but also the indirect impacts on civilian systems. This includes evaluating the cascading effects of disrupting interconnected networks like healthcare or financial systems. Furthermore, a unified international agreement should establish universally accepted proportionality standards for cyberwarfare, fostering collaboration between states, legal experts, and technology providers to create enforceable guidelines. An Additional Protocol IV should clarify key terms and thresholds for cyber warfare under IHL. This protocol would address ambiguities related to data as a protected object and establish consistent methodologies for collateral damage estimation.

7.5 Clause 5: Prohibition of Cyber Hostage-Taking

The Geneva Conventions prohibit hostage-taking(Geneva Conventions (1949)), and in the cyber realm, this could extend to ransomware attacks targeting civilian and critical infrastructure. Hostage-taking in cyber warfare often involves encrypting data and demanding ransom, essentially holding essential digital resources "hostage." An example would be the 2017 WannaCry attack, which locked access to the UK's National Health Service systems, endangering patient care. Prohibiting ransomware tactics in cyber warfare would reduce the risk of paralyzing vital services.

7.5.1 Alignment of clause 4 with existing frameworks and research

Lubin (2022) underscores the inadequacy of existing legal frameworks to effectively combat ransomware attacks. The transnational and decentralized nature of these operations presents significant enforcement challenges, as there is no unified international policy to address them. Lubin proposes treating ransomware as an international crime, which would enable coordinated cross-border prosecution, policy-making, and deterrence strategies. The lack of consensus and consistent enforcement mechanisms further exacerbates the issue, especially as ransomware disproportionately targets civilian systems, amplifying the importance of applying International Humanitarian Law (IHL) principles to such cases.

Biller (2023) highlights critical ambiguities within IHL regarding ransomware operations in armed conflicts. Key issues include whether data should qualify as an "object" under IHL and whether encrypting data constitutes an "attack." While IHL does not currently prohibit most ransomware uses against civilian targets, Biller points out areas of potential application, such as protections for medical data and critical infrastructure. Additionally, the prohibition on collective punishment could offer a basis for restricting ransomware operations that affect civilian systems indiscriminately.

7.6 Proposed Application in Cyber Warfare Context

The cyber Geneva Conventions could explicitly prohibit ransomware operations, treating them as violations of the prohibition against hostage-taking. This would ensure protections for civilian data and critical infrastructure against encryption-based extortion tactics. Building on insights from Lubin (2022) and Biller (2023), we propose establishing data as a protected entity under IHL, closing the gap that currently leaves ransomware operations ambiguously regulated. Additionally, ransomware attacks should be clearly defined as acts of hostility under IHL to ensure accountability. There should also be strengthened protections for categories such as medical systems, critical infrastructure, and civilian data repositories, which are often prime ransomware targets. Furthermore, international agreements should classify ransomware as an international crime, enabling coordinated responses to transnational operations.

8. Conclusion

This proposal outlines a pioneering approach to humanizing cyber warfare by establishing a framework akin to the Geneva Conventions, aimed at regulating the ethical use of cyber capabilities. By clearly defining permissible targets, enforcing accountability, and integrating humanitarian principles, the framework aims to safeguard critical digital infrastructure, protect civilian data, and minimize the collateral damage caused by cyber conflicts. Through international cooperation and robust monitoring, the framework emphasizes the urgent need for a secure, ethical, and stable cyberspace. This includes ensuring that vital systems, such as hospitals, chemical plants, and communication networks, are shielded from cyberattacks that could severely disrupt civilian life and economic activity.

References

Akande, D., (2012). Classification of armed conflicts: Relevant legal concepts. In: E. Wilmshurst, ed., International Law and the Classification of Conflicts, chapter 3. Oxford University Press. Oxford Legal Studies Research Paper No. 50/2012.

Baezner, M. and Robin, P., (2017). Hotspot analysis: Stuxnet. Version 1. Risk and Resilience Team, Center for Security Studies (CSS), ETH Zürich. Zürich,

Biller, J. (2018) 'Cyber operations and the Second Geneva Convention', International Review of the Red Cross, 100(907–909), pp. 165–183. doi:10.1017/S1816383119000055.

Biller, J., 2023. The Strategic Use of Ransomware Operations as a Method of Warfare. International Law Studies, 100, pp.483-511.

Bothe, M., Partsch, K.J., & Solf, W.A., (1982). New Rules for Victims of Armed Conflicts. Martinus Nijhoff Publishers

CNN, 2024. Israel pager attack Hezbollah Lebanon. [online] Available at: https://www.cnn.com/2024/09/27/middleeast/israel-pager-attack-hezbollah-lebanon-invs-intl/index.html [Accessed 14 November 2024].

Council of Europe, (2001). Convention on Cybercrime. Council of Europe. Adopted on 23 November 2001. Available at: https://www.refworld.org/legal/agreements/coe/2001/en/90189 [Accessed 19 November 2024].

Dinstein, Y. (2016) The Conduct of Hostilities under the Law of International Armed Conflict. 3rd edn. Cambridge: Cambridge University Press.

Eilstrup-Sangiovanni, M., (2018). Why the world needs an international cyberwar convention. Philosophical Technology, 31(3), pp.379-407. https://doi.org/10.1007/s13347-017-0271-5.

European Parliament, 2023. EXPO_BRI(2023)702594_EN.pdf. [online] Available at: https://www.europarl.europa.eu/RegData/etudes/BRIE/2023/702594/EXPO_BRI(2023)702594_EN.pdf [Accessed 14 November 2024].

Federal Bureau of Investigation (FBI) (2022) TRITON Malware Remains Threat to Global Critical Infrastructure Industrial Control Systems (ICS). Available at: https://www.ic3.gov/CSA/2022/220325.pdf [Accessed: 15 Nov. 2024].

Fleck, D., (2021). Historical development and legal basis. In: D. Fleck, ed., The Handbook of International Humanitarian Law, 4th ed. Oxford Academic.

Forsythe, D.P. (2005) The Humanitarians: The International Committee of the Red Cross. Cambridge: Cambridge University Press.

Geneva Conventions, (1949). Common Article 3. Cited in: Volume II, Chapter 32, § 2046.

Gervais, M. (2012). Cyber Attacks and the Laws of War. Journal of Law & Cyber Warfare, 1(1), 8–98.

Gorman, S., (2008). Georgia State's Computers Hit by Cyberattack. The Wall Street Journal, 12 August 2008.

Hughes, Rex. (2009). Toward a Regime for Global Cyber Warfare. 10.3233/978-1-60750-060-5-106.

Hutchins, Todd. (2021). Safeguarding Civilian Internet Access During Armed Conflict: Protecting Humanity's Most Important Resource in War. Science and Technology Law Review.

Hutton, B., and Bray, J., (2021). HSE may be impacted for six months by cyberattack, says Reid. The Irish Times, 16 June 2021.

International Committee of the Red Cross (ICRC) (2023) The Geneva Conventions of 1949 and their Additional Protocols. Available at: https://www.icrc.org/en/law-and-policy/geneva-conventions-and-their-commentaries#text940072 (Accessed: 11 Nov. 2024).

International Review of the Red Cross, n.d. IRRC-886-lin.pdf. [online] Available at: https://international-review.icrc.org/sites/default/files/irrc-886-lin.pdf [Accessed 14 November 2024].

Kalshoven, F., Zegveld, L. & International Committee Of The Red Cross. (2001) Constraints on the Waging of War an Introduction to International Humanitarian Law. Geneva: ICRC.

Lubin, A., 2022. The Law and Politics of Ransomware. Articles by Maurer Faculty, 3063.

Maritime Security Centre of Excellence (MARSEC COE) 2023, Maritime Critical Infrastructure Protection (MCIP) in a Changing Security Environment, MARSEC COE, Istanbul.

Microsoft, n.d. RW67QH. [online] Available at: https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RW67QH [Accessed 14 November 2024].

The White House (2013) Executive Order – Improving Critical Infrastructure Cybersecurity, 12 February. Available at: https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity [Accessed: 14 November 2024].

Pascucci, CDR Peter, "Distinction and Proportionality in Cyber War: Virtual Problems with a Real Solution" (2017). Minnesota Journal of International Law. 257.

Pauwels, E., 2022. Civilian Data in Cyberconflict: Legal and Geostrategic Considerations. In: The Ethics of Automated Warfare and Artificial Intelligence. [online] Available at: https://www.cigionline.org/articles/civilian-data-in-cyberconflict-legal-and-geostrategic-considerations/ [Accessed 14 November 2024].

Pictet, J., (1952). Commentary on the Geneva Conventions of 12 August 1949. ICRC.

Pollard, Miles (2024) "A Case Study of Russian Cyber-Attacks on the Ukrainian Power Grid: Implications and Best Practices for the United States," Pepperdine Policy Review: Vol. 16, Article 1.

Rauscher, K.,(2013). Writing the rules of cyberwar. IEEE Spectrum, 50(12), pp. 30-32.

Sandoz, Y., Swinarski, C. and Zimmermann, B., 1987. Commentary on the Additional Protocols. International Committee of the Red Cross (ICRC).

Schmitt, M. N., (2017). Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations. Cambridge University Press.

Shinkaretskaya, G.G. & Lyalina, I.S.. (2019). Safeguarding of critical digital infrastructures. 10.2991/iscde-19.2019.166.

Sivaraman, S. and Varadharajan, S., (2021). Investigative consequence analysis: A case study research of Beirut explosion accident. Journal of Loss Prevention in the Process Industries, 69, 104387.

Stewart, J.G.,(2011). The Grave Breaches Regime in the Geneva Conventions: A Critique of Codification. Journal of International Criminal Justice, 7(4), pp. 657-678.

Sutherland, I. et al. (2015) 'The Geneva Conventions and Cyber-Warfare: A Technical Approach', The RUSI Journal, 160(4), pp. 30–39. doi: 10.1080/03071847.2015.1079044.

Tedeschi, P., Sciancalepore, S. and Di Pietro, R. (2022) 'Satellite-based communications security: A survey of threats, solutions, and research challenges', Computer Networks, 216, p. 109246.

The New York Times (2003) 'Gas Well Explosion and Fumes Kill 191 in China', 26 December. Available at: https://www.nytimes.com/2003/12/26/world/gas-well-explosion-and-fumes-kill-191-in-china.html (Accessed: 15 Nov. 2024])

U.S. Department of State, 2023. Geneva Conventions Overview. Available at: https://www.state.gov/geneva-conventions/ [Accessed: 14 Nov. 2024]

United Nations Treaty Collection (2023) Geneva Conventions of 1949. Available at: https://treaties.un.org/doc/Publication/UNTS/Volume%2075/volume-75-I-973-English.pdf [Accessed: 11 Nov. 2024].

UNODC, n.d. Core principles of IHL. [online] Available at: https://www.unodc.org/e4j/en/terrorism/module-6/key-issues/core-principles-of-ihl.html [Accessed 14 November 2024].

Wallace, D., & Visger, M. (2018). Responding to the Call for a Digital Geneva Convention: An Open Letter to Brad Smith and the Technology Community. Journal of Law & Cyber Warfare, 6(2), 3–55.

WAUGH, S. (2020). Geneva Conventions for Cyber Warriors Long Overdue. National Defense, 104(797), 18–19. https://www.jstor.org/stable/27022945

Wilson, H.A., (2007). International Law and the Use of Force by National Liberation Movements. Oxford University Press.

Yang, X., Li, Y., Chen, Y., Li, Y., Dai, L., Feng, R. and Duh, Y.-S., (2020). Case study on the catastrophic explosion of a chemical plant for production of m-phenylenediamine. Journal of Loss Prevention in the Process Industries, 67, 104232.