INTERNATIONAL JOURNAL FOR LEGAL RESEARCH AND ANALYSIS

Open Access, Refereed Journal Multi Disciplinary
Peer Reviewed

www.ijlra.com

DISCLAIMER

EDITORIAL TEAM

EDITORS

Dr. Samrat Datta

Dr. Samrat Datta Seedling School of Law and Governance, Jaipur National University, Jaipur. Dr. Samrat Datta is currently associated with Seedling School of Law and Governance, Jaipur National University, Jaipur. Dr. Datta has completed his graduation i.e., B.A.LL.B. from Law College Dehradun, Hemvati Nandan Bahuguna Garhwal University, Srinagar, Uttarakhand. He is an alumnus of KIIT University, Bhubaneswar where he pursued his post-graduation (LL.M.) in Criminal Law and subsequently completed his Ph.D. in Police Law and Information Technology from the Pacific Academy of Higher Education and Research University, Udaipur in 2020. His area of interest and research is Criminal and Police Law. Dr. Datta has a teaching experience of 7 years in various law schools across North India and has held administrative positions like Academic Coordinator, Centre Superintendent for Examinations, Deputy Controller of Examinations, Member of the Proctorial Board

Dr. Namita Jain

Head & Associate Professor

School of Law, JECRC University, Jaipur Ph.D. (Commercial Law) LL.M., UGC -NET Post Graduation Diploma in Taxation law and Practice, Bachelor of Commerce.

Teaching Experience: 12 years, AWARDS AND RECOGNITION of Dr. Namita Jain are - ICF Global Excellence Award 2020 in the category of educationalist by I Can Foundation, India.India Women Empowerment Award in the category of "Emerging Excellence in Academics by Prime Time & Utkrisht Bharat Foundation, New Delhi.(2020). Conferred in FL Book of Top 21 Record Holders in the category of education by Fashion Lifestyle Magazine, New Delhi. (2020).Certificate of Appreciation for organizing and managing the Professional Development Training Program on IPR in Collaboration with Trade Innovations Services, Jaipur on March 14th, 2019

Mrs.S.Kalpana

Assistant professor of Law

Mrs.S.Kalpana, presently Assistant professor of Law, VelTech Rangarajan Dr. Sagunthala R & D Institute of Science and Technology, Avadi.Formerly Assistant professor of Law,Vels University in the year 2019 to 2020, Worked as Guest Faculty, Chennai Dr.Ambedkar Law College, Pudupakkam. Published one book. Published 8Articles in various reputed Law Journals. Conducted 1Moot court competition and participated in nearly 80 National and International seminars and webinars conducted on various subjects of Law. Did ML in Criminal Law and Criminal Justice Administration.10 paper presentations in various National and International seminars. Attended more than 10 FDP programs. Ph.D. in Law pursuing.

Avinash Kumar

Avinash Kumar has completed his Ph.D. in International Investment Law from the Dept. of Law & Governance, Central University of South Bihar. His research work is on "International Investment Agreement and State's right to regulate Foreign Investment." He qualified UGC-NET and has been selected for the prestigious ICSSR Doctoral Fellowship.He is an alumnus of the Faculty of Law, University of Delhi. Formerly he has been elected as Students Union President of Law Centre-1, University of Delhi.Moreover, he completed his LL.M. from the University of Delhi (2014-16), dissertation on "Cross-border Merger & Acquisition"; LL.B. from the University of Delhi (2011-14), and B.A. (Hons.) from Maharaja Agrasen College, University of Delhi. He has also obtained P.G. Diploma in IPR from the Indian Society of International Law, New Delhi.He has qualified UGC – NET examination and has been awarded ICSSR – Doctoral Fellowship. He has published six-plus articles and presented 9 plus papers in national and international seminars/conferences. He participated in several workshops on research methodology and teaching and learning.

ABOUT US

INTERNATIONAL JOURNAL FOR LEGAL RESEARCH & ANLAYSIS ISSN

2582-6433 is an Online Journal is Monthly, Peer Review, Academic Journal, Published online, that seeks to provide an interactive platform for the publication of Short Articles, Long Articles, Book Review, Case Comments, Research Papers, Essay in the field of Law & Multidisciplinary issue. Our aim is to upgrade the level of interaction and discourse about contemporary issues of law. We are eager to become a highly cited academic publication, through quality contributions from students, academics, professionals from the industry, the bar and the bench. INTERNATIONAL JOURNAL FOR LEGAL RESEARCH & ANALYSIS ISSN 2582-6433 welcomes contributions from all legal branches, as long as the work is original, unpublished and is in consonance with the submission guidelines.

AN ENQUIRY INTO THE LEGAL CHALLENGES OF CYBER WARFARE IN INTERNATIONAL LAW

AUTHORED BY - DR. M.S. SHARMILA[**]

VISHWA. B[*]

Abstract:

This article examines the legal issues raised by cyberwar in the context of international law. It explores how current legal standards, such as the Geneva Conventions, apply to cyberwar and points out where gaps exist in their coverage. The paper also discusses the accountability implications and challenges of attributing cyberattacks to specific perpetrators. It also highlights current efforts to create new legal frameworks and policies to address these issues. Using several recent case studies, the essay highlights the urgent need to modify legal responses to adequately address the complexities of modern cyberwar.

Keywords: Cyber Warfare, jus in bello, jus ad bellum, International Law.

1. Introduction:

The earliest reference of the terminology cyber war was used in an article written by John Arquilla and David Ronfeldt which in itself was titled as "Cyberwar is Coming"[1]. Cyber war simply would seem to mean that it is the war in the cyberspace of one country into another. I am sure that none of us would have forgotten the WannaCry Ransomware in 2017 or the Blue Whale Challenge. Going further into these topics, we are now concerned about what cyber war actually is. The UNODC module defines it as "*cyberwarfare* is used to describe cyber acts that compromise and disrupt critical infrastructure systems, which amount to an armed attack."[2] With the increasing advancements in the globe in relation to the technology, on one hand we are all elated to see the world inside a six inch device; on the other hand, we are constantly in a paranoid as to what this will all lead to. Cyber war generally becomes a subject of international law because it denotes an attack on the nation as a whole. In this article, I have

[1] John Arquilla and David Ronfeldt, Cyberwar is Coming! in Comparative Strategy, Vol. 12, No. 2, Spring 1993, pp. 141–165, 144.

[2] Katharina.kiener-Manu *Cybercrime module 14 key issues: Cyberwarfare*, *Cybercrime Module 14 Key Issues: Cyberwarfare*. Available at: https://www.unodc.org/e4j/en/cybercrime/module-14/key-issues/cyberwarfare.html (Accessed: 15 August 2024).

made an attempt to discuss how this concept of cyber warfare in international law, and also tried to explain the problems in attribution of cyber war with real world examples.

2. International Law and Cyber Warfare:

As we all know, international law is the law of the nations. International law aims at creating a set of principles or norms and obligations like the *jus cogens* and *erga omnes* to maintain international peace and security among nations. When it is about wars, international law intervenes to set the standards, and the measures to prevent wars and also it deals with the maintenance of human rights and humanitarian rights. This brings us now to a question. What is the reaction of International Law to the emerging concerns of cyber warfare? Whether the law regulates cyber war the way it regulates an armed war?

There are two doctrines/concepts that are in relevance to cyber warfare under international law. One is the concept of *jus ad bellum*, which delineates the use of force in international law. This concept literally translates to 'right of war'. This concept of *jus ad bellum* is found to be present in the UN Charter under article 2(4)[3], 39[4] and 51[5]. However, there is no definition for "use of force," "threat of force," or "armed attack" in the United Nations Charter[6]. Nations recognise, nevertheless, that some unfriendly acts—regardless of their magnitude—do not qualify as the use of force. Examples of these include trade decisions that are unfavourable, space-based surveillance, boycotts, the termination of diplomatic relations, communication blockages, espionage, economic competition or sanctions, and political and economic coercion. A declared war, a territorial occupation, a naval blockade, and the use of armed force against civilians or military personnel stationed overseas are all examples of an armed attack. On the other hand, there are no established guidelines for evaluating offensive cyber activities.

Let us now move into another concept involving cyber war, which is *jus in bello* or simply, International Humanitarian Law. *Jus in bello* refers to the body of international law that dictates how parties behave during armed conflict. Its fundamental tenets are necessity—limiting force to that which is required to achieve military objectives—proportionality—minimizing injury

[3] **Article 2(4) of the UN Charter 1945 which states about** Prohibition on the threat or use of force
[4] **Article 39 of the UN Charter 1945 which states about** Action with respect to threats to the peace, breaches of the peace, and acts of aggression
[5] **Article 51 of the UN Charter 1945 which states about** Right of self-defense
[6] Madubuike-Ekwe, J.N. (2021) 'Cyberattack and the use of force in international law', Beijing Law Review, 12(02), pp. 631–649. doi:10.4236/blr.2021.122034.

to civilians, and distinction—differentiating between military targets and civilians[7]. It is evident from the definition of this concept that this concept was used only at times of armed conflict. The central problem even faced today is that how this concept could be connected to a cyber war or a cyber operation, In cyber war, it calls into question the legitimacy of cyberattacks in the context of cyberwar, particularly when they result in bodily injury. One complicated example is the Stuxnet worm, which was created by the USA and Israel to interfere with Iran's nuclear program[8]. Although it seriously damaged centrifuges physically, its legality is still up for discussion because digital sabotage rather than conventional military force was deployed. This emphasises how difficult it is to modify current legislation to account for the particularities of cyber operations. Cyberwarfare is impacted by a number of provisions from important agreements under International Humanitarian Law (IHL), especially those that deal with protecting civilians. Parties are required to use the principle of distinction, which requires them to distinguish between civilians and combatants, as stated in Article 48 of the Additional Protocol I (1977) to the Geneva Conventions[9]. The same protocol's Article 51[10] forbids direct assaults on civilians. Attacks on undefended towns, villages, or buildings are prohibited by Article 25 of the Hague Convention IV (1907)[11], which also applies to civilian infrastructure in cyberspace. Cyberattacks directed at water sources or hospitals would go against this accepted *jus in bello* guidelines.

Other than International Humanitarian law, there are numerous other concepts by which Cyberwarfare and International Law are connected. The area where cyberwarfare and international law collide is complicated and constantly changing. Traditional legal frameworks, such as the UN Charter, offer some advice, but there are difficulties because cyber activities are distinct. Important questions include identifying whether an attack on a computer system qualifies as a use of force, assigning blame, and incorporating international humanitarian law into cyber operations. Additional frameworks for tackling cyber-related issues include human rights law, regulations from the International Telecommunication Union (ITU), and special treaties like the Budapest Convention on Cybercrime[12]. The need for precise and functional

[7] *Jus ad bellum and jus in Bello* (2024) *International Committee of the Red Cross*. Available at: https://www.icrc.org/en/law-and-policy/jus-ad-bellum-and-jus-bello (Accessed: 17 August 2024).
[8] Kushner, D. (2024) *The real story of stuxnet, IEEE Spectrum*. Available at: https://spectrum.ieee.org/the-real-story-of-stuxnet (Accessed: 18 August 2024).
[9] Article 51 of the Additional Protocol I (1977) to the Geneva Conventions
[10] Article 48 of the Additional Protocol I (1977) to the Geneva Conventions
[11] Supra, note 10
[12] *Budapest Convention - Cybercrime - www.coe.int* (2024b) *Cybercrime*. Available at: https://www.coe.int (Accessed: 17 August 2024).

international legal principles governing cyberwarfare is growing as technology develops.

3. Challenges faced in attribution of cyber attacks

For a number of reasons, attribution in cyberattacks is a difficult and complex process. Attackers' identities may be hidden by their anonymity and traceability, which are frequently made possible by tools like VPNs, proxies, and botnets[13]. Advanced techniques like "false flags,"[14] in which attackers purposefully mislead investigators, can make attribution efforts even more difficult. Different legal systems and investigation practices between nations make it challenging to exchange information and coordinate efforts, which impedes international collaboration.[15]

It might take a lot of time and resources to analyse digital evidence due to its technological complexity, which calls for specific knowledge and advanced equipment. A climate of doubt can also be created by political objectives, which might persuade governments or state-sponsored groups to refrain from attributing assaults to their enemies.

Particularly, when international law tries to step in, attribution in cyberattacks becomes complex because of the challenges regarding state responsibilities and sovereignty. For fear of worsening diplomatic ties or raising tensions, states frequently hesitate to assign blame for attacks to other states[16]. The efficacy of legislative frameworks intended to combat cyber dangers may be harmed by this unwillingness to abide by international law. Furthermore, it may be challenging to establish whether non-state actors or a state is directly accountable for a cyberattack due to their complexity. These difficulties leave a legal void that may make it more difficult to prosecute offenders and prevent such incidents in the future.

The mere fact that a cyberattack or cyberespionage does not qualify as an act of war does not

[13] Sheldon, R. (2024) *What is cyber attribution? Definition from TechTarget*, *Security*. Available at: https://www.techtarget.com/searchsecurity/definition/cyber-attribution#:~:text=Challenges%20of%20cyber%20attribution,be%20challenging%20even%20for%20them. (Accessed: 17 August 2024).

[14] *What is a false flag? how state-based hackers cover their tracks* (2020) *CSO Online*. Available at: https://www.csoonline.com/article/568799/what-is-a-false-flag-how-state-based-hackers-cover-their-tracks.html (Accessed: 17 August 2024).

[15] Supra, note 14

[16] Vis Legis Law Practice, A. (2023) *Cybersecurity challenges in international law*, *LinkedIn*. Available at: https://www.linkedin.com/pulse/cybersecurity-challenges-international-law-vllp2017-y5uxf/ (Accessed: 17 August 2024).

imply that there is no legislation against such wrongs in international law. interference with the territory, airspace, seaspace, or economy of a state, even if not forbidden by UN Charter Article 2(4) is forbidden by the general non-interventionist stance. This feature is seen in several UN accords, ICJ rulings and resolutions denouncing coercion, meddling, or intrusion that stops short of using physical force. Some of this behaviour has been described by the ICJ as "fewer grave forms" of force that transgress the non-interventionist principle yet do not invoking a victim's Article 51 rights[17].

4. Case Studies

Although several significant cases provide pertinent insights, the International Court of Justice (ICJ) has not yet directly decided any cases that are solely concerned with cyber-attacks. State responsibility and the principle of due diligence, which can be applied to cyber activities, were established in the "Corfu Channel Case" (1949)[18]. State responsibility and non-intervention were emphasized in the 1986 case Nicaragua v. United States[19], which is relevant to situations involving state-sponsored cyberattacks. The 1996 advisory opinion titled "Legality of the Threat or Use of Nuclear Weapons"[20] emphasized the application of proportionality and necessity principles, as well as international humanitarian law, to cyberattacks that have a significant impact on civilian infrastructure. In addition, in order to comprehend accountability in cyber warfare, the "Application of the Convention on the Prevention and Punishment of the Crime of Genocide" case from 2007 established standards for state responsibility. The international legal framework for dealing with cyberattacks is influenced collectively by these cases.

The intricate relationship between cyberwarfare and international law is brought to light by recent cyberconflicts. Russian cyberattacks against Ukraine's infrastructure during the conflict between the two countries (2022–2023)[21] raised questions about compliance with international humanitarian law, specifically with regard to proportionality and distinction. Similar

[17] *Cyber Security and international law*. Available at: https://www.chathamhouse.org (Accessed: 17 August 2024).
[18] ICJ Rep 244, ICGJ 201 (ICJ 1949)
[19] 1984] ICJ Rep 392
[20] ICJ Rep 226, ICGJ 205
[21] *The role of cyber in the Russian War against Ukraine*. Available at: https://www.europarl.europa.eu/RegData/etudes/BRIE/2023/702594/EXPO_BRI(2023)702594_EN.pdf (Accessed: 17 August 2024).

cyberattacks on vital infrastructure occurred during the Israeli Iranian cyber conflict (2023)[22], testing the boundaries of state sovereignty in cyberspace and upending the non-intervention principle. The relevance of economic security in international law was highlighted in 2022 by a cyberattack on Taiwan's semiconductor sector. Additionally, debates on the potential applicability of Article 5 of the NATO Treaty[23] to cyber operations were spurred by several cyberattacks against NATO military systems in 2022. These instances show how cyberwarfare is a dynamic field that is governed by international law.

5. Conclusion

The legal difficulties posed by cyber warfare in international law are a reflection of a complex and changing landscape in which conventional legal frameworks struggle to keep up with technological advancements. When it comes to attribution, accountability, and the application of existing legal norms, cyber-attacks are unique, necessitating a nuanced strategy to guarantee effective regulation and response.

One of the most significant obstacles in combating cyberwarfare is still attribution. Cyber operations, in contrast to conventional attacks, frequently conceal the identity of the perpetrator, making it more difficult to hold states or actors accountable. Cybercriminals can operate with relative impunity due to the anonymity and borderlessness of cyberspace, making it difficult to pinpoint and demonstrate responsibility. International law and cybersecurity practices must advance simultaneously to resolve this problem. The accuracy of attribution can be improved through enhanced collaboration and information sharing among states, organizations from the private sector, and international organizations. In cyber incidents, standard procedures for gathering and analyzing evidence can also make it easier to identify those responsible. In addition, consistent attribution and accountability can be established through the establishment and implementation of international norms for cyber operations that are comparable to those for conventional warfare.

In addition, the current international legal system must be more stringent and adaptable to cyber

[22] *Cyberattacks by Iran, Hezbollah have tripled during the war, says Israel Cyber czar | The Times of Israel*. Available at: https://www.timesofisrael.com/cyberattacks-by-iran-hezbollah-have-tripled-during-the-war-says-israel-cyber-czar/ (Accessed: 17 August 2024).

[23] Nato (2022) *The North Atlantic Treaty, NATO*. Available at: https://www.nato.int/cps/en/natohq/official_texts_17120.htm (Accessed: 18 August 2024).

warfare's realities. Even though the Geneva Conventions are fundamental, they do not fully address the particulars of cyber conflicts. New or revised international agreements that are specifically tailored to cyber warfare are urgently needed. The definitions, rules of engagement, and accountability mechanisms for cyber operations that cause significant harm or disruption ought to be clearly outlined in these agreements. The legal basis for responding to and preventing cyberattacks would be strengthened as a result of this.

The protection of civilian entities and critical infrastructure in cyberspace must also be emphasized in international law. In order to safeguard civilian life and maintain economic stability, the legal principles governing cyberattacks must evolve as they increasingly target infrastructure and essential services. This could entail developing comprehensive response strategies for states and international organizations as well as specific international regulations to protect critical infrastructure from cyber threats.

Furthermore, it is essential to encourage international dialogue and cooperation. As a global problem that crosses national boundaries, cyber warfare must be effectively addressed through collaboration. Common standards and procedures for cyber security, attribution, and response can be developed with the help of multilateral agreements and forums. Regular discussions and exercises between nations can improve preparedness and establish a common understanding of acceptable cyberspace behavior.

In conclusion, a multifaceted strategy that includes enhancing global cooperation, strengthening international legal frameworks, and improving attribution methods is necessary to address the legal challenges posed by cyber warfare. The international community will be able to better manage and reduce the risks posed by cyber warfare if these areas are developed. This will ensure that the legal system effectively upholds the principles of accountability, security, and justice in the digital age.