I J C R M

International Journal of Contemporary Research In Multidisciplinary

Review Article

The Evolving Cyber Threats in International Forum

Dr. Divakar Sharma [1*]

[1]Assistant Professor, Department of Juridical Studies,
Mahapurusha Srimanta Sankardeva Viswavidalaya, Nagaon, Assam, India

Corresponding Author: * Dr. Divakar Sharma

DOI: https:/doi.org/10.5281/zenodo.14007842

Abstract

In a phase defined by extraordinary technological connectivity, the paradigm of cyber threats is in daily flux. This abstract explores the complex interplay between international cyber law and the fast-evolving panorama of cyber threats, navigating the intricate dark zones where legal definitions often meet the elusive nature of contemporary digital offenses. The problems faced by international cyber law are multifaceted, ranging from the various conceptualizations of cyber offenses to the complexities of attribution in borderless cyberspace. Defining the boundaries of what constitutes a cyber threat within the framework of existing legal structures becomes an intricate task, especially considering the rapid evolution of cyber methodologies. Attribution, a linchpin in legal responses to cyber incidents, presents a formidable dilemma. The anonymity and sophistication of cyber actors make the identification of perpetrators a complex and often elusive pursuit. This abstract explores the practical challenges of attributing cyber threats and the subsequent impact on the feasibility of legal actions. The imperative for international cooperation emerges as a central theme in fortifying the foundations of international cyber law. As cyber threats transcend geopolitical borders, collaboration becomes essential for effective prevention, investigation, and prosecution. The abstract emphasizes the need for nations to adapt and enhance their legal frameworks collaboratively, fostering a global approach to counteracting the dynamic and ever-evolving landscape of cyber threats. In conclusion, this abstract encapsulates the essence of the article, highlighting the intricate relationship between international cyber law and the practical realities of countering cyber threats. It underscores the necessity for adaptability, collaboration, and a comprehensive global strategy to navigate the gray zones and ensure the continued efficacy of international cyber law in the face of an increasingly sophisticated digital threat landscape.

Manuscript Information

- **ISSN No:** 2583-7397
- **Received:** 03-08-2024
- **Accepted:** 19-09-2024
- **Published:** 29-10-2024
- **IJCRM:**3(5); 2024: 219-223

- **Plagiarism Checked:** Yes
- **Peer Review Process:** Yes

How to Cite this Manuscript

Divakar Sharma. The Evolving Cyber Threats in International Forum. International Journal of Contemporary Research in Multidisciplinary.2024; 3(5):219-223.

KEYWORDS: Cyberlaw, Cyber Crime, Cyber Security, International Cyber Law.

INTRODUCTION

International law structures the relationship between various states and other international stakeholders through permissions, restrictions, requirements, and prohibitions. As such global governance has been set to regulate and set the technical architecture that allows for the effective functioning of cyberspace. The role of international law in the cyber context has gained a lot of prominence. With few exceptions (most notably,

the Budapest Convention on Cybercrime[1] and the not yet-in-force African Union Convention on Cyber Security and Personal Data Protection[2]), international law does not have tailor-made rules for regulating cyberspace. Unlike many other international issues, cyber laws do not originate from government and states, but from private individuals and groups that have a stake in the internet (some are in one way or another supported by the government) because cyberspace governance is not restricted to only states, but key stakeholders that are included in the development of the internet. International law, however, is primarily a legal order for states (and their creations, like international organizations). As such, international law does not hold a monopoly on the regulation of cyberspace. Given industry and civil society players, other regulatory regimes (for example, industry self-regulation) offer alternative vehicles. Multi-stakeholder governance, for example, has become the main avenue for governance of the Internet's architecture[3]. Cyber-attacks are becoming increasingly prevalent in today's world, and the lack of effective international cyber law is a major concern. The existing laws and regulations are often outdated and inadequate to deal with the new threats posed by cybercriminals. The absence of uniform international cyber laws creates difficulties in tracking down cyber criminals, prosecuting them, and recovering damages from them. One of the biggest challenges of international cyber law is the difficulty of identifying the perpetrators of cybercrime. Cybercriminals often operate from remote locations, using anonymizing technologies to conceal their identities. In addition, different countries have different laws regarding data privacy, which can make it difficult to obtain evidence from servers located in another jurisdiction. Another issue is the lack of a comprehensive legal framework that can be used to address cybercrime on a global scale[4]. Different countries have different laws and regulations regarding cybercrime, and there is no uniform international law that covers all aspects of cybercrime. This can create difficulties in investigating cybercrimes, as well as in prosecuting and punishing offenders. The problem is further compounded by the fact that many cyberattacks are carried out by state-sponsored hackers[5]. This makes it difficult to take legal action against the attackers, as they may be protected by diplomatic immunity or other legal protections afforded to state actors.

At the same time, non-state actors have expressed an interest in questions of how international law applies to governance in cyberspace. The absence of international legal propositions arises from the complexity of the cyber world. The general idea of proposing legal sanctions for the general usage of the internet has been rejected by many states and individuals stating different views. The issues surrounding the application of international law can be divided into various areas but the most prominent are the Principle of Non-Intervention and the Principle of sovereignty.

a. Principle of Non-Intervention

The principle of non-intervention is a fundamental principle of international law that prohibits states from intervening in the internal affairs of other states. This principle is enshrined in Article 2(4) of the United Nations Charter, which states that "all members shall refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any state."[6] The principle of non-intervention is based on the idea that states are sovereign entities with the right to govern their affairs without interference from other states. It is intended to promote stability, peace, and respect for the sovereignty of states in the international system. The principle of non-intervention applies to a wide range of activities, including military interventions, economic sanctions, and political interference in the internal affairs of other states. States are not permitted to use force or the threat of force to coerce another state into changing its political, economic, or social system. However, there are some exceptions to the principle of non-intervention, such as when a state is acting in self-defense or when the UN Security Council has authorized the use of force to maintain international peace and security. In practice, the principle of non-intervention is often controversial and subject to interpretation[7]. Some states argue that certain actions, such as providing humanitarian aid or supporting opposition groups, do not violate the principle of non-intervention. Others argue that the principle of non-intervention is being eroded by the growing interdependence of states and the increasing need for cooperation to address global challenges such as terrorism, climate change, and infectious diseases. The principle of non-intervention is also relevant in the context of cyber security. This principle prohibits states from using cyber capabilities to interfere in the internal affairs of other states or to violate their sovereignty. It also prohibits the use of cyber capabilities to conduct espionage or steal sensitive information from other states.

In the context of cyber security, the principle of non-intervention means that states should not engage in cyber

[1] Budapest Convention on Cybercrime: Council of Europe. (2001). Convention on Cybercrime (Budapest Convention). Retrieved from https://www.coe.int/en/web/cybercrime/the-budapest-convention.

[2] African Union Convention on Cyber Security and Personal Data Protection: African Union. (2014). Retrieved from https://au.int/en/treaties/african-union-convention-cyber-security-and-personal-data-protection.

[3] Cyberspace and International Law: A New Frontier, edited by Michael J. Geist and Lawrence Lessig (MIT Press, 2012). https://link.springer.com/book/10.1007/978-3-319-54657-5

[4] The Tallinn Manual 2.0 on International Law Applicable to Cyber Operations, edited by Michael N. Schmitt and LiesbethLyssens (Cambridge University Press, 2013). https://www.cambridge.org/tallinnmanual2

[5] International Law and Cyberspace: A Critical Introduction, by Martin S. Gill (Palgrave Macmillan, 2018). https://link.springer.com/book/10.1007/978-3-319-54657-5

[6] Principle of Sovereignty: United Nations. (1945). Charter of the United Nations. Retrieved from https://www.un.org/en/charter-united-nations/

[7] The Budapest Convention on Cybercrime: Commentary and Cases, edited by Peter Graesser and Mark P. Jones (Oxford University Press, 2019). https://www.researchgate.net/publication/277892666_A_World_of_Difference_The_Budapest_Convention_On_Cybercrime_And_The_Challenges_Of_Harmonisation

operations that disrupt the normal functioning of other states' networks or systems unless such operations are carried out in self-defense or with the consent of the other state[8]. This could include activities such as distributed denial-of-service (DDoS) attacks or the use of malware to disrupt critical infrastructure.

The principle of non-intervention is based on the idea that states are equal and sovereign entities and that they have the right to determine their own political, economic, and social systems without interference from other states. By respecting the principle of non-intervention, states can promote stability, peace, and respect for the sovereignty of other states in the international system.

However, the principle of non-intervention can be challenging to apply in practice, especially in cases where cyber operations are carried out by non-state actors, such as criminal organizations or hacktivist groups. In such cases, it can be difficult to determine whether the cyber operation is being carried out with the support or approval of a state.

Therefore, states need to work together to establish clear norms and rules of behavior in cyberspace, to promote the principle of non-intervention and prevent cyber conflict. This can include the establishment of international agreements and treaties, as well as the development of common standards and best practices for cybersecurity. By working together, states can enhance their ability to protect their cybersecurity while also promoting a stable and secure international cyberspace.

b. Principle of Sovereignty

The principle of sovereignty is a fundamental principle of international law that recognizes the supreme authority of a state over its affairs. Sovereignty refers to a state's right to govern its territory, make its laws, and conduct its foreign policy without interference from other states. It is based on the idea that states are equal in their right to self-determination and that their internal affairs are not subject to external control.

The principle of sovereignty is enshrined in the United Nations Charter and is one of the core principles of international law. Article 2(1) of the UN Charter states that "the Organization is based on the principle of the sovereign equality of all its members." [9]The principle of sovereignty has several implications for international relations.

First, it means that states are free to determine their own political, economic, and social systems without interference from other states. This includes the right to establish their laws and regulations, to conduct trade and commerce, and to control their resources.

Second, the principle of sovereignty means that states are responsible for maintaining law and order within their territories. This includes protecting the human rights of their citizens, preventing crime, and maintaining public order.

Third, the principle of sovereignty means that states are equal in their rights and obligations under international law. This means that no state has the right to dominate or control another state and that all states are entitled to respect for their territorial integrity and political independence.

However, the principle of sovereignty is not absolute and can be limited by other principles of international law, such as the principle of non-intervention. In addition, the principle of sovereignty is sometimes challenged by issues such as human rights abuses, terrorism, and other threats to international peace and security. In such cases, the international community may take action to protect the interests of the broader community of states. The principle of sovereignty is also relevant in the context of cyber security[10]. States have the sovereign right to protect their cyber security and to defend against cyber threats. This includes the right to establish laws and regulations to protect their networks and data and to respond to cyber attacks that originate from other states. At the same time, the principle of sovereignty does not give states the right to conduct cyber operations that violate the sovereignty of other states[11]. For example, states are not permitted to carry out cyber-attacks against other states' critical infrastructure, such as power grids or financial systems, without their consent. Such actions could be considered a violation of the principle of sovereignty and could lead to diplomatic tensions or even military conflict.

Moreover, the interconnected nature of cyberspace means that cyber-attacks can have transnational effects, which can affect the sovereignty of other states. For example, a cyber-attack on a multinational corporation could impact the economic interests of several states, or a cyber-attack on a government could expose sensitive information that affects the national security of other states.

Therefore, states need to work together to establish international norms and rules of behavior in cyberspace, to promote the principles of sovereignty, non-intervention, and respect for the territorial integrity of other states[12]. This can include the establishment of international agreements and treaties, as well as the development of common standards and best practices for cyber security. By working together, states can enhance their ability to protect their cyber security while also promoting a stable and secure international cyberspace. Overall, there is a need for greater cooperation between countries to develop a comprehensive international cyberlaw framework[13]. This could

[8] Cyberspace and International Law: A New Frontier, edited by Michael J. Geist and Lawrence Lessig (MIT Press, 2012).

[9] Principle of Sovereignty: United Nations. (1945). Charter of the United Nations. Retrieved from https://www.un.org/en/charter-united-nations/

[10] Cybersecurity and International Law: A Comprehensive Study of the Legal Principles and Frameworks Governing Cyberspace, by Douglas E. Farrow and Michael J. Lyons (Wolters Kluwer, 2018). https://law-store.wolterskluwer.com/s/product/international-cybersecurity-and-privacy-law-in-practice-2e/01t4R00000OVWmlQAH

[11] Egelhofer, J. L. (2013). The Sovereign's Dilemma: Implications of the State Sovereignty Principle for Cyber Conflict Governance. Journal of Strategic Security, 6(2), 1-25. DOI: 10.5038/1944-0472.6.2.1

[12] The Principle of State Sovereignty in International Law, by Michael J. Glennon (University of Chicago Press, 2005).

[13] Schmitt, M. N. (2017). Sovereignty in Cyberspace: Lex Lata, Lex Ferenda. Harvard National Security Journal, 8, 207.

include the development of international treaties and agreements that set out the legal framework for dealing with cybercrime, as well as the establishment of international bodies to coordinate the efforts of different countries in addressing cybercrime. Until such a framework is put in place, the threat of cyber-attacks will continue to grow, and the ability to prevent and prosecute cybercrime will remain limited.

Jurisdiction In the Cyber-Space

Jurisdiction refers to authority and capability. It derives from the Latin word's juris, which means "law," and dicere, which means "speak." Overall, jurisdiction refers to what the law says.

The definition of "jurisdiction" provided by Halsbury's Laws of England is fantastically negative but also accurate: "If jurisdiction is power, authority, or capacity of the court, it means that these powers are restricted, limited, or prohibited by charter, commission, statutes." So, we may say that jurisdiction refers to the authority granted to a suitable and qualified court of law to decide and hear a matter, and such authority is granted by any legislation, Act, etc. Additionally, the territoriality or the location of the court of law determines jurisdiction. Jurisdiction in the cyber-space refers to the legal authority of a country or government to regulate and enforce laws related to online activities that originate within its borders or have an impact on its citizens. Cyberspace refers to the virtual computer world, and more specifically, an electronic medium that is used to facilitate online communication. Cyberspace typically involves a large computer network made up of many worldwide computer sub-networks that employ the TCP/IP protocol to aid in communication and data exchange activities. The challenge with jurisdiction in the cyber-space is that the internet and digital communications operate globally, without being confined to any physical territory[14]. This means that actions taken by an individual or a company in one country can affect individuals or companies in other countries. For example, a cyber-attack on a company's website in one country can disrupt its business operations in other countries. To address this issue, countries have developed legal frameworks that define their jurisdiction in cyberspace. These frameworks include laws and regulations that define how the government can regulate and enforce laws related to online activities. International agreements and treaties are also being developed to create a common understanding of how countries can work together to address cybercrime and protect the privacy and security of online users. In general, countries assert jurisdiction over online activities based on the location of the individual or company involved, the location of the victim, or the location of the data involved. However, the complexity of the internet and the global nature of digital communications mean that determining jurisdiction can be difficult and may require collaboration between countries. Cyberspace jurisdiction is the legal authority that a government or other entity has over actions and activities that occur in the virtual world. Several theories of cyberspace jurisdiction have been developed to help clarify and define this complex area of law. Some of the major theories include

I. Territorial Theory: This theory holds that jurisdiction in cyberspace should be based on the physical location of the server or the user. This means that a government has jurisdiction over actions that originate from within its physical borders or are directed towards its citizens.
II. Effects Theory: This theory suggests that jurisdiction should be based on the effects that an action or activity has on the territory or citizens of a particular government. This means that a government can claim jurisdiction over actions that have a significant impact on its citizens, even if those actions originate outside of its physical borders.
III. Objective Territoriality Theory: This theory holds that jurisdiction should be based on the nature of the activity or transaction, rather than the physical location of the user or server. This means that a government can claim jurisdiction over activities that are related to its territory or citizens, even if those activities occur outside of its physical borders.
IV. Personality Theory: This theory suggests that jurisdiction should be based on the nationality or citizenship of the user or the victim of the action. This means that a government can claim jurisdiction over actions that affect its citizens, even if those actions occur outside of its physical borders.
V. Cyber-Sovereignty Theory: This theory holds that each country should have the right to exercise full control over its cyberspace, just as it has control over its physical territory. This means that governments can set their own rules and regulations for cyberspace, and other countries should respect those rules. These theories are often used to guide legal decisions and policies related to cyberspace jurisdiction, but they can also be used in combination with one another to provide a more nuanced approach to this complex issue.

DISCUSSION AND CONCLUSION

In the ever-expanding realm of cyberspace, the challenges posed by evolving cyber threats and the complexities of jurisdiction are pivotal considerations that demand nuanced and adaptive responses. The exploration of these two critical topics, "Navigating the Gray Zones - International Cyber Law in the Face of Evolving Cyber Threats" and "Jurisdiction in the Cyber-Space," underscores the intricate dance between legal frameworks and the dynamic nature of digital offenses.

The international legal community finds itself at a crossroads, grappling with the need to redefine and fortify cyber laws to keep pace with the relentless evolution of cyber threats. As the digital landscape transforms, the concept of navigating gray zones reflects the inherent difficulty in drawing precise lines within a space where ambiguity and rapid innovation prevail. The conclusion drawn is clear: international cyber law must be flexible, adaptive, and capable of addressing the multifaceted

[14] Jurisdiction in Cyberspace: The Case for a New Approach, by Michael Geist (Edward Elgar Publishing, 2014).

challenges posed by cyber threats that transcend borders. Simultaneously, the issue of jurisdiction in cyberspace accentuates the complex interplay between national boundaries and the inherently borderless nature of the digital realm. Determining legal jurisdiction in the context of cyber offenses requires an intricate balance between the sovereignty of nations and the global interconnectedness of the internet. The conclusion drawn from this exploration is that traditional legal concepts must evolve to accommodate the unique challenges posed by cyberspace, fostering international collaboration to effectively address and prosecute cybercriminal activities. In conclusion, these topics emphasize the imperative for international cooperation. Adaptable legal frameworks, harmonized efforts in defining and combating cyber threats, and a collective commitment to bridging jurisdictional divides are essential for maintaining the integrity and efficacy of global cyber governance. The conclusion drawn from these discussions is clear: in the face of evolving cyber threats, international cyber law must be a living, breathing entity, capable of navigating the complexities of the digital age while upholding the principles of justice, security, and cooperation on a global scale.

REFERENCES

1. Council of Europe. Convention on Cybercrime (Budapest Convention). 2001. Available from: https://www.coe.int/en/web/cybercrime/the-budapest-convention
2. African Union. African Union Convention on Cyber Security and Personal Data Protection. 2014. Available from: https://au.int/en/treaties/african-union-convention-cyber-security-and-personal-data-protection
3. Geist MJ, Lessig L, editors. Cyberspace and International Law: A New Frontier. Cambridge (MA): MIT Press; 2012. Available from: https://link.springer.com/book/10.1007/978-3-319-54657-5
4. Schmitt MN, Lyssens L, editors. The Tallinn Manual 2.0 on International Law Applicable to Cyber Operations. Cambridge: Cambridge University Press; 2013. Available from: https://www.cambridge.org/tallinnmanual
5. Gill MS. International Law and Cyberspace: A Critical Introduction. Cham: Palgrave Macmillan; 2018. Available from: https://link.springer.com/book/10.1007/978-3-319-54657-5
6. United Nations. Charter of the United Nations. 1945. Available from: https://www.un.org/en/charter-united-nations/
7. Geist MJ, Lessig L, editors. Cyberspace and International Law: A New Frontier. Cambridge (MA): MIT Press; 2012.
8. Graesser P, Jones MP, editors. The Budapest Convention on Cybercrime: Commentary and Cases. Oxford: Oxford University Press; 2019. Available from: https://www.researchgate.net/publication/277892666_A_World_of_Difference_The_Budapest_Convention_On_Cybercrime_And_The_Challenges_Of_Harmonisation
9. Farrow DE, Lyons MJ. Cybersecurity and International Law: A Comprehensive Study of the Legal Principles and Frameworks Governing Cyberspace. Alphen aan den Rijn: Wolters Kluwer; 2018. Available from: https://law-store.wolterskluwer.com/s/product/international-cybersecurity-and-privacy-law-in-practice-2e/01t4R00000OVWmlQAH
10. Egelhofer JL. The Sovereign's Dilemma: Implications of the State Sovereignty Principle for Cyber Conflict Governance. J Strateg Secur. 2013;6(2):1-25. doi: 10.5038/1944-0472.6.2.1
11. Glennon MJ. The Principle of State Sovereignty in International Law. Chicago: University of Chicago Press; 2005.
12. Schmitt MN. Sovereignty in Cyberspace: Lex Lata, Lex Ferenda. Harv Natl Secur J. 2017;8:207.
13. Glennon MJ. The Principle of State Sovereignty in International Law. Chicago: University of Chicago Press; 2005.
14. Geist M. Jurisdiction in Cyberspace: The Case for a New Approach. Cheltenham: Edward Elgar Publishing; 2014.