**International Journal of Law**
**www.lawjournals.org**
**ISSN: 2455-2194**
**Received: 08-12-2025, Accepted: 07-01-2026, Published: 22-01-2026**
**Volume 12, Issue 1, 2026, Page No. 150-154**

# A study on International Court of Justice and regulation of cyberspace

**Manjula**
Assistant Professor, Sarada Vilas Law College, Karnataka, India

**Abstract**
The quick growth of digital technologies and the increasing dependence of nations on cyberspace have led to a notable increase in cybercrime, creating intricate legal challenges on an international scale. Cybercrime crosses national borders, threatens national security, disrupts economic systems, and endangers individual rights, thus requiring a unified international legal response. In this scenario, the function of the International Court of Justice (ICJ) becomes more significant in developing the legal principles that govern State accountability and global collaboration in cyberspace. While the ICJ does not have direct authority over cybercrime, its decisions are vital in clarifying international legal norms related to cyber activities.

This paper examines the contribution of the ICJ to the regulation of cybercrime through its interpretation of general principles of international law, including State sovereignty, due diligence, non-intervention, and attribution of State responsibility. The study analyses how these principles may be applied to cyber operations that facilitate or enable cybercrime, such as cross-border hacking, cyber espionage, and large-scale cyberattacks. The paper further explores the interaction between ICJ jurisprudence and existing international regulatory frameworks, including multilateral conventions, United Nations resolutions, and customary international law, which collectively seek to combat cybercrime.

The research argues that while international cybercrime regulation remains fragmented, the ICJ provides authoritative guidance on the legal obligations of States in preventing, investigating, and responding to malicious cyber activities emanating from their territory. By clarifying the scope of State responsibility and due diligence in cyberspace, the ICJ indirectly strengthens global efforts to regulate cybercrime. The paper concludes that enhanced reliance on ICJ jurisprudence, combined with stronger international cooperation and harmonised legal frameworks, is essential for developing a coherent and effective international legal regime to address cybercrime in the digital age.

**Keywords:** International Court of Justice, cybercrime regulation, state responsibility in cyberspace, international cyber law, transnational cyber offences

## Introduction

The rapid expansion of cyberspace has transformed the way States interact, communicate, and exercise power in the international system. Cyberspace today underpins critical infrastructure, financial systems, military operations, diplomatic communications, and the everyday lives of individuals. Alongside its benefits, cyberspace has also emerged as a domain of conflict, giving rise to cyberattacks, digital espionage, misinformation campaigns, and transboundary cyber harms. These developments have posed significant challenges to the traditional framework of international law, which was primarily designed to regulate physical territory, armed conflict, and conventional inter-State relations. In this evolving context, the role of international legal institutions, particularly the International Court of Justice (ICJ), assumes critical importance.

The ICJ, established under the Charter of the United Nations, is entrusted with the task of settling legal disputes between States and providing advisory opinions on questions of international law. Although the Court was constituted in a pre-digital era, its mandate is sufficiently broad to encompass disputes arising from new and emerging domains, including cyberspace. Cyber operations often implicate foundational principles of international law such as State sovereignty, non-intervention, prohibition on the use of force, due diligence, and State responsibility. The interpretation and application of these principles to cyberspace-related conduct raise complex legal questions that demand authoritative judicial guidance [1].

Unlike other domains such as the law of the sea or international humanitarian law, cyberspace lacks a comprehensive and binding multilateral treaty governing State behavior. The absence of a unified regulatory framework has resulted in fragmented norms, soft law instruments, and competing State practices. In this normative uncertainty, the ICJ plays a vital role by clarifying how existing rules of international law apply to cyber activities. Even in the absence of direct cyber-specific cases, the Court's jurisprudence on attribution, jurisdiction, transboundary harm, and due diligence offers valuable insights for regulating State conduct in cyberspace [2].

Furthermore, the advisory jurisdiction of the ICJ provides an important avenue for the progressive development of international law relating to cyberspace. Advisory opinions requested by UN organs can address legal ambiguities surrounding cyber warfare, cyber espionage, and the protection of human rights in the digital sphere. While such opinions are not legally binding, they carry considerable persuasive authority and contribute to the formation of customary international law.

The study of the ICJ in relation to the regulation of cyberspace is therefore both timely and necessary. As cyber operations increasingly threaten international peace, security, and economic stability, reliance on rule-based governance becomes indispensable. Judicial clarification by the ICJ can help prevent escalation, promote accountability, and reinforce the principle that cyberspace is not a lawless domain beyond the reach of international law [3].

This research seeks to examine the role of the International Court of Justice in regulating cyberspace by analyzing its jurisdiction, jurisprudence, and normative influence. It aims to assess how far existing principles of international law, as interpreted by the ICJ, are capable of addressing cyber challenges and what limitations persist in the absence of explicit cyber-specific adjudication. By doing so, the study contributes to the broader discourse on international law, technological change, and global governance in the digital age [4].

**Research Methodology**

This research adopts a doctrinal and analytical method. Primary sources include ICJ judgments, advisory opinions, the UN Charter, and International Law Commission (ILC) Draft Articles on State Responsibility. Secondary sources consist of books, journal articles, UN reports, and scholarly commentaries on cyber law. Comparative references to State practice and emerging international norms are also used to support the analysis.

**Hypothesis**

1. The International Court of Justice is not adequately equipped to effectively regulate cyberspace due to the absence of explicit cyber-specific jurisdiction and technical expertise.
2. Existing principles of international law, as interpreted by the International Court of Justice, are insufficient to address the unique challenges posed by cyber operations and cyber warfare.

**Research Questions**

a. Does the absence of cyber-specific treaties and binding norms limit the effectiveness of the International Court of Justice in resolving cyberspace-related disputes?
b. To what extent does the lack of direct cyber adjudication by the International Court of Justice weaken legal certainty in the regulation of cyberspace?
c. Are traditional doctrines such as sovereignty, attribution, and state responsibility inadequate when applied to anonymous and transboundary cyber operations?
d. Has the voluntary nature of the International Court of Justice's jurisdiction reduced its practical relevance in regulating cyber conflicts between States?

**Cyberspace and International Law**

Cyberspace has emerged as a critical domain of human activity, reshaping governance, security, commerce, and diplomacy at both national and international levels. Defined broadly as the interconnected network of digital systems, data, and communication technologies, cyberspace transcends territorial boundaries and challenges the traditional foundations of international law, which are largely based on State sovereignty and physical geography. As cyber operations increasingly affect national security, critical infrastructure, and human rights, the applicability and adequacy of international law in regulating cyberspace have become central legal concerns.

At the international level, there is no single comprehensive treaty governing cyberspace. Instead, States rely on existing principles of international law, including sovereignty, non-intervention, prohibition on the use of force, due diligence, and State responsibility. The consensus emerging from United Nations processes is that international law applies to cyberspace, and cyber activities are not immune from legal regulation. Reports of the UN Group of Governmental Experts and the Open-Ended Working Group have affirmed that the Charter of the United Nations and customary international law govern State conduct in cyberspace [5]. However, the application of these principles to cyber operations raises complex issues such as attribution, anonymity, jurisdiction, and proportionality.

One of the major challenges in applying international law to cyberspace is attribution of responsibility. Cyber attacks are often conducted through proxy servers and non-State actors, making it difficult to identify the responsible State. Traditional doctrines of State responsibility, though theoretically applicable, face practical limitations in cyber contexts. Similarly, determining when a cyber-operation amounts to a "use of force" or an "armed attack" under international law remains contested [6]. These uncertainties weaken enforcement and create the risk of escalation without accountability.

From an Indian perspective, cyberspace regulation operates at the intersection of international obligations and domestic law. India has consistently maintained that international law applies to cyberspace while emphasizing State sovereignty and the need for capacity-building for developing countries. Domestically, India regulates cyberspace primarily through the Information Technology Act, 2000, which addresses cybercrime, data protection, and intermediary liability. While the Act provides a foundational legal framework, it is largely focused on internal regulation and does not directly address issues of international cyber conflict or State responsibility [7].

India's growing digital economy and strategic reliance on cyberspace make it increasingly vulnerable to cross-border cyber threats. Cyberattacks on financial systems, power grids, and government databases raise concerns relating to national security and international cooperation. In this context, India's engagement with international law on cyberspace reflects a cautious approach—supporting global norms while safeguarding strategic autonomy. The absence of binding international rules, however, places greater emphasis on judicial interpretation and customary law development.

International adjudicatory bodies such as the International Court of Justice play an indirect but significant role in shaping cyberspace regulation. Although the Court has not yet adjudicated a case exclusively on cyber operations, its jurisprudence on sovereignty, due diligence, and transboundary harm provides normative guidance for cyber disputes. Advisory opinions, in particular, offer a potential avenue for clarifying the legal status of cyber activities under international law [8].

The cyberspace presents both an opportunity and a challenge for international law. Existing legal principles are adaptable but strained by the technical and transboundary nature of cyber operations. For countries like India, the effective regulation of cyberspace requires a balanced approach that integrates domestic legislation, international cooperation, and judicial clarification. Strengthening international legal norms, while respecting sovereignty and developmental concerns, is essential to ensure that cyberspace remains a secure, stable, and law-governed domain [9].

**State Responsibility for Cyber Operations**

According to the ILC Draft Articles on State Responsibility, a State is internationally responsible for an act or omission attributable to it that constitutes a breach of an international obligation. These principles apply equally to cyber operations conducted by State organs or non-State actors acting under State control.

The principle of State responsibility is a cornerstone of international law, ensuring that States are held accountable for internationally wrongful acts attributable to them. With the rapid growth of cyber operations affecting national security, economic stability, and critical infrastructure, the application of State responsibility to cyberspace has become a crucial legal issue. Although cyber activities differ in form from traditional acts, they nonetheless raise questions of attribution, breach of international obligations, and consequences under established principles of international law.

Under classical international law, a State incurs responsibility when two conditions are satisfied: first, the conduct in question is attributable to the State, and second, the conduct constitutes a breach of an international legal obligation. These principles, reflected in the Articles on Responsibility of States for Internationally Wrongful Acts, are technologically neutral and therefore applicable to cyber operations. Cyber activities such as hacking, malware deployment, or cyber espionage may attract State responsibility if they violate obligations relating to sovereignty, non-intervention, prohibition of the use of force, or human rights [10].

Attribution presents the most significant challenge in cyber contexts. Cyber operations are often conducted anonymously, routed through multiple jurisdictions, and carried out by non-State actors or proxy groups. International law attributes conduct to a State when the actors operate under its instructions, direction, or control. While this standard is well established, proving such control in cyberspace is complex due to technical obfuscation and evidentiary difficulties. Nonetheless, the inability to easily attribute cyber conduct does not negate the applicability of State responsibility; it merely complicates its enforcement [11].

Another important aspect is the due diligence obligation of States. International law requires States to ensure that their territory is not used to cause harm to other States. In the cyber context, this implies a duty to take reasonable measures to prevent cyber operations emanating from a State's territory when the State has knowledge of such activities. Failure to act may itself constitute an internationally wrongful omission, even if the cyber operation is conducted by private actors [12].

The jurisprudence of the International Court of Justice, though not directly addressing cyber operations, provides authoritative guidance. The Court's reasoning in cases concerning attribution, use of force, and transboundary harm is increasingly relied upon in cyber law discourse. These principles support the view that cyber operations causing serious consequences—such as disruption of essential services or damage to critical infrastructure—may amount to internationally wrongful acts triggering State responsibility [13].

For States such as India, the doctrine of State responsibility is particularly relevant due to increasing exposure to cross-border cyber threats. While domestic laws like the Information Technology Act, 2000 address internal cybercrime, international responsibility mechanisms remain essential for addressing hostile cyber operations by or against States. India has emphasized the application of existing international law to cyberspace while advocating for greater clarity and cooperation at the global level [14].

State responsibility for cyber operations reflects the adaptability of international law to technological change. Although practical challenges of attribution and enforcement persist, the legal framework governing State responsibility remains applicable and essential. Strengthening international cooperation, evidentiary mechanisms, and judicial interpretation is necessary to ensure accountability and stability in cyberspace. Cyber operations, like traditional acts, must remain subject to the rule of law to prevent impunity and escalation in the digital domain.

**Limited Role of Artificial Intelligence in the Regulation of Cyberspace**

Artificial intelligence may enhance cyber capabilities by automating attacks or improving surveillance. However, from the perspective of the ICJ, AI is legally relevant only insofar as it affects attribution, scale, and consequences of cyber operations. AI does not alter the fundamental principles of State responsibility.

Artificial Intelligence (AI) has increasingly become an integral component of cyberspace, influencing areas such as data analytics, cybersecurity, surveillance, decision-making systems, and autonomous cyber operations. Despite its growing technological relevance, the role of Artificial Intelligence in the legal regulation of cyberspace, particularly within the framework of international law, remains limited and largely indirect. This limitation arises from normative uncertainty, lack of specific legal standards, and the State-centric structure of international legal responsibility.

One of the primary reasons for the limited role of AI in international cyberspace regulation is the absence of binding international legal instruments governing AI-enabled cyber operations. Existing international law frameworks were developed for human-controlled actions and do not adequately address autonomous or semi-autonomous systems. As a result, AI is treated as a tool used by States rather than as an independent legal actor. Accountability for AI-driven cyber operations continues to rest with States under traditional doctrines of attribution and State responsibility, thereby restricting AI's independent legal relevance [15].

Secondly, the opacity and unpredictability of AI systems pose serious challenges to legal regulation. Many AI systems operate through complex algorithms that lack transparency, making it difficult to explain decision-making processes or foresee outcomes. This "black box" nature complicates issues such as intent, proportionality, and foreseeability—key elements in assessing the legality of cyber operations under international law. Consequently, international adjudicatory bodies and policymakers remain cautious in recognizing an expanded regulatory role for AI [16].

Furthermore, from an institutional perspective, international courts and legal mechanisms are not yet equipped with the technical expertise required to adjudicate disputes involving advanced AI technologies. This limits the extent to which

AI-related cyber disputes can be effectively addressed through judicial processes. As a result, AI governance in cyberspace is currently shaped more by soft law instruments, ethical guidelines, and national policies rather than enforceable international legal norms.

While Artificial Intelligence plays a significant operational role in cyberspace, its legal role remains limited. International law continues to rely on human and State accountability, treating AI as a facilitating technology rather than a subject of regulation in itself. Until clear international standards and enforcement mechanisms emerge, AI's role in cyberspace regulation will remain constrained and supplementary rather than central [17].

**Case Laws**

1. **LICRA v. Yahoo! (France / U.S.) – Internet Jurisdiction & Effects Doctrine (2000–2006)**

**Facts:** French courts ordered Yahoo! to prevent French users from accessing Nazi memorabilia auctions hosted on its servers (outside France).

**Legal Issue:** Whether a national court can apply its domestic criminal law to Internet content accessible globally.

**Significance:** Established that effects of online activity in a territory could justify jurisdiction — a key issue for Internet jurisdiction and international disputes about which law applies to global online content. 19

2. **Schrems II (Data Protection Commissioner v Facebook / CJEU, 2020)**

**Court:** Court of Justice of the European Union (CJEU) Core Ruling: The EU-U.S. *Privacy* Shield framework for cross-border data transfers was invalidated because it did not adequately protect EU data subjects' privacy rights.

**International Impact:** Affects global data flows and the application of EU privacy standards to foreign states and multinational data systems — shaping how international rights like privacy are protected online [18].

3. **WhatsApp Inc. v. NSO Group (U.S., 2024)**

**Court:** U.S. District Court (Northern District of California) **Issue:** Deployment of Pegasus spyware through WhatsApp infrastructure.

**Outcome:** Court ruled NSO Group violated U.S. anti-hacking laws and breached contractual obligations due to unauthorized access to WhatsApp servers.

**Relevance for International Law:** Although a U.S. case, it demonstrates *cross-border cyber-surveillance accountability*, private entities' roles in state-linked cyber actions, and potential human rights impacts [19].

4. **United States v. Ivanov (U.S., 2001)**

**Jurisdiction-Related Ruling:** An American federal court held that U.S. cybercrime laws could apply to actions by a hacker physically located in Russia because the harmful effects occurred in the United States.

**Significance:** Sets an early precedent on extraterritorial application of cyber laws — important when considering *sovereignty and enforcement* online [20].

5. **Zakharov v. Russia (European Court of Human Rights, 2015)**

**Court:** European Court of Human Rights (ECtHR) Issue: Government mass surveillance of communications and lack of safeguards.

**Holding:** Russia's surveillance law violated Article 8 (privacy) of the European Convention on Human Rights.

**Relevance:** Though regional, *this decision influences international standards* on surveillance and privacy in cyberspace [21].

6. **Google Spain v. AEPD (CJEU, "Right to Be Forgotten")**

**Court:** CJEU (case often summarized in privacy law compilations)

**Outcome:** Individuals can request removal of links to personal information from search engine results under certain conditions.

**Significance:** Broadly shapes *data protection norms* in cyberspace and influences global digital privacy frameworks [22].

**Suggestions**

- Need for a global cyber treaty
- Expansion of International Court of Justice jurisdiction
- Establishment of a Cyber Dispute Tribunal
- Strengthening UN cyber norms
- Enhancing state reporting and attribution mechanisms
- Development of clearer international norms on cyber attribution
- Strengthening cooperation between legal and technical experts
- Encouraging States to accept International Court of Justice jurisdiction in cyber-related disputes
- Adoption of confidence-building measures in cyberspace

**Conclusion**

Cyberspace presents unprecedented challenges to international law, but it does not exist outside the legal order. The ICJ, through its interpretative authority and jurisprudence, is well placed to apply established principles of international law to cyber disputes. While practical and jurisdictional challenges remain, the Court can play a significant role in ensuring that State conduct in cyberspace remains governed by the rule of law. Strengthening international cooperation and normative clarity will be essential for effective cyber governance in the future.

However, international law has only partially adjusted to these realities. Existing frameworks like the UN Charter, Tallinn Manuals, and international human rights treaties provide guiding principles, but they lack binding enforcement mechanisms and universal consensus. Key issues such as attribution, state responsibility, jurisdiction, and privacy remain unsettled. The absence of harmonized global norms allows misuse of cyberspace and fuels geopolitical tensions.

Therefore, the future of international law must focus on developing clearer rules, strengthening cooperation, and balancing security with rights such as privacy and freedom of expression. Multilateral treaties, confidence-building

measures, and international cyber courts or reporting mechanisms may become essential. Ultimately, protecting cyberspace requires collective commitment, because no single state can address cyber threats alone. A stable and secure digital environment depends on evolving international law that reflects technological realities and shared global values.

**References**


1. Malcolm N. Shaw, International Law (9th ed.), 2021, 64–66.
2. James Crawford. State Responsibility: The General Part, 2013, 87–90.
3. Michael N. Schmitt (ed.), Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations, 2017, 1–3.
4. Nicholas Tsagourias, Russell Buchan. Research Handbook on International Law and Cyberspace, 2015, 15–18.
5. UN Group of Governmental Experts, Report on Developments in the Field of Information and Telecommunications in the Context of International Security, U.N. Doc. A/70/174, 2015.
6. Michael N. Schmitt (ed.), Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations, 2017, 4–8.
7. Information Technology Act, 2000, No. 21, Acts of Parliament, 2000 (India)
8. James Crawford, Brownlie's Principles of Public International Law (9th ed.), 2019, 451–453.
9. Nicholas Tsagourias, Russell Buchan, International Law and Cyberspace, 2021, 22–25.
10. James Crawford, State Responsibility: The General Part, 2013, 50–55.
11. Michael N. Schmitt (ed.), Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations, 2017, 82–90.
12. Nicholas Tsagourias, Russell Buchan. International Law and Cyberspace, 2021, 115–118.
13. Corfu Channel (U.K. v. Alb.), Judgment, 1949 I.C.J. Rep. 4.
14. Malcolm N. Shaw, International Law (9th ed.), 2021, 807–810.
15. James Crawford, State Responsibility: The General Part, 2013, 68–70.
16. Michael N. Schmitt (ed.), Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations, 2017, 35–37.
17. Nicholas Tsagourias, Russell Buchan. International Law and Cyberspace, 2021, 201–204.
18. Ligue contre le racism et I' antisemitisme (LICRA) and Union des etudiants juifs de France V/s Yahoo! Inc. *et al*
19. Data Protection Commissioner v/s Facebook Ireland Ltd and Maximilian Schrems (Case C-311/18)
20. Whatsapp Inc., v/s NSO Group Technologies Ltd.