INDIAN JOURNAL OF LEGAL REVIEW

VOLUME 5 AND ISSUE 11 OF 2025

INSTITUTE OF LEGAL EDUCATION

INDIAN JOURNAL OF LEGAL REVIEW

APIS – 3920 – 0001 | ISSN - 2583-2344

(Open Access Journal)

Journal's Home Page – https://ijlr.iledu.in/

Journal's Editorial Page - https://ijlr.iledu.in/editorial-board/

Volume 5 and Issue 11 of 2025 (Access Full Issue on - https://ijlr.iledu.in/volume-5-and-issue-11-of-2025/)

Publisher

Prasanna S,

Chairman of Institute of Legal Education

No. 08, Arul Nagar, Seera Thoppu,

Maudhanda Kurichi, Srirangam,

Tiruchirappalli – 620102

Phone : +91 94896 71437 - info@iledu.in / Chairman@iledu.in

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]

VOLUME 5 AND ISSUE 11 OF 2025

APIS – 3920 - 0001 *(and)* ISSN - 2583-2344

Published by

Institute of Legal Education

https://iledu.in

THE ATTRIBUTION CHALLENGE IN CYBER WARFARE AND INTERNATIONAL LAW

AUTHOR - AMAN KUMAR JHA, SUJAL CHHAJED & TANISHK BHAWSAR

STUDENTS AT NATIONAL LAW INSTITUTE UNIVERSITY, BHOPAL

BEST CITATION – AMAN KUMAR JHA, SUJAL CHHAJED & TANISHK BHAWSAR, THE ATTRIBUTION CHALLENGE IN CYBER WARFARE AND INTERNATIONAL LAW, INDIAN JOURNAL OF LEGAL REVIEW (IJLR), 5 (11) OF 2025, PG. 763-772, APIS – 3920 – 0001 & ISSN - 2583-2344

ABSTRACT

The increasing frequency and sophistication of cyber operations directed against states has exposed a critical gap in international law, the problem of attribution. Unlike conventional armed attacks, cyber operations are often conducted through obfuscation techniques, proxy actors, and transnational infrastructures, making it exceedingly difficult to identify perpetrators with legal certainty. This paper examines the attribution challenge in the context of cyber warfare and its implications for state responsibility under international law. It begins by outlining the existing legal framework governing the use of force, sovereignty, and non-intervention, with particular attention to the U.N. Charter and the International Law Commission's Draft Articles on State Responsibility. It then explores how these rules operate when applied to cyber operations, highlighting the unique technical and evidentiary barriers that complicate attribution. The paper further analyses landmark judicial decisions, including the ICJ's Nicaragua case and relevant jurisprudence from international tribunals, to demonstrate how thresholds of "effective control" and "overall control" remain contested when transposed to cyberspace. The role of international initiatives such as the Tallinn Manual, U.N. GGE and OEWG reports, and state practice is critically assessed to evaluate the gradual evolution of norms. By engaging with case studies of cyber incidents such as the Stuxnet attack, WannaCry ransomware, and election interference campaigns, the paper illustrates the intersection of law, technology, and geopolitics in shaping attribution strategies. Ultimately, it advocates for a more nuanced approach to attribution that blends legal, technical, and policy considerations, and proposes potential pathways for developing clearer standards of state responsibility in cyberspace.

Keywords: Cyber Warfare, Attribution, State Responsibility, International Law

1. INTRODUCTION

The rapid advancement of digital technologies has transformed cyberspace into a new domain of conflict, alongside land, sea, air, and outer space. Cyber warfare encompasses hostile activities conducted through computer networks with the potential to disrupt critical infrastructure, exfiltrate sensitive information, and weaken the military or economic stability of states. Unlike conventional warfare, cyber operations are characterized by anonymity, speed, and the involvement of non-traditional actors, which makes them difficult to detect, deter, and punish.

Incidents such as the Stuxnet attack on Iran's nuclear facilities in 2010, the NotPetya malware campaign of 2017, and the SolarWinds breach of 2020 have demonstrated the significant impact of cyber operations on global security. These incidents reveal the centrality of attribution the process of identifying and assigning responsibility for cyber operations to a state or non-state actor to the enforcement of international law. In traditional warfare, the origin of an armed attack is usually observable

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]

VOLUME 5 AND ISSUE 11 OF 2025

APIS – 3920 - 0001 *(and)* ISSN - 2583-2344

Published by

Institute of Legal Education

https://iledu.in

through physical evidence; in cyberspace, attackers can conceal their identities, route operations through multiple jurisdictions, and employ false flag tactics to mislead investigators.

The difficulty of attribution creates uncertainty in determining whether a cyber incident constitutes an armed attack, a violation of sovereignty, or merely an act of espionage. This lack of clarity undermines deterrence, weakens accountability, and threatens the stability of the international order. The existing legal framework, including the United Nations Charter, the Articles on State Responsibility, and guidance from instruments such as the Tallinn Manual, offers some tools for assessing attribution, but these remain inadequate to address the complexity of modern cyber operations.

This paper examines the legal standards that govern attribution in cyber warfare and highlights the gap between technological capability and legal responsibility. It analyses how attribution challenges complicate the application of international law and draws on case studies where attribution has been contested. Further, it evaluates emerging doctrines and international efforts aimed at strengthening accountability in cyberspace, ultimately suggesting ways to bridge the divide between law and practice.

2. DEFINITIONAL COMPLEXITIES OF CYBER WARFARE

2.1 Absence Of A Universally Accepted Definition

Cyber warfare remains a contested concept within both technological and legal discourse. Unlike traditional warfare, which is defined by armed hostilities and the use of kinetic force, cyber warfare operates through the manipulation of information systems and digital networks. It encompasses a range of hostile actions such as disabling critical infrastructure, interfering with communication systems, stealing sensitive state information, and spreading disinformation to destabilize political or economic systems. The ambiguity of its definition arises from the difficulty of distinguishing cyber warfare from related phenomena such as cybercrime, cyber espionage, and hacktivism, all of which may employ similar tools but differ in terms of purpose, scale, and actors involved.

2.2 Overlap Between Espionage, Sabotage, And Warfare

A key challenge in understanding cyber warfare lies in its hybrid character. Modern conflicts often combine conventional military operations with large-scale cyber campaigns, creating a layered battlefield where digital and physical strategies reinforce one another. The ongoing conflict in Ukraine demonstrates how cyber operations can be used to weaken adversary infrastructure and disrupt communication while complementing traditional military offensives.[1193] This fusion of domains complicates both strategic planning and legal regulation, as cyber operations may fall below the threshold of armed attack while still causing effects comparable to conventional warfare.[1194]

Another critical feature of cyber warfare is the diversity of actors involved. While states remain the primary players in large-scale cyber operations, non-state actors such as private contractors, hacktivist groups, and criminal syndicates often play a significant role.[1195] States may employ these actors directly or indirectly, creating layers of plausible deniability. This raises significant legal challenges in attribution, as existing frameworks of international law focus on state responsibility and struggle to address the blurred boundaries between state-sponsored and independently initiated cyber activities.

[1193] Florian J. Egloff, *Why International Law and Norms Do Little in Preventing Non-State Cyber Attacks*, 7 J. Cybersecurity 1 (2021), https://academic.oup.com/cybersecurity/article/7/1/tyab009/6168044.

[1194] Russell Buchan, *Cyber Operations Against Critical Infrastructure Under Norms of Responsible State Behaviour and International Law*, 30 Int'l J.L. & Info. Tech. 423 (2022), https://academic.oup.com/ijlit/article/30/4/423/7095534.

[1195] Kubo Mačák, *Decoding Article 8 of the International Law Commission's Articles on State Responsibility: Attribution of Cyber Operations by Non-State Actors*, 21 J. Conflict & Sec. L. 405 (2016), https://academic.oup.com/jcsl/article-abstract/21/3/405/2525375.

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]
VOLUME 5 AND ISSUE 11 OF 2025
APIS – 3920 - 0001 *(and)* ISSN - 2583-2344
Published by
Institute of Legal Education
https://iledu.in

2.3 Ambiguities In International Legal Classification

Furthermore, cyber operations transcend national borders almost instantly. A single attack may involve servers in multiple jurisdictions, making it difficult to identify its origin or establish jurisdiction for legal accountability. Unlike conventional warfare, where borders and territorial control provide clear markers of aggression, cyberspace is decentralized and borderless, limiting the effectiveness of traditional legal categories. This global reach allows states to project power asymmetrically and at relatively low cost, creating opportunities for weaker states or even non-state actors to challenge stronger powers.

Understanding the unique characteristics of cyber warfare is therefore crucial to examining the attribution challenge. Its anonymity, hybrid nature, multi-actor involvement, and transnational scope not only complicate technical detection but also strain the applicability of international legal norms.[1196] Before assessing the attribution problem directly, it is necessary to consider how international law currently regulates state responsibility in cyberspace and the extent to which existing doctrines can accommodate these new forms of conflict.[1197]

3. INTERNATIONAL LEGAL FRAMEWORK GOVERNING ATTRIBUTION

The attribution of cyber operations to states or state-controlled entities is primarily addressed through the general principles of international law rather than through a dedicated treaty regime. Existing frameworks, such as the United Nations Charter, the International Law Commission's Articles on State Responsibility, and interpretations developed by scholars and expert groups, provide the legal basis for assessing responsibility in cyberspace. However, the unique nature of cyber operations often makes it difficult to apply these principles with clarity and consistency.

3.1 The UN Charter And The Prohibition On The Use Of Force

The United Nations Charter establishes the foundational rules governing the use of force and the prohibition of aggression. Article 2(4)[1198] prohibits the threat or use of force against the territorial integrity or political independence of any state, while Article 51[1199] preserves the right of self-defence in the event of an armed attack. Whether and when a cyber operation crosses the threshold of "use of force" or "armed attack" remains contested.[1200] International jurisprudence, particularly the Nicaragua case before the International Court of Justice, provides guidance on the concepts of state responsibility and effective control over non-state actors, but these precedents were developed in the context of conventional conflicts and require adaptation to cyberspace.[1201]

The Articles on State Responsibility further provide that acts carried out by individuals or groups can be attributed to a state if they act on the instructions of, or under the direction or control of, that state.[1202] This principle becomes difficult to apply when cyber operations are routed through multiple networks, involve loosely affiliated groups, or rely on proxies that operate with tacit state support. The distinction between direct control, indirect encouragement, and mere tolerance is blurred in cyberspace, where states can maintain plausible deniability while benefiting from hostile operations conducted by third parties.

[1196] Marco Benatar & Kubo Mačák, *Cyber Attribution: Technical and Legal Approaches and Challenges*, 31 Eur. J. Int'l L. 941 (2020), https://academic.oup.com/ejil/article/31/3/941/5897247.
[1197] Jeffrey Carr, *Inside Cyber Warfare: Mapping the Cyber Underworld* (O'Reilly Media 2d ed. 2011).
[1198] Charter of the United Nation (adopted on 26 June 1945, entered into force on 24 October 1945) XV UNCIO 335 art 2, para. 4.
[1199] Charter of the United Nation (adopted on 26 June 1945, entered into force on 24 October 1945) XV UNCIO 335 art 51.
[1200] Marco Roscini, *Cyber Operations and the Use of Force in International Law* (Oxford Univ. Press 2014).
[1201] Military and Paramilitary Activities in and Against Nicaragua (Nicar. v. U.S.), Judgment, 1986 I.C.J. Rep. 14, para. 115 (June 27).
[1202] Int'l Law Comm'n, Draft Articles on State Responsibility for Internationally Wrongful Acts, U.N. Doc. A/56/10, art. 8 (2001).

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]

VOLUME 5 AND ISSUE 11 OF 2025

APIS – 3920 - 0001 *(and)* ISSN - 2583-2344

Published by

Institute of Legal Education

https://iledu.in

3.2 The Tallinn Manual And Expert Contributions

In the absence of binding treaties specifically regulating cyber warfare, non-binding instruments have played an influential role. The Tallinn Manual, prepared by a group of international law experts under the auspices of NATO's Cooperative Cyber Defence Centre of Excellence[1203] offers an interpretation of how existing rules of international law apply to cyber operations. Although not legally binding, it has been widely cited by policymakers and scholars for its attempt to adapt doctrines of sovereignty, due diligence, and state responsibility to cyberspace. The manual suggests that a cyber operation causing significant physical damage or equivalent effects may constitute a use of force, but it acknowledges that evidentiary challenges make attribution especially difficult.

3.3 Confidence-Building Measures And Voluntary Norms

Customary international law and soft law instruments have also contributed to shaping the discussion. Confidence-building measures adopted by the Organization for Security and Co-operation in Europe (OSCE) and voluntary norms promoted by the United Nations Group of Governmental Experts reflect emerging consensus on responsible state behaviour.[1204] However, these measures remain politically binding rather than legally enforceable, limiting their effectiveness in resolving disputes over attribution.

4. THE ATTRIBUTION CHALLENGE IN PRACTICE

4.1 The Centrality And Complexity Of Attribution

Attribution lies at the heart of regulating cyber warfare, yet it remains one of the most complex and contested issues in international law. Unlike conventional attacks, where the aggressor can often be identified through physical evidence, cyber operations are intentionally designed to obscure responsibility.[1205] Attackers may disguise their digital footprints, employ anonymizing technologies, or route operations through servers in multiple jurisdictions, creating a chain of false leads that frustrates efforts to establish accountability. This technical opacity makes attribution not only a matter of forensic analysis but also of political judgment and legal interpretation.[1206]

From a technical standpoint, attribution relies on digital forensics, intelligence gathering, and behavioural analysis of malware and network traffic. These tools can sometimes identify likely perpetrators, but they rarely yield certainty. False flag operations, where attackers mimic the tactics or digital signatures of another state or group, further complicate the process. Moreover, the global nature of the internet allows malicious actors to exploit the infrastructure of neutral states, raising questions about whether responsibility lies with the state whose infrastructure was misused or with the true originator of the attack.[1207]

4.2 Legal Standards And The Burden Of Proof

The legal dimension of attribution presents even greater difficulties. International law requires a sufficiently high standard of proof before responsibility can be assigned to a state. The International Court of Justice has consistently emphasised the requirement of "effective

[1203] Michael N. Schmitt et al., *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (Cambridge Univ. Press 2017).

[1204] *U.N. Group of Gov't Experts on Devs. in the Field of Info. & Telecomms. in the Context of Int'l Sec., Rep. of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*, U.N. Doc. A/70/174 (July 22, 2015); *U.N. Open-Ended Working Grp. on Devs. in the Field of Info. & Telecomms. in the Context of Int'l Sec., Final Substantive Report*, U.N. Doc. A/AC.290/2021/CRP.2 (Mar. 10, 2021); Org. for Sec. & Co-operation in Eur., Decision No. 1202: *OSCE Confidence-Building Measures to Reduce the Risks of Conflict Stemming from the Use of Information and Communication Technologies*, PC.DEC/1202 (Dec. 3, 2013); Org. for Sec. & Co-operation in Eur., Decision No. 1106: *Initial Set of OSCE Confidence-Building Measures to Reduce the Risks of Conflict Stemming from the Use of Information and Communication Technologies*, PC.DEC/1106 (Dec. 3, 2011).

[1205] Heather Harrison Dinniss, *Cyber Warfare and the Laws of War* (Cambridge Univ. Press 2012).

[1206] Oona A. Hathaway et al., *The Law of Cyber-Attack*, 100 Cal. L. Rev. 817 (2012).

[1207] Austria, *Position Paper: Cyber Activities and International Law* (April 2024) https://docs-library.unoda.org/Open-Ended_Working_Group_on_Information_and_Communication_Technologies_-_(2021)/Austrian_Position_Paper_-_Cyber_Activities_ and_International_Law_(Final_23.04.2024).pdf.

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]

VOLUME 5 AND ISSUE 11 OF 2025

APIS – 3920 - 0001 *(and)* ISSN - 2583-2344

Published by

Institute of Legal Education

https://iledu.in

control" over non-state actors for attribution to occur.[1208] In the cyber context, however, proving such control is extremely difficult, as states may provide safe havens or indirect support without leaving evidence that meets the evidentiary threshold of international tribunals. States are therefore able to exploit ambiguity, denying involvement while reaping the strategic benefits of offensive cyber operations.

This gap between technical evidence and legal accountability is exacerbated by the political nature of attribution. States are often reluctant to disclose sensitive intelligence sources that could strengthen legal claims, as doing so might compromise national security or reveal classified capabilities. Instead, attribution is frequently declared through political statements, press releases, or coordinated announcements among allied states, rather than through judicial processes.[1209] This practice undermines the consistency and neutrality expected of international law, turning attribution into a tool of geopolitical contestation rather than a purely legal determination.

Another challenge arises from the spectrum of harm caused by cyber operations. Many operations fall below the threshold of armed attack yet still cause serious disruption, such as shutting down financial systems or paralyzing public services. In such cases, attribution becomes even more difficult to frame legally, as existing doctrines were developed with kinetic attacks in mind and do not account for the grey zone of cyber operations. The ambiguity surrounding thresholds enables states to conduct aggressive cyber campaigns while avoiding accountability under international law.

5. CASE STUDIES OF CONTESTED ATTRIBUTION

The complexity of attribution in cyber warfare is best illustrated through real-world incidents where responsibility has been disputed or deliberately obscured. Examining these cases provides insight into the technological, legal, and political difficulties of holding states accountable under international law.

5.1 The Stuxnet Operation (2010)

One of the earliest and most prominent examples is the Stuxnet operation of 2010, which targeted Iran's Natanz nuclear facility.[1210] The highly sophisticated malware disrupted centrifuge operations, setting back Iran's nuclear programme significantly. Although widely attributed to the United States and Israel based on technical indicators and intelligence leaks, no state has formally accepted responsibility. The lack of official acknowledgment highlights how states can benefit from strategic cyber operations while avoiding the legal and diplomatic consequences of attribution.[1211] For international law, Stuxnet raises fundamental questions about whether such operations constitute a "use of force" and how responsibility can be assigned in the absence of open admission.

5.2 The Notpetya Malware Attack (2017)

Another significant case is the NotPetya attack of 2017, which initially appeared to be ransomware but was later revealed to be a destructive malware campaign. The attack disrupted businesses and critical infrastructure worldwide, causing billions of dollars in damage.[1212] Western governments attributed the operation to Russia, asserting that it was aimed at destabilizing Ukraine, though Russia has consistently denied involvement. Despite broad political consensus on attribution, no legal proceedings have been pursued, reflecting the gap between political declarations and

[1208] Nicaragua case, p 3.

[1209] White House, Statement by the Press Secretary on the Executive Order, *Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure* (May 11, 2017), https://obamawhitehouse.archives.gov/the-press-office/2017/05/11/statement-press-secretary-executive-order-strengthening-cybersecurity ; U.K. Foreign & Commonwealth Office, *UK Attributes WannaCry Cyber Attack to North Korea* (Dec. 19, 2017), https://www.gov.uk/government/news/uk-attributes-wannacry-cyber-attack-to-north-korea; U.S. Dep't of Justice, *Six Russian GRU Officers Charged in Connection with Worldwide Deployment of Destructive NotPetya Malware and Other Disruptive Cyberattacks* (Oct. 19, 2020), https://www.justice.gov/opa/pr/six-russian-gru-officers-charged-connection-worldwide-deployment-destructive-notpetya-malware.

[1210] Ralph Langner, *Stuxnet: Dissecting a Cyberwarfare Weapon*, IEEE Security & Privacy, May-June 2011, p 49.

[1211] Nicolas Falliere et al., *W32.Stuxnet Dossier* (Symantec Corp., Version 1.4, Feb. 2011).

[1212] Andy Greenberg, *Sandworm: A New Era of Cyberwar and the Hunt for the Kremlin's Most Dangerous Hackers* (Doubleday 2019).

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]

VOLUME 5 AND ISSUE 11 OF 2025

APIS – 3920 - 0001 *(and)* ISSN - 2583-2344

Published by

Institute of Legal Education

https://iledu.in

enforceable accountability under international law. NotPetya illustrates how states can conduct wide-ranging operations with transnational consequences while leveraging plausible deniability to escape liability.

5.3 The SolarWinds Supply Chain Breach (2020)

The SolarWinds breach of 2020 further underscores attribution challenges. Hackers compromised a widely used software update, granting access to the networks of multiple United States government agencies and private companies. The United States attributed the operation to Russia's Foreign Intelligence Service, but once again, definitive legal proof was difficult to produce publicly.[1213] This incident demonstrated how sophisticated supply chain attacks complicate attribution by embedding malicious code deep within trusted systems, making it almost impossible for victims to distinguish between routine network activity and hostile intrusion until significant damage has been done.

5.4 Cyber Operations In The Russia–Ukraine Conflict

Finally, the ongoing Russia–Ukraine conflict provides a contemporary example of cyber warfare's hybrid nature. Since 2014, Ukraine has been subject to repeated cyberattacks targeting its power grid, financial systems, and government networks. Many of these operations have been attributed to Russian state-backed groups, yet formal legal accountability has been elusive. The integration of cyber operations with kinetic military offensives further complicates attribution, as it becomes difficult to disentangle cyber tactics from broader acts of aggression. These cases reveal that while political attribution may serve strategic purposes, the absence of reliable legal attribution mechanisms weakens the credibility of international law in addressing such conflicts.

Taken together, these incidents reveal the recurring pattern of contested attribution in cyber warfare. States exploit the anonymity of cyberspace, deny responsibility despite mounting evidence, and rely on the reluctance of adversaries to disclose intelligence sources.[1214] While technical forensics and political consensus can point toward likely perpetrators, the lack of judicially recognized standards leaves attribution in a grey zone, undermining the enforcement of international norms.

6. DOCTRINAL AND PRACTICAL LIMITATIONS IN ATTRIBUTION

6.1 Evidentiary And Doctrinal Challenges

The application of international law to cyber warfare encounters significant obstacles, most of which stem from the difficulties of attribution. Even though general principles such as sovereignty, non-intervention, and state responsibility are well established, their effectiveness in cyberspace is undermined by evidentiary, doctrinal, and enforcement challenges.

One of the most pressing difficulties is the evidentiary standard required for attribution. International tribunals, including the International Court of Justice, have traditionally required a high threshold of proof before holding states responsible for unlawful acts. In the Nicaragua case, the Court emphasised the need to demonstrate "effective control" by a state over the conduct of non-state actors. In cyberspace, however, evidence is often fragmentary, circumstantial, or classified, making it nearly impossible to meet such standards in judicial proceedings.[1215] States are

[1213] U.S. Cybersecurity & Infrastructure Sec. Agency, Joint Statement from the Cybersecurity and Infrastructure Security Agency (CISA), The Federal Bureau of Investigation (FBI), and The National Security Agency (NSA) (Jan. 5, 2021), https://www.cisa.gov/news/2021/01/05/joint-statement-cybersecurity-and-infrastructure-security-agency-cisa-federal-bureau.

[1214] FireEye, APT1: *Exposing One of China's Cyber Espionage Units* (2013); CrowdStrike, *Bears in the Midst: Intrusion into the Democratic National Committee* (June 15, 2016); Microsoft, *Defending Democracy Program: Lessons from the 2020 Elections*, https://blogs.microsoft.com/on-the-issues/2021/05/04/defending-democracy-program-lessons-2020-elections/.

[1215] Military and Paramilitary Activities in and Against Nicaragua (*Nicar. v. U.S.*), Judgment, 1986 I.C.J. Rep. 14, para. 115 (June 27); Corfu Channel (*U.K. v. Alb.*), Judgment, 1949 I.C.J. Rep. 4, 23 (Apr. 9) (establishing due diligence obligations); Application of the International Convention on the Elimination of All Forms of Racial Discrimination (*Geor. v. Russ.*), Preliminary Objections, 2011 I.C.J. Rep. 70, para. 142 (Apr. 1) (discussing effective control).

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]

VOLUME 5 AND ISSUE 11 OF 2025

APIS – 3920 - 0001 *(and)* ISSN - 2583-2344

Published by

Institute of Legal Education

https://iledu.in

reluctant to disclose sensitive intelligence sources or technological capabilities that could strengthen legal attribution, which results in attribution being made primarily through political channels rather than legal ones. This reliance on political attribution diminishes the neutrality and credibility of international law.[1216]

Sovereignty and jurisdictional issues present another layer of difficulty. Cyber operations frequently transit through multiple jurisdictions, using servers or digital infrastructure located in third states. This raises questions about whether the territorial sovereignty of those states has been violated and whether they bear any responsibility for failing to prevent the misuse of their infrastructure.[1217] The borderless nature of cyberspace challenges the traditional territorial foundations of international law, creating uncertainty about where and against whom legal responsibility should be asserted.

The involvement of non-state actors further complicates attribution. Cyber operations are often carried out by loosely organised hacker groups, private contractors, or criminal syndicates, some of which may have connections to state authorities while retaining nominal independence. Existing doctrines such as "effective control" or "overall control" are ill-suited to capture the complex and often opaque relationships between states and these actors.[1218] As a result, states can exploit such ambiguities by outsourcing cyber operations to third parties, maintaining plausible deniability while pursuing strategic objectives.[1219]

6.2 Enforcement And Accountability Gaps

Enforcement remains a final and significant challenge. Even when attribution is politically accepted, international law lacks robust mechanisms to compel accountability. The United Nations Security Council, which might otherwise serve as a forum for enforcement, is constrained by the veto powers of its permanent members many of whom are themselves accused of conducting cyber operations. Other mechanisms, such as international arbitration or claims commissions, are rarely invoked in this context.[1220] In practice, states resort to unilateral or coordinated countermeasures, including sanctions, indictments, and retaliatory cyber operations, which reflect power politics rather than consistent application of law.

These challenges collectively illustrate that the problem of attribution in cyber warfare is not merely technical but deeply legal and structural. Without clear evidentiary standards adapted to the cyber domain, without doctrines that reflect the realities of non-state involvement, and without effective enforcement mechanisms, international law struggles to impose accountability. The consequence is a legal vacuum in which cyber operations proliferate unchecked, undermining both the credibility of international law and the stability of the international order.

7. EMERGING APPROACHES AND PROPOSED SOLUTIONS

7.1 Due Diligence And Expanded Doctrines Of Responsibility

In response to the persistent difficulties of attribution, states and international bodies have begun exploring approaches that seek to adapt existing legal principles or develop new frameworks for cyberspace.[1221] These efforts remain fragmented and largely non-binding,

[1216] Duncan B. Hollis, *Re-Thinking the Boundaries of Law in Cyberspace: A Duty to Hack Back?*, 23 Va. J.L. & Tech. 503 (2020),https://ssrn.com/abstract=2424230.

[1217] Michael N. Schmitt, *Cyber Operations in International Law: The Use of Force, Collective Security, Self-Defense, and Armed Conflicts*, Nat'l Acad. Press (2010), https://nap.nationalacademies.org/read/12997/chapter/12.

[1218] *Prosecutor v. Tadić*, Case No. IT-94-1-A, Appeals Chamber Judgment, para. 131 (Int'l Crim. Trib. for the Former Yugoslavia July 15, 1999) (establishing "overall control" test).

[1219] William Banks, *The Bumpy Road to a Meaningful International Law of Cyber Attribution*, 113 Am. J. Int'l L. Unbound 430 (2019), https://www.cambridge.org/core/journals/american-journal-of-international-law/article/bumpy-road-to-a-meaningful-international-law-of-cyber-attribution/346DD8EBEB55C47469060CC3E9871538.

[1220] James A. Lewis, *Creating Accountability for Global Cyber Norms*, Ctr. for Strategic & Int'l Stud. (Aug. 2024), https://www.csis.org/analysis/creating-accountability-global-cyber-norms.

[1221] Scott J. Shackelford, *Managing Cyber Attacks in International Law*, Business, and Relations: In Search of Cyber Peace (Cambridge Univ. Press 2014).

but they represent important steps toward strengthening accountability in the digital domain.

One promising avenue has been the application of due diligence and related doctrines to cyberspace. Under international law, states have an obligation not to knowingly allow their territory to be used for acts that harm other states. Applied to cyber operations, this principle would require states to take reasonable measures to prevent their infrastructure from being used for hostile activities, even if they are not directly responsible for the attack. Although due diligence does not eliminate attribution challenges, it helps expand accountability by shifting some responsibility onto states that fail to act against malicious activities launched from within their jurisdictions.

7.2 Revisiting Control Doctrines And Multilateral Norm-Building

Doctrines of effective control and overall control, originally developed in relation to armed groups, are also being revisited in the cyber context. Scholars and practitioners argue that states should be held responsible not only for cyber operations they directly command but also for those carried out with substantial support or encouragement. Expanding the interpretation of control could help close the gap between the realities of cyber sponsorship and the narrow thresholds set by existing jurisprudence.

At the multilateral level, confidence-building measures and voluntary norms have played an important role. The United Nations Group of Governmental Experts (GGE) and the Open-Ended Working Group (OEWG) have produced reports outlining principles of responsible state behaviour in cyberspace, including commitments not to target critical infrastructure and to cooperate on attribution. Regional organisations such as the OSCE have adopted similar measures to promote transparency and reduce the risk of misattribution. While these initiatives lack legal enforceability, they create shared expectations of behaviour that can influence state practice over time.

7.3 Toward Treaties, Mechanisms, And Collective Attribution

Proposals for a dedicated cyber treaty or a specialised attribution mechanism have also gained traction. Some scholars advocate the establishment of an international body tasked with investigating cyber incidents and issuing impartial attribution findings, similar to the role of the International Atomic Energy Agency in nuclear governance. Others suggest integrating cyber-specific provisions into existing arms control or humanitarian law treaties. These proposals face political resistance, particularly from major powers reluctant to cede sovereignty or disclose capabilities, but they highlight the growing recognition that current frameworks are insufficient.

In parallel, states have developed unilateral and collective measures to address attribution outside formal legal channels. Coordinated public attributions by alliances such as NATO, the European Union, and the Five Eyes intelligence network aim to strengthen the credibility of political statements by presenting a unified front. While not equivalent to legal attribution, such collective action increases diplomatic pressure and reinforces deterrence.[1222] Additionally, domestic indictments and sanctions regimes have become tools for attributing cyber operations to specific individuals or organisations, thereby creating consequences even in the absence of international enforcement.

[1222] NATO, *Wales Summit Declaration*, NATO *Press Release* (2014) 120 (Sept. 5, 2014); NATO, *Cyber Defence Pledge*, NATO *Press Release* (2016) 124 (July 8, 2016); Council of the Eur. Union, *Council Conclusions on a Framework for a Joint EU Diplomatic Response to Malicious Cyber Activities ("Cyber Diplomacy Toolbox")*, 9916/17 (June 19, 2017); Eur. Parl., *Resolution on Cyber Defence*, 2016/2052(INI) (Jan. 23, 2017).

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]

VOLUME 5 AND ISSUE 11 OF 2025

APIS – 3920 - 0001 *(and)* ISSN - 2583-2344

Published by

Institute of Legal Education

https://iledu.in

8. RECONCILING TECHNICAL FORENSICS WITH LEGAL STANDARDS OF ATTRIBUTION

8.1 Bridging The Gap Between Technical Forensics And Legal Standards

The challenges of attribution in cyber warfare reveal a fundamental tension between the realities of technology and the structures of international law. While cyberspace enables anonymity, plausible deniability, and the outsourcing of operations to non-state actors, international law continues to rely on doctrines developed in the context of conventional conflicts.[1223] Bridging this gap requires not only technical innovation but also legal and institutional reform.

A key step forward lies in strengthening cooperation between states on information sharing and technical forensics. Attribution cannot rest on the capabilities of a single state; rather, collaborative mechanisms involving intelligence agencies, private cybersecurity firms, and international organisations can help produce more credible and transparent attribution assessments. Multilateral platforms, including regional security organisations, should be encouraged to develop shared standards for cyber incident response and attribution, thereby reducing the risk of politically motivated or inconsistent declarations.

On the legal front, the adaptation of existing principles such as due diligence, effective control, and sovereignty to the cyber domain offers a pragmatic pathway. Expanding their interpretation would make it more difficult for states to exploit the grey zones of sponsorship and toleration of hostile cyber activities. At the same time, the codification of cyber-specific rules whether in the form of a new treaty or an additional protocol to existing conventions would provide clarity and uniformity, even if such efforts are initially limited to smaller coalitions of willing states.

8.2 Institutional Innovation And Building Resilience

Institutional innovation is also essential. The establishment of an impartial, internationally recognised body tasked with investigating major cyber incidents could help depoliticise attribution and provide a forum for accountability. Although such a mechanism faces obstacles of sovereignty and trust, precedents in nuclear governance, arms control, and humanitarian law show that similar institutions can emerge over time through incremental consensus-building.

Finally, building resilience against cyber operations must complement efforts at attribution. States should invest in strengthening critical infrastructure, developing deterrent strategies, and fostering norms of responsible behaviour in cyberspace.[1224] Attribution, while essential for accountability, will never be flawless therefore, resilience and deterrence must serve as parallel pillars of international security in the digital age.

9. CONCLUSION

The attribution problem lies at the heart of cyber warfare and its uneasy relationship with international law. Unlike conventional conflicts, where physical evidence, geographic borders, and visible command structures enable clearer accountability, cyberspace introduces layers of obfuscation, anonymity, and state-sponsored proxies that challenge traditional doctrines of responsibility. As a result, the principles of sovereignty, state responsibility, and the prohibition of force struggle to retain their coherence in the digital realm.

This difficulty is not merely technical but fundamentally legal and political. International law, rooted in the Westphalian system of state

[1223] Theresa Ntiting Mose, *Attribution and its Challenges and the Implications for State Responsibility Under International Cyber Security Law* (Feb. 28, 2025) (Working Paper), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=5087840.

[1224] Jason D. Jolley, *Attribution, State Responsibility, and the Duty to Prevent Malicious Cyber-Attacks in International Law* (Oct. 29, 2017) (Working Paper), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3056832.

accountability, presupposes identifiable actors and tangible acts. Cyber operations, however, thrive on ambiguity and deniability, enabling states to engage in hostile activities while avoiding legal consequences. The lack of universally accepted attribution mechanisms further exacerbates mistrust, incentivises escalation, and undermines the deterrent effect of international law.

Yet, the picture is not entirely one of paralysis. Emerging approaches including the reinterpretation of due diligence, the adoption of voluntary norms, coordinated public attributions, and proposals for specialised international mechanisms signal an ongoing evolution of legal and institutional responses. These efforts reflect a growing recognition that international law cannot remain static in the face of technological transformation. While imperfect, they provide building blocks for a more adaptive and resilient framework.

The challenge ahead is to transform these fragmented initiatives into a coherent structure that balances technical feasibility, legal clarity, and political legitimacy. Attribution in cyberspace may never achieve the precision of traditional conflicts, but it can be strengthened through cooperation, transparency, and norm-building. For international law, the task is not to eliminate uncertainty altogether but to develop standards that can operate within it, ensuring that accountability, deterrence, and stability remain viable in the digital age.

In this sense, the attribution problem is not only a test of legal doctrine but also of international resolve. How states address it will shape not just the future of cyber warfare but also the credibility of international law itself in an era defined by technological disruption.