Contemporary Readings in Law and Social Justice
ISSN: 1948-9137, e-ISSN: 2162-2752
Vol 17 (01), 2025
pp. 1143 – 1152

Legal Attribution of Cyberattacks: Evidence Standards and International Cooperation in the Kudankulam Case

[1] Houari Boumediene Bouziane, [2] Bakhta Bensaid*

[1] Faculty of Law and Political Science, University of Ibn Khaldoun, 14000, Tiaret, Algeria
houariboumediene.bouziane@univ-tiaret.dz

[2] Faculty of Law and Political Science, University of Djillali Liabes, 22000, Sidi Bel Abbes, Algeria
*bensaidebakhta@yahoo.fr

ABSTRACT: This research highlights the growing prevalence of cyberattacks on an international level, focusing on the limitations of "public attribution" (publicly naming and condemning the responsible entities) as a tool for deterrence and punishment. It underscores the need for legal attribution within the framework of international law to ensure compensation or legal redress. The study reviews the current standards and methods of proof in international law, specifying the nature and extent of evidence required to establish a state's responsibility for a cyberattack in an international judicial forum. It concludes that judicial forums are unlikely to relax proof standards to accommodate cyber challenges, but circumstantial evidence remains a viable option. This issue is examined contextually through the cyber incident at India's Kudankulam Nuclear Power Plant, with an in-depth analysis of its legal and technical implications. The research also addresses emerging cyber threats, the role of non-state actors, and mechanisms for international cooperation, offering recommendations for the development of international law.

Keywords: Cyberattack Attribution, International Law, Legal Accountability, Circumstantial Evidence, Kudankulam Incident, International Cooperation .

Received: 15 Aug 2025 **Received:** 28 Sep 2025 **Accepted:** 5 Oct 2025

1. Introduction

Amid the rapid digital transformation, cyberattacks represent an escalating global threat targeting critical infrastructure, governmental institutions, and private sectors, endangering national security, economic stability, and even public safety on an international scale. Joel Brenner likens cyberspace to a "massive masquerade party," where advanced technologies such as IP address spoofing, Onion Routing, and sophisticated encryption enable actors—whether states, non-governmental groups, or individuals—to carry out malicious attacks with relative impunity. These challenges are compounded by the difficulty of precisely identifying the source of attacks, which undermines the effectiveness of attribution (publicly naming responsible parties) and complicates the proof of legal accountability in international forums such as the International Court of Justice.

This research aims to explore the challenges of legal attribution of cyberattacks, focusing on standards of evidence in international law, the role of circumstantial evidence, and the urgent need to enhance international cooperation to confront rising cyber threats. The study uses the 2019 Kudankulam Nuclear Power Plant incident in India as a key case study to analyze the legal and technical implications of the attack and to draw lessons supporting the development of international legal frameworks. Within this analytical framework, the study seeks to achieve the following objectives:

- Evaluate the limitations of public attribution and justify the importance of legal forums in achieving

accountability and deterrence.

• Review standards of proof in international law and define evidentiary thresholds required for cyberattacks.

• Analyze the role of circumstantial evidence in proving responsibility for cyber violations, noting its technical and legal challenges.

• Contextually study the Kudankulam incident through an in-depth legal and technical analysis to extract lessons learned.

• Discuss emerging cyber threats, such as AI-supported attacks and targeting of the Internet of Things, and the role of non-state actors.

• Provide practical recommendations for developing international legal frameworks, including establishing cooperation mechanisms and unified standards of proof.

The research relies on International Court of Justice decisions, landmark precedents such as the Nicaragua v. United States case (1986) and the Bosnia Genocide case (2007), alongside the Tallinn Manual (1.0 and 2.0) as a reference framework for analyzing legal and technical challenges in cyberspace. It also considers the geopolitical context and the role of the private sector, such as cybersecurity companies' reports (Mandiant and CrowdStrike), in enhancing attribution. Through this comprehensive approach, the study aspires to offer an integrated vision that contributes to strengthening accountability, supporting international norms, and building a safer and fairer cyberspace that balances technological progress with legal responsibility in facing contemporary cyber threats.

2. Theoretical Overview of the Main Concepts

Public attribution is considered a central strategic tool in confronting cyberattacks, where states seek to publicly name the responsible entities to enhance deterrence, activate international pressure, and encourage cyber norms. However, the inherent limitations of this approach, such as limited international participation and lack of enforcement measures, reveal the urgent need for legal attribution through international forums to ensure accountability and achieve justice. This section addresses the concept of public attribution, its strategic benefits, technical tools, limitations, and the importance of transitioning to legal attribution as an effective alternative, enriching the discussion with practical examples and contemporary contexts.

2.1 The Concept of Public Attribution and Its Benefits

Public attribution is defined as the public declaration of the entities responsible for cyberattacks, whether states, non-governmental groups, or individuals, based on intelligence investigations, official statements, or reports from specialized security companies such as Mandiant, CrowdStrike, and FireEye. This approach aims to enhance transparency, expose violators, and support the development of international norms defining acceptable behavior in cyberspace.

Strategic Benefits of Public Attribution

Public attribution achieves several strategic benefits including:

• Exposing Violators: It reveals the involved parties, whether states or non-governmental groups, thereby strengthening international pressure and limiting their ability to escape punishment. For example, the US and its partners' accusation of Russia for the NotPetya attack in 2017 helped raise global awareness of cyber threats and prompted states to adopt preventive measures.

• Enhancing Cyber Defenses: Public attribution motivates targeted entities, such as government institutions and private companies, to improve their security systems to protect critical infrastructure. For instance, after the WannaCry attack in 2017, many countries increased their investments in cybersecurity.

• Raising Public and Institutional Awareness: It contributes to spreading awareness about the risks of cyberattacks, promoting a culture of cybersecurity at individual and institutional levels.

• Developing Cyber Norms: It helps establish "red lines" for acceptable behavior in cyberspace, supporting the creation of international legal and ethical frameworks. For example, public attribution in the SolarWinds attack in 2020 fostered discussions on the need for binding cyber norms.

• Diplomatic Pressure: It enables states to use public attribution as a diplomatic tool to impose economic or political sanctions, as happened when the US imposed sanctions on Russian entities involved in cyberattacks.

Tools Used in Public Attribution

Public attribution relies on a range of technical and intelligence tools to identify the source of cyberattacks, including:

• Digital Data Analysis: This includes examining IP addresses, malware signatures, and activity patterns. For example, FireEye used malware analysis to link the 2020 SolarWinds attack to Russia based on unique software signatures.

• Intelligence Reports: States depend on intelligence from agencies such as the NSA or GCHQ to support their accusations.

• Diplomatic Alliances: Alliances like the Five Eyes enhance the credibility of public attribution through information sharing. For example, several countries supported the accusation against China for the 2021 Microsoft Exchange Server attacks, which increased the impact of the attribution.

• Temporal and Contextual Analysis: Identifying attack patterns, such as working hours or languages used in code, helps associate attacks with specific actors. For example, investigations linked the WannaCry attack to North Korea based on similarities to previous Lazarus Group attacks.

2.2 Limitations of Public Attribution and the Need for a Legal Alternative

Despite its benefits, the intrinsic limitations of public attribution reduce its effectiveness, necessitating the search for legal alternatives that ensure more effective and legitimate accountability.

Main Limitations of Public Attribution

• **Limited International Participation:** Public attribution is often restricted to Western countries or specific alliances, reducing its global impact. For instance, accusations against China for the 2021 Microsoft Exchange Server attacks were largely confined to the US and the EU, diminishing overall global pressure due to lack of broader international involvement.

• **Absence of Tangible Sanctions:** Public attribution lacks effective enforcement measures, such as legal sanctions or compensation, weakening its deterrent capability. For example, accusing Russia of the NotPetya attack had no significant legal consequences, which reduced deterrence.

• **Challenges of Trust and Legitimacy**: Public accusations frequently face denials from the accused states, raising questions about their credibility. For instance, Russia described the 2018 allegations of attempting to hack the Organisation for the Prohibition of Chemical Weapons as a "Western spying hysteria," obstructing international consensus.

• **Technical Challenges:** Obfuscation techniques, such as spoofing and encryption, complicate public attribution, as actors can manipulate data to mislead investigations.

• **Politicization**: Public accusations can be used as political tools, which diminishes their neutrality and sparks controversies about their motives.

The Importance of Legal Attribution

Legal attribution through international forums, such as the International Court of Justice, is a more effective

and legitimate alternative to overcome the limitations of public attribution. Its advantages include:

• **Concrete Compensation:** It allows issuing judicial orders or financial reparations to affected states, strengthening corrective justice. For example, affected states could claim compensation for damages caused by cyberattacks that disrupt critical infrastructure.

• **Legal Legitimacy:** It relies on rigorous audits and clear evidence standards, enhancing transparency and international trust in accusations.

• **Effective Deterrence:** It imposes binding legal consequences, such as sanctions or court orders, which promote adherence to international law.

• **Supporting International Norms:** Legal attribution helps develop binding rules of conduct in cyberspace, fostering global stability.

The UN Group of Governmental Experts report (2015) emphasizes the necessity of supporting accusations with substantive evidence, highlighting the importance of legal forums for accountability. Furthermore, the Tallinn Manual 2.0 points out that legal attribution can strengthen states' capacity to respond to cyberattacks by providing a clear legal framework for assigning responsibility.

3. Standards of Proof and Circumstantial Evidence in International Law

Holding states accountable for cyberattacks requires meeting strict standards of proof within the framework of international law, given the complexities of cyberspace and advanced concealment technologies. This section focuses on reviewing the standards of proof applied in international judicial forums, evaluating the role of circumstantial evidence as a critical tool in proving responsibility, and analyzing the legal and technical challenges associated with establishing liability in the context of cyberattacks. The discussion is enriched by referencing recent judicial precedents, practical applications, and the framework provided by the Tallinn Manual to enhance understanding of these challenges.

3.1 Standards of Proof in International Law

Standards of proof vary between domestic and international laws, with international judicial forums evaluating each case based on its nature and severity. This subsection aims to analyze these standards, focusing on their application in the context of cyberattacks and highlighting the associated challenges.

International Judicial Standards

In domestic criminal law, responsibility must be proven "beyond reasonable doubt," while civil cases require a "preponderance of the evidence." As for international litigation, the International Court of Justice (ICJ) refrains from adopting a fixed standard, preferring flexibility to suit the nature of each case. Notable precedents include:

• **Bosnia Genocide Case (2007):** The court required "fully conclusive evidence" to prove serious violations, given the gravity of the accusations.
• **Nicaragua v. United States (1986):** The court asked for "convincing evidence" to establish facts, focusing on evidence quality and context.
• **Democratic Republic of Congo v. Uganda (2005):** The court adopted a standard of "sufficient and convincing evidence," considering circumstantial evidence when necessary.
• **Iran v. United States (Oil Platforms, 2003):** The court emphasized the necessity of strong and coherent evidence to prove responsibility for hostile acts.

These precedents show that international courts tend to demand high levels of proof in politically or security-sensitive cases, complicating their application to cyberattacks.

Application of Standards to Cyberattacks

Proving responsibility in cyberattacks is complicated by concealment technologies such as identity spoofing, encryption, and Onion Routing. Tallinn Manual 1.0 notes that attacks originating from government infrastructure may indicate state involvement but are insufficient alone to prove responsibility without additional evidence directly or indirectly linking the state to the attack. For example:

• Attacks considered "use of force" under Article 2(4) of the UN Charter, such as disrupting critical infrastructure, require high standards of proof demonstrating intent and control.
• Less severe activities, such as cyber espionage or data theft, may allow for lower standards of proof, such as circumstantial evidence, provided it is consistent and supported.

For instance, in the Stuxnet attack (2010) on Iran's Natanz nuclear facilities, technical evidence—like the malware's complexity and specific targeting—pointed to a technologically advanced state actor, but the lack of direct evidence prevented official attribution. Furthermore, Tallinn Manual 2.0 states that states may be held responsible for attacks if it is proven they supported or directed non-state actors, broadening the scope of proof to include indirect relationships.

3.2 The Role of Circumstantial Evidence in Proving Responsibility

Circumstantial evidence is a crucial tool in proving cyber responsibility, given the difficulty of obtaining direct evidence in cyberspace. This subsection discusses the nature of circumstantial evidence, its types, practical applications, and associated challenges, enriched with contemporary examples.

Nature of Circumstantial Evidence

Evidence is divided into direct (which proves a conclusion directly, such as recordings or documents) and circumstantial (which leads to reasonable inferences through a chain of facts). In cyberspace, circumstantial evidence is more common due to concealment techniques. Examples of circumstantial evidence include:

• **Malware Signatures:** Identifying unique code patterns associated with particular actors. For example, investigations linked the WannaCry attack (2017) to North Korea based on malware signatures similar to Lazarus Group attacks.

• **Activity Patterns:** Such as working hours, languages used in code, or attack styles. For example, investigations linked the SolarWinds attack (2020) to Russia based on operational patterns consistent with groups like Cozy Bear.

• **IP Addresses and Domain Names:** May indicate infrastructure tied to a state or group, though these can be forged.

• **Geopolitical Context:** Such as political or economic motives. For example, the Microsoft Exchange Server attack (2021) was linked to China due to targeting of strategic sectors aligned with its economic interests.

• **Network Logs and Metadata:** Provide information about attack origins or data paths, as seen in analyses of Advanced Persistent Threat (APT) attacks.

Tallinn Manual 2.0 confirms that circumstantial evidence can be sufficient if it is consistent and interconnected, especially in contexts of exclusive control where the accused state governs the relevant data.

Challenges of Circumstantial Evidence

Circumstantial evidence faces significant challenges in cyberspace, including:

• **Identity Spoofing:** Actors can forge IP addresses or malware signatures to mislead investigations. For example, unknown parties used spoofing in the NotPetya attack (2017) to blame uninvolved entities.

• **Encryption**: Hinders communication analysis or extraction of direct data, making circumstantial evidence the primary option.

• **Exclusive Control**: The accused state often controls key data, limiting access to direct evidence. For example, in the 2018 attack on the Organisation for the Prohibition of Chemical Weapons, Russia refused to provide data to refute accusations.

• **Technical Complexity:** Analyzing evidence requires advanced technical expertise, challenging for developing countries with limited resources.

• **Risks of False Accusations:** Studies such as Rossini (2020) warn against lowering standards of proof to adapt to cyber challenges, as this may lead to unjust accusations or escalation of international tensions.

Ways to Overcome Challenges:

• **Enhancing International Cooperation**: Establishing protocols for evidence exchange between states, such as the Budapest Convention on Cybercrime, can improve evidence quality.

• **Using Advanced Technology:** Applying artificial intelligence and big data analytics to improve the accuracy of circumstantial evidence analysis.

• **Developing Unified Standards:** Tallinn Manual 2.0 calls for a unified framework to assess circumstantial evidence in cyber cases, enhancing transparency and trust.

• **Involving the Private Sector:** Cooperation between states and companies like Microsoft and CrowdStrike leverages their expertise in analyzing cyberattacks. For example, Microsoft provided critical reports analyzing the Microsoft Exchange Server attack.

4. Case Study of the Kudankulam Incident

The Kudankulam nuclear incident in India in 2019 stands as a prominent example of the challenges involved in legal attribution of cyberattacks. A sophisticated cyberattack targeted a vital nuclear power plant, raising global concerns about the security of critical infrastructure. This section addresses the background of the incident, its technical and legal analysis, and the lessons learned, while enriching the discussion with additional details about the geopolitical context, judicial challenges, and the incident's impact on international norms. It also presents a hypothetical analysis of a case before the International Court of Justice, focusing on the role of circumstantial evidence and accountability mechanisms.

4.1 Background of the Incident and Technical Analysis

The cyberattack targeted the Kudankulam Nuclear Power Plant in Tamil Nadu, India, a strategic nuclear energy facility, raising questions about the security of critical infrastructure and the potential escalation of cyber threats to catastrophic levels. This subsection reviews details of the incident and analyzes technical aspects that revealed the nature of the attack and its likely source.

Incident Details

Investigations conducted by Indian authorities and cybersecurity companies revealed the following:

• **Nature of the Attack:** The attack targeted the plant's administrative control system through malware of the "Dtrack" type, an advanced spyware tool used to steal data and monitor systems. The attack did not affect critical operational systems but exposed serious security vulnerabilities.

• **Technical Evidence:** Investigations uncovered MAC signatures and IP addresses linked to infrastructure in North Korea, along with Korean language used in the malware's code.

• **Malware Signatures:** The code matched tools previously attributed to the Lazarus Group, a cyber hacking group linked to North Korea, which carried out attacks such as WannaCry (2017) and the Bangladesh Bank heist (2016).

• **Geopolitical Context**: The attack coincided with diplomatic tensions between India and other countries, leading to speculation about political or strategic motives, such as disrupting India's nuclear program or gathering intelligence.

• **Initial Response:** Indian authorities confirmed that the attack caused no physical damage but subsequently enhanced cybersecurity measures at nuclear facilities.

Legal Analysis

To establish North Korea's responsibility before the International Court of Justice, India must meet strict standards of proof, including:

• **Refuting Identity Spoofing:** Proving that the IP addresses and MAC signatures were not forged, a major challenge due to the possibility of technical manipulation. For example, other actors could imitate Lazarus Group signatures to mislead investigations.

• **Proving Exclusivity:** Linking the "Dtrack" malware exclusively to the North Korean government, requiring evidence of control or direction by the state. Tallinn Manual 2.0 notes that effective control over non-state groups like Lazarus is essential to hold the state accountable.

• **Connecting the Attack to State Interests:** Demonstrating the attack served strategic goals, such as disrupting India's nuclear program or intelligence gathering, thereby strengthening the claim of sovereignty violation.

• **Circumstantial Evidence:** India can rely on activity patterns, such as code matching previous attacks and geopolitical context, to support its accusations. For example, intelligence reports indicated North Korea targeted nuclear programs in other countries to bolster its own.

The incident highlights the challenges of legal attribution amid the absence of direct evidence, making circumstantial evidence the most viable option.

4.2 Hypothetical International Litigation

This subsection presents a hypothetical scenario where India brings a case against North Korea before the International Court of Justice, analyzing judicial challenges and potential outcomes, and enriching the discussion with a legal framework and similar examples.

Details of the Hypothetical Case

• **Legal Claim:** India accuses North Korea of violating its sovereignty under international law, relying on Article 2(4) of the UN Charter, which prohibits intervention in the internal affairs of states. The attack on a nuclear facility qualifies as a sovereignty violation due to targeting critical infrastructure.

• **Presented Evidence:** Includes analysis of the "Dtrack" malware, intelligence reports from international

agencies, expert testimony from companies like FireEye, and network metadata showing the attack source. The case may also draw on patterns from previous attacks attributed to the Lazarus Group.

• **Judicial Challenges:**
  o **Refuting identity spoofing:** India must prove that the technical evidence was not fabricated, complicated by advanced spoofing techniques.
  o **Proving intent:** Linking the attack to North Korean interests, such as disruption of India's nuclear program, requires strong contextual evidence.
  o **Lack of cooperation:** North Korea may refuse to cooperate with the court, complicating the access to direct evidence.
• **Potential Outcome:** The court may accept circumstantial evidence if it is consistent and meets the "beyond reasonable doubt" standard, as in the Nicaragua v. United States case (1986), where the court relied on circumstantial evidence to establish responsibility. However, limited direct evidence may impede a final judgment.

Lessons Learned and Impact on International Norms

The Kudankulam incident offers crucial lessons for developing international legal frameworks:
• **Importance of Circumstantial Evidence:** The incident shows that circumstantial evidence such as malware signatures and activity patterns can sufficiently support accusations if presented consistently and backed by detailed technical analysis.
• **Need for Unified Standards of Proof:** The incident reveals the lack of international unified standards for evaluating cyber evidence, highlighting the need to develop a common legal framework, as suggested by Tallinn Manual 2.0.
• **Enhancing Cybersecurity:** The incident prompted India to strengthen cybersecurity measures at its nuclear facilities, underscoring the importance of investing in cyber defenses for critical infrastructure.
• **International Cooperation:** The incident emphasized the necessity of information sharing among states and private sector companies to improve attribution and response to attacks. Companies like Kaspersky provided crucial reports that helped analyze the incident.
• **Impact on International Norms:** The incident contributed to advancing discussions on prohibiting attacks on critical infrastructure, as recommended by the United Nations Group of Governmental Experts (2021), which called for binding rules of conduct in cyberspace.

5. Emerging Threats and International Cooperation

With rapid technological advances, emerging cyber threats are increasing, such as AI-powered attacks and targeting of the Internet of Things (IoT), posing risks to critical infrastructure and national security on a global scale. These challenges are exacerbated by the involvement of non-state actors, such as terrorist groups and cybercriminals, complicating attribution of responsibility. This section addresses emerging cyber threats, the role of non-state actors, and mechanisms of international cooperation, enriching the discussion with analysis of recent technological developments, international legal frameworks, and practical recommendations to enhance accountability and deterrence in cyberspace.

5.1 Emerging Cyber Threats and Their Challenges

Emerging cyber threats pose growing challenges due to technological evolution and diversity of actors. This subsection reviews the major types of threats, analyzes their impact on global security, and discusses associated challenges.

Types of Emerging Threats

Emerging cyber threats include a range of advanced technologies and methods:
• **Artificial Intelligence (AI):** AI is used to design automated attacks, such as self-adaptive malware and deepfake attacks that deceive security systems or spread disinformation. For example, 2023 saw an increase in deepfake usage to impersonate officials in sophisticated phishing attacks.
• **Internet of Things (IoT):** The proliferation of connected devices, such as industrial control systems and smart home devices, increases cybersecurity risks. For instance, the Mirai Botnet attack (2016), which exploited IoT networks, exposed vulnerabilities in these systems.
• **Cloud Computing:** Cloud systems are attractive targets because they store massive amounts of sensitive data. A 2020 attack on AWS services demonstrated how attackers can exploit vulnerabilities in cloud infrastructures.
• **Supply Chain Attacks:** These attacks target third parties, such as software providers, to infiltrate larger

systems. The SolarWinds attack (2020) is a notable example, where software updates were compromised to target governmental and private institutions.
• **Fileless Malware:** This type exploits memory rather than files, making detection more difficult. Such attacks were used in advanced breaches against banks in 2022.

Role of Non-State Actors

Non-state actors—including terrorist groups, cybercriminals, and state-sponsored hacking groups—complicate attribution:
• **Terrorist Groups:** Groups like ISIS use cyberspace to spread propaganda, recruit members, and conduct simple attacks like Distributed Denial of Service (DDoS). For example, in 2021, terrorist groups claimed cyberattacks against government websites in the Middle East.
• **Cybercriminals:** Ransomware gangs like Conti and REvil pose rising threats, targeting critical institutions such as hospitals. The Colonial Pipeline attack (2021) disrupted fuel supplies in the United States, revealing the significant impact of these actors.
• **State-Sponsored Groups:** Groups like Lazarus (North Korea) and Sandworm (Russia) act as proxies for states, complicating legal accountability. Tallinn Manual 2.0 indicates states may be held responsible for actions by such groups if effective control or direct support is proven.
These actors increase attribution complexity due to lack of direct governmental control, requiring flexible legal frameworks for response.

5.2 Mechanisms of International Cooperation

Addressing emerging cyber threats demands effective international cooperation involving information exchange, norm development, and capacity building. This subsection discusses existing international cooperation frameworks, their challenges, and recommendations to strengthen global response.

Current Framework for International Cooperation

Current global efforts include:
• **United Nations Group of Governmental Experts (UNGGE):** Reports (2015, 2021) that call for developing cyber norms such as banning attacks on critical infrastructure and enhancing inter-state information sharing.
• **Budapest Convention (2001):** The first international treaty against cybercrime, focusing on harmonizing legislation and facilitating cross-border investigations. More than 60 countries had joined by 2025.
• **Bilateral and Regional Agreements:** Such as information-sharing agreements within the European Union or the Five Eyes alliance, which bolster cooperation in cyber intelligence.
• **International Organizations:** Entities like Interpol and the International Telecommunication Union (ITU) coordinate efforts and provide technical support to developing countries. For example, Interpol launched a program in 2023 to train African states in fighting cybercrime.
• **Private Sector Cooperation:** Companies like Microsoft and Kaspersky contribute to analyzing attacks and providing intelligence reports. For instance, Microsoft supplied decisive data in investigating the Microsoft Exchange Server attack (2021).

Challenges and Recommendations

Cooperation efforts face significant challenges, with practical solutions suggested:

• Challenges:
o **Differences in Legal Jurisdictions:** Cyber laws vary between countries, hindering cross-border investigations. For example, some countries refuse to extradite cybercriminals due to lack of extradition treaties.
o **Lack of Trust Between States: Political** tensions cause reluctance to share sensitive information. For instance, US-China tensions impeded cooperation in cyberattack investigations.
o **Absence of Binding Enforcement Mechanisms:** There is no international court specialized in cybercrime, limiting accountability effectiveness.
o **Capacity Gaps in Developing Countries:** Lack of technical and human resources makes developing states easy targets for attacks.

• Recommendations:

o **Establish a Specialized International Court:** Create an international cybercrime court to serve as a

neutral forum for dispute resolution and binding judgments, modeled after the International Criminal Court.

o **Develop Protocols for Evidence Exchange**: Set unified standards for sharing cyber evidence inspired by the Budapest Convention to ensure transparency and speed up investigations.

o **Support Developing Countries:** Provide training and funding programs through UN and ITU to strengthen cybersecurity capabilities in resource-limited states.

o **Enhance Private Sector Collaboration:** Encourage partnerships between governments and tech companies to develop advanced detection tools and attack analysis. For example, companies like CrowdStrike could provide real-time analyses to support international investigations.

o **Establish Binding Norms:** Develop an international treaty banning attacks on critical infrastructure such as hospitals and nuclear plants, with clear enforcement mechanisms, as proposed by the UN Open-ended Working Group (OEWG) in 2023.

6. Synopsis of the Main Research Outcomes

The research yields several key findings:

• **Limitations of Public Attribution: Public** attribution, while useful for raising awareness and diplomatic pressure, lacks enforceable sanctions and global participation, limiting its deterrent effect.

• **Importance of Legal Attribution:** Legal attribution through international forums offers legitimacy, compensation, and deterrence, supported by rigorous evidence standards.

• **Role of Circumstantial Evidence:** Circumstantial evidence, such as malware signatures and activity patterns, is a viable tool for proving cyber responsibility, though it faces challenges like spoofing and encryption.

• **Kudankulam Case Insights:** The 2019 Kudankulam incident underscores the feasibility of circumstantial evidence in legal attribution but highlights the need for unified standards and international cooperation.

• **Emerging Threats:** AI, IoT, and supply chain attacks pose increasing risks, requiring adaptive legal frameworks and enhanced cooperation.

• **International Cooperation:** Mechanisms like the Budapest Convention and private sector partnerships are critical for improving attribution and response capabilities.

7. Conclusions

The challenges of legal attribution for cyberattacks highlight the urgent need to develop international legal frameworks to ensure accountability and deterrence in cyberspace. The limitations of public attribution, which relies on public naming without tangible enforcement measures, make the "good enough" standard insufficient in international judicial forums that require strong and consistent evidence. The 2019 Kudankulam nuclear incident in India demonstrates the importance of circumstantial evidence as an effective tool for proving responsibility in contexts of exclusive control, but it also exposes gaps in current legal standards, including the absence of a unified framework for evaluating cyber evidence.

With the rise of emerging cyber threats—such as AI-powered attacks, supply chain attacks, and targeting of the Internet of Things—the need for effective international cooperation grows, including information sharing, development of binding norms, and capacity building in developing countries. The establishment of a specialized international cybercrime court and unified protocols for evidence exchange, alongside strengthened public-private partnerships, are essential steps toward accountability.

8. Limitations, Implications, and Further Directions of Research

Limitations: The research is constrained by the limited availability of direct evidence in cyberattack cases, relying heavily on circumstantial evidence and open-source intelligence. The Kudankulam case analysis is based on publicly available reports, which may lack comprehensive technical details. Additionally, the evolving nature of cyber threats limits the generalizability of findings.

Implications: The study underscores the need for robust international legal frameworks to address cyberattack attribution. It highlights the potential of circumstantial evidence and private sector collaboration in enhancing accountability. The findings support the development of international norms to protect critical infrastructure, as recommended by the UNGGE (2021).

Further Directions: Future research should focus on developing unified standards for cyber evidence evaluation, exploring AI-driven attribution techniques, and assessing the feasibility of a specialized cybercrime court. Comparative studies on regional cooperation mechanisms and their impact on attribution could further inform global strategies.

References

[1] Tameem Hadi Fadhil, Mustafa I. Al-Karkhi, and Luttfi A. Al-Haddad, “Legal and Communication Challenges in Smart Grid Cybersecurity: Classification of Network Resilience Under Cyber Attacks Using Machine Learning," Journal of Communications, vol. 20, no. 2, pp. 221-228, 2025.

[2] Henrico, S., & Els, S. (2025). Cyber Attacks in South Africa: Geopolitical and legal implications. African Security Review, 1–25. https://doi.org/10.1080/10246029.2025.2489352

[3] Saraswat, A., Tiwari, G. (2025). United Nations and Beyond: Legal Strategies for Defending Critical Energy Infrastructure Against Cyber Attacks. In: Chawki, M., Abraham, A. (eds) Cybercrime Unveiled: Technologies for Analysing Legal Complexity. Studies in Computational Intelligence, vol 1181. Springer, Cham. https://doi.org/10.1007/978-3-031-80557-8_13

[4] Hasrina, S., Sari, I., Manguma, T. T. F., & Fatra, E. (2025). Analisis Hukum Pidana Atas Keamanan Data Dan Serangan Siber Terhadap Pertahanan Nasional: Criminal Law Analysis of Data Security and Cyber Attacks on National Defense. KIRANA: Social Science Journal, 2(1), 1–5. https://doi.org/10.61579/kirana.v2i1.227

[5] Mohammed Jabbar Jadoua Al-Abdeli, Ahmed Sabbar Abdulameer. (2025). The Cyber warfare according to the rules of international law. Tikrit University Journal for Rights, 9(4), 147-179. https://tujr.tu.edu.iq/index.php/tujr/article/view/81

[6] Ramadan Abdullah Al-Amouri. (2024). Cyber Wars (Reality – Challenges) In light of international humanitarian law (I.H.L.). Al-Haq Journal for Sharia and Legal Sciences, 196-210. https://doi.org/10.58916/alhaq.vi.246

[7] Leventopoulos, S., Pipyros, K. & Gritzalis, D. (2024). Retaliating against cyber-attacks: a decision-taking framework for policy-makers and enforcers of international and cybersecurity law. Int. Cybersecur. Law Rev., 5, 237–262. https://doi.org/10.1365/s43439-024-00113-5

[8] Bace, B., Gökce, Y., & Tatar, U. (2024). Law in orbit: International legal perspectives on cyberattacks targeting space systems. Telecommunications Policy, 48(4), 102739. https://doi.org/10.1016/j.telpol.2024.102739

[9] Sarkar, G., & Shukla, S. K. (2024). Reconceptualizing online offenses: A framework for distinguishing cybercrime, cyberattacks, and cyberterrorism in the Indian legal context. Journal of Economic Criminology, 4, 100063. https://doi.org/10.1016/j.jeconc.2024.100063

[10] Katagiri, N. (2023). Defending medical facilities from cyber attacks: critical issues with the principle of due diligence in international law. International Review of Law, Computers & Technology, 38(1), 1–20. https://doi.org/10.1080/13600869.2023.2183449