VIDWAN Journal of Law and Justice

OPEN ACCESS

PEER-REVIEWED - OPEN ACCESS Vol. 01 · Issue 01 · 2026 · pp. 25-29 | ISSN: APPLIED (Online) | INAGURAL EDITION

NON STATE ACTOR CYBERATTACKS AND THE COMPLEXITY OF STATE ATTRIBUTION UNDER INTERNATIONAL LAW

R.Ranjith Kumar, *Associate Professor*,
Vinayaka Law College, Siddipet

ABSTRACT

This research investigates the difficulties associated with ascertaining which governments are accountable for cyberattacks in accordance with international law, as well as the increasing danger posed by cyberattacks perpetrated by non-state groups. This paper investigates the ways in which the decentralized, anonymous, and global nature of cyberspace threatens the well-established legal principles that regulate the culpability of states. This is particularly relevant in cases where criminal networks, hacktivist groups, terrorist organizations, or private individuals are conducting operations on the internet, regardless of whether the state is involved. The paper examines the legal standards of attribution outlined in the Papers on State Responsibility for Internationally Wrongful Acts (ARSIWA), as well as relevant international law and developing state practice, in order to emphasize the evidentiary and technical challenges associated with establishing an adequate connection between non-state actors and states. It is also feasible to assess the effectiveness of current international legal frameworks, including the United Nations Charter and laws that regulate the use of force, in relation to cyber operations that do not qualify as armed conflict. As a means of ensuring effective legal accountability and contributing to the maintenance of international peace and security, this paper advocates for the gradual establishment of international cyber norms, stronger evidentiary standards, and improved international cooperation. It accomplishes this by emphasizing deficiencies in accountability frameworks and attribution mechanisms.

Keywords: *Cyberattacks; Non-State Actors; State Attribution; International Law; State Responsibility; Cybersecurity; Attribution Doctrine; ARSIWA; Cyber Warfare; Tallinn Manual.*

Article history: Received 11 July 2026 · Revised 21 July 2026 · Accepted 27 July 2026 · Published 5 August 2026

I. INTRODUCTION

The internet's rapid expansion has introduced novel security risks and revolutionized governance, commerce, and communication. Individual hackers, hacktivist collectives, terrorist organizations, and cybercriminals are perpetrating increasingly intricate cyberattacks. The international community and governments are apprehensive about cyberthreats that operate anonymously across borders.

International law, particularly state accountability, is complicated by non-state actors. In order to be held accountable, a state must either lead, support, or regulate non-state actors. Cyber attacks are challenging to identify due to their anonymity and global reach.

State liability attribution in international cyber law is challenging due to the constantly evolving character of cyber threats. The new challenges presented by non-state actor cyberattacks are beyond the capacity of the legal system to address. This paper investigates these challenges and evaluates the capacity of international law to address cyber attribution and accountability.

II. AVAILABLE LEGAL FRAMEWORK FOR ATTRIBUTION

Paper 8 of the Papers on Responsibility of States for Internationally Wrongful Acts (ARSIWA)

States are held accountable for the actions of private individuals or non-state actors under their control under Paper 8 of the ARSIWA. In order to hold the state accountable for the actions of private entities, it is necessary

to establish a distinct factual relationship between the state and the private firm. The declaration contends that the state should limit certain forms of misconduct, rather than emphasizing political influence. Numerous individuals contend that Paper 8, which permits flexibility through case-by-case analysis, necessitates direct state oversight of operations.

Nicaragua Effective Control Test

In 1986, the Effective Control Test for Military and Paramilitary Activities was established by the International Court of Justice. The efficacy of Nicaragua's military and paramilitary was evaluated in this examination. A state cannot be held globally accountable for the activities of non-state actors solely because it provides financial, logistical, or training support, according to the Supreme Court. In order to establish culpability, it is necessary to provide evidence that the government regulated the activities of each organization. The verdict has been subject to criticism, particularly in cases involving concealed activity, as a result of the high and challenging proof burden.

Tadić Overall Control Test

In the Tadić case, the ICTY implemented the Overall Control Test. In contrast to the Effective Authority Test, this method necessitates sovereign jurisdiction over an organized armed force. In contrast to the Effective Authority Test. Aid, funding, supplies, training, or direction may be necessary to manage a group's military operations. Despite the Tribunal's determination that organized groupings are more pertinent to the distinction between effective control and overall control, it remains a topic of debate.

III. APPLICATION TO CYBERSPACE

Applicability of International Humanitarian Law

International humanitarian law should govern cyber operations, according to the document. This perspective is substantiated by the subsequent points:

- (2013) Tallinn Handbook Manual
- Tallinn's Manual 2.0, 2017
- The War Crimes Protocols
- Claus Martens' name
- The structure of the United Nations Appellate Body
- The Right to International Freedom for All
- UN Intergovernmental Experts on Governance Panel

According to these sources, cyberspace is subject to laws that regulate armed conflict. sovereignty and non-intervention are regulated by these laws.

B. Problems of Attribution in Cyberspace

The following are the reasons why traditional cyber activity attribution standards are challenging:

- The perpetrators maintain their anonymity.
- Cyberspace is subject to numerous legal frameworks.
- Manipulation is feasible with digital substantiation.
- Demonstrating state control over cybercriminals is a challenging task.

Three steps are typically included in an attribution procedure:

- determining the type of weapon system.
- Locate the perpetrator.
- The relationship between the government and the populace.

Research indicates that the Effective Control Test is inaccurate and that the Overall Control Test is superior for cyber attribution.

IV. CASE STUDIES ON CYBERATTACKS BY NON-STATE ACTORS

Estonia v. Russia (2007)

Following the relocation of the Bronze Soldier monument in Estonia, hackers launched attacks on government websites, financial systems, media outlets, and ISPs. Russian interference was suggested by IP addresses, technological evidence, and the pro-Kremlin Nashi Youth Group. The Effective Control Test was unable to establish attribution due to a lack of direct operational control, despite the fact that the Overall Control Test more accurately depicted the financial and organizational relationship between Russia and the perpetrators.

Georgia–Russia War (2008)

Cyberattacks transpired amid the conflict between Russia and Georgia. The websites of the Georgia government, banks, and citizens were all unavailable. The attribution of the assaults to Russian networks and the Russian Business Network (RBN) remains uncertain, as neither the Effective Control Test nor the Overall Control Test produced any results, despite the evidence linking them.

Iran v. Albania (2022)

Hackers affiliated with Iran gained access to Albanian government servers and implemented ransomware to erase all data. Iranian state-sponsored enterprises affiliated with the Iranian Ministry of Intelligence were responsible for the attacks, as per investigations conducted by the United States, the United Kingdom, NATO, the NIAS, and Microsoft. Albania's separation from Iran was a significant cyber event in the 20th century.

V. POSSIBLE REFORMS

This report suggests four significant changes to international law regarding cyber attribution.

Reform Existing Attribution Standards

The current attribution criteria are excessively stringent due to their origins in conventional warfare. In order to more accurately represent cyberspace, the author recommends a control test that is both realistic and adaptable.

Establish an International Cyber Attribution Agency

An international institution that is impartial should conduct an investigation into cyber incidents, assess technical evidence, and produce conclusions to ascertain the responsibility of the state.

Apply the Principle of Due Diligence

States that intentionally permit cyber entities operating within their borders to conduct attacks against other nations should be subject to repercussions. Discover the potential benefits of data, prevention methods, and cyber operations.

Adopt a Multi-Factor Attribution Test

For attribution to be valid, it must encompass numerous variables, such as the following, rather than a single legal criterion:

- data from scientific research,
- Internet Protocol addresses, or IP addresses, are
- Malware characteristics include:
- Initially introduced,
- geographic origins of the region,
- Differing ideologies motivate
- This encompasses the capability of attackers, circumstantial evidence, and the interests of states.

The author also suggests that the Control and Capabilities Test be employed to combine these qualities in order to achieve a more authentic attribution technique.

VI. CONCLUSION

The paper asserts that international law does not permit the imposition of liability on non-state actors for cyberattacks. The traditional attribution standards, which were developed for land-based battles, are inadequate for the complexity of cyberspace.

The author proposes that political attribution should incorporate technical, behavioral, and circumstantial factors in addition to direct evidence. Cyber operations cannot be effectively managed by a universal legal framework. This paper suggests the establishment of a cyber attribution authority that ensures international cyber law responsibility, justice, and uniformity by integrating legal analysis with technical expertise.

REFERENCES

[1] Michael N Schmitt, 'Below the Threshold Cyber Operations: The Countermeasures Response Option and International Law' (2014) 54(3) Virginia Journal of International Law 697.

[2] Russell Buchan, 'Cyber Attacks: Unlawful Uses of Force or Prohibited Interventions?' (2012) 17(2) Journal of Conflict and Security Law 211.

[3] Nicholas Tsagourias, 'Cyber Attacks, Self-Defence and the Problem of Attribution' (2012) 17(2) Journal of Conflict and Security Law 229.

[4] Oona A Hathaway, Rebecca Crootof, Philip Levitz, Haley Nix, Aileen Nowlan, William Perdue and Julia Spiegel, 'The Law of Cyber-Attack' (2012) 100(4) California Law Review 817.

[5] Joanna Kulesza, 'State Responsibility for Cyber Attacks by Non-State Actors' (2010) 1(2) International Journal of Public Law and Policy 139.

[6] Herbert S Lin, 'Attribution of Malicious Cyber Incidents: From Soup to Nuts' (2016) 70(1) Journal of International Affairs 75.

[7] Duncan B Hollis, 'Why States Need an International Law for Information Operations' (2017) 11 Lewis & Clark Law Review.

[8] Duncan B Hollis, 'An e-SOS for Cyberspace' (2011) 52(2) Harvard International Law Journal 373.

[9] Michael N Schmitt, 'Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework' (1999) 37 Columbia Journal of Transnational Law 885.

[10] Michael N Schmitt, 'Cyber Operations and the Jus ad Bellum Revisited' (2011) 56 Villanova Law Review 569.

[11] Sean Watts, 'Low-Intensity Cyber Operations and the Principle of Non-Intervention' (2015) 93 International Law Studies 141.

[12] Kristen E Eichensehr, 'The Law and Politics of Cyberattack Attribution' (2020) 67(3) UCLA Law Review 520.

[13] Kristen E Eichensehr, 'Cyberwar and International Law Step Zero' (2015) 50(2) Texas International Law Journal 355.

[14] Gary D Brown and Keira Poellet, 'The Customary International Law of Cyberspace' (2012) Strategic Studies Quarterly 126.

[15] Michael Schmitt and Liis Vihul, 'The Nature of International Law Cyber Norms' (2017) NATO CCDCOE International Conference on Cyber Conflict Proceedings.

