Page: 768-782 *URL: www.lijdlr.com*

LAWFOYER INTERNATIONAL JOURNAL OF DOCTRINAL LEGAL RESEARCH

ISSN: 2583-7753

LawFoyer International Journal of Doctrinal Legal Research

[ISSN: 2583-7753]

Volume 4 | Issue 1

2026

DOI: https://doi.org/10.70183/lijdlr.2026.v04.33

BEYOND TRADITIONAL ATTRIBUTION: RETHINKING STATE RESPONSIBILITY UNDER ARSIWA IN LIGHT OF THE SOLARWINDS CYBERATTACK

Aakriti Khattry[1]

I. ABSTRACT

This paper brings to light the evidentiary and normative gaps in cyberspace for the attribution of State responsibility under the Articles on Responsibility of States for Internationally Wrongful Acts (ARSIWA), while also questioning whether the ARSIWA attribution framework is adequately suited to modern cyber operations. This paper also studies how political attribution of cyber operations very often outpaces the stricter and finer legal standards which are required under ARSIWA, through the 2020 SolarWinds cyberattack case. Simultaneously, it argues that while States are fast when it comes to political attribution, they lag in the legal attribution due to the strict evidentiary and structural limitations.

II. KEYWORDS

State Responsibility; ARSIWA; Cyber Attribution; SolarWinds; Tallinn Manual

III. INTRODUCTION

State responsibility, as enunciated by Dionisio Anzilotti, emerges from the breach of an international law obligation, hinges solely on the violation of that obligation.[2] This principle has been widely accepted in international law[3]. Outsourcing malicious activities to non-State actors does not, in itself, absolve a State of responsibility; however, under ARSIWA, such conduct is attributable only where the applicable thresholds particularly under Articles 5 or 8 are satisfied. As the International Court

[1] 3rd year (VI semester) Student at Manipal Law School, Manipal Academy of Higher Education, Bengaluru, (India). Email: khattry.aakriti@gmail.com
[2] D. Anzilotti, *International Law* 100–105 (C.G. Fenwick trans., Henry Regnery Co. 1955)
[3] Vishakha Jaiprakash Thanvi, State Responsibility Under International Law, 6 Int'l J.L. Mgmt. & Human. 486, 489-90, (2023).

of Justice held in the *Nicaragua* case[4] (1986) "effective control" of a State over such actors suffices for attribution.

Attribution in cyberspace is crucial in order to invoke responsibility and allow lawful countermeasures, but it remains underdeveloped in international law. The Tallinn Manual 2.0 applies ARSIWA to cyber operations, yet it also notes practical challenges like anonymity and proxy use, and difficulty in evidentiary verification[5].

Against this background, this paper examines the attribution problem via analysing the 2020 SolarWinds supply-chain attack to determine if the traditional framework of ARSIWA can respond effectively and hold States accountable in today's cybersecurity environment.

This paper proceeds in four parts. The first section outlines the theoretical framework of attribution under international law, focusing on ARSIWA and the jurisprudence of the International Court of Justice. The second section examines the adaptation of these principles to cyberspace, with particular reference to the Tallinn Manual 2.0 and contemporary scholarly debates. The third section analyses the SolarWinds incident as a case study to evaluate the gap between political and legal attribution. The final section concludes by assessing whether ARSIWA's attribution regime remains normatively and practically adequate in the cyber domain.

A. Research Objectives

1. To examine the applicability of the Articles on Responsibility of States for Internationally Wrongful Acts (ARSIWA) to cyber operations.
2. To analyse the legal standards governing attribution of cyber activities to States under international law.
3. To evaluate the evidentiary and doctrinal challenges in attributing sophisticated cyber operations such as the SolarWinds incident.

[4] *Military and Paramilitary Activities in and Against Nicaragua (Nicar. v. U.S.)*, 1986 I.C.J. 14, ¶ 115 (June 27).
[5] TALLINN MANUAL 2.0 ON THE INTERNATIONAL LAW APPLICABLE TO CYBER OPERATIONS (Michael N. Schmitt ed., Cambridge Univ. Press 2017).

4. To assess the interpretative guidance provided by the Tallinn Manual framework in determining State responsibility for cyber conduct.

B. Research Questions

1. To what extent do ARSIWA principles adequately address the attribution of cyber operations to States?
2. What evidentiary and legal thresholds govern the attribution of cyber operations under international law?
3. How does the SolarWinds incident illustrate the practical limitations of existing attribution doctrines?
4. Does the Tallinn Manual provide sufficient normative clarity regarding State responsibility in cyberspace?

C. Research Hypotheses

1. Existing principles under ARSIWA are formally applicable to cyber operations but face significant evidentiary limitations in practice.
2. The absence of uniform attribution standards in cyberspace creates interpretative inconsistencies in determining State responsibility.
3. Soft-law instruments such as the Tallinn Manual partially clarify legal standards but do not eliminate ambiguity regarding proof and evidentiary thresholds.

D. Research Methodology

This paper adopts a doctrinal and analytical methodology, primarily examining treaty law, customary international law principles, and the International Law Commission's Articles on Responsibility of States for Internationally Wrongful Acts (ARSIWA). It further engages in analytical evaluation of State practice and scholarly interpretations, particularly in the context of cyber operations such as the SolarWinds incident. Relevant academic commentary and international legal materials are critically assessed to determine the scope and limits of attribution standards in cyberspace.

E. Literature Review

Scholarly discourse on cyber attribution and State responsibility has evolved significantly over the past decade. Kristen Eichensehr examines the decentralised enforcement mechanisms in cyberspace and the growing role of States in attributing malicious cyber conduct. Mikanagi and Mačák analyse evidentiary complexities and the fragmentation of attribution standards. James Crawford's commentary on ARSIWA provides foundational guidance on the legal principles governing attribution and State responsibility. Michael Schmitt, through the Tallinn Manual project, offers interpretative clarification on how international law applies to cyber operations. Conforti contributes to broader doctrinal discussions on the structure and scope of State responsibility under customary international law.

Collectively, these works highlight both the formal applicability of traditional attribution principles and the practical challenges posed by technical anonymity, proxy actors, and evidentiary uncertainty in cyberspace.

IV. THEORETICAL FRAMEWORK OF ATTRIBUTION IN INTERNATIONAL LAW

A. Historical Roots

Grounded in Westphalian sovereignty, the doctrine of State responsibility has developed around the idea that States are accountable for wrongful acts, taking place within, or birthing in their territory.[6] In *Corfu Channel* (1949), the ICJ articulated the principle that a State must not knowingly allow its territory to be used for acts contrary to the rights of other States. While this formulation has become foundational in discussions of due diligence and State responsibility, the case itself was grounded in territorial knowledge and control rather than in the technologically mediated context of cyberspace. Its direct transposition to cyber operations remains contested in contemporary scholarship, particularly in analyses of incidents such as SolarWinds.

Expanding on this basis, the Court in the *Nicaragua* judgement further clarified attribution rules, ruling that even significant or predominant support such as

[6] JAMES CRAWFORD, STATE RESPONSIBILITY: THE GENERAL PART (Cambridge Univ. Press 2013).

"financing, organizing, training, supplying and equipping" a non-state armed group is insufficient to attribute the group's conduct to the State. Attribution, as stated by the Court, requires proof that the State exercised 'effective control' over the specific military or paramilitary operations during which the wrongful acts were committed. This 'effective control' standard, articulated in *Nicaragua* (para. 115), demands operational control over the precise conduct in question. It is distinct from the ICTY's 'overall control' test in *Tadić*, which permits attribution on the basis of a broader relationship of organization and coordination. The divergence between these standards remains central to contemporary debates on proxy attribution, including in the cyber domain, where the threshold of control is often determinative.[7]

V. ARSIWA'S ATTRIBUTION REGIME

The International Law Commission's Draft Articles on Responsibility of States for Internationally Wrongful Acts (ARSIWA) lay down the *secondary rules* governing when conduct is attributed to a State. ARSIWA determines the legal channel by which a State becomes responsible when States break these obligations.

Article 2 of ARSIWA codifies the twin elements of State responsibility, namely attribution and breach. Both of these must be simultaneously met for an internationally wrongful act to occur[8].

The ARSIWA commentary emphasises that attribution is normatively established, and not factual, the question is whether international law recognises the conduct as that of the State.

Article 4 makes the conduct of all of its organs (executive, military, intelligence), automatically attributable to the State, including cyber units or intelligence directorates acting within or beyond domestic authority[9].

[7] *Nicaragua,* supra note 2, ¶115.
[8] Draft Articles on Responsibility of States for Internationally Wrongful Acts, UN Doc A/56/10 (2001), art.2.
[9] ARSIWA, supra note 6, art. 4 cmt. at 65–67.

Article 5 extends attribution to private entities empowered by domestic law to exercise governmental authority, such as State-mandated cybersecurity or defence enterprises undertaking sovereign functions[10].

Article 7 confirms that ultra vires or unauthorized acts of State organs remain attributable, even when operatives exceed instructions or competence[11].

The ILC integrates the ICJ's *Nicaragua* "effective control", requiring operational control over the specific activity. If non-State actors acting as proxies were directed or effectively controlled by State intelligence, attribution follows even without formal organ status[12].

Article 8 follows this "effective control" standard, requiring proof that the State directed the specific operation. This high threshold established by the article and the judgement, becomes legally challenging in cyber contexts which often involve proxy wars or blended operations.

Article 11 further provides that conduct not otherwise attributable to a State shall nevertheless be considered an act of that State if and to the extent that the State acknowledges and adopts the conduct as its own. Although this provision is invoked sparingly in practice, it remains doctrinally significant in cyber contexts. Public endorsement, explicit approval, or formal adoption of a cyber operation may trigger attribution even where Articles 4, 5, or 8 thresholds are not conclusively satisfied. Conversely, in the SolarWinds incident, Russia's categorical denial of involvement precluded the operation of Article 11, thereby reinforcing the centrality of evidentiary proof under Articles 4 and 8.

VI. CONSENT IN ATTRIBUTION

ARSIWA's structure reflects the positivist foundations of international law, particularly the centrality of State consent in the creation and limitation of legal obligations. As Anzilotti observed, international responsibility arises within a system premised on the voluntary acceptance of binding norms. In this framework, Article 20

[10] ARSIWA, supra note 6, art. 5 cmt. at 67–68.
[11] ARSIWA, supra note 6, art.7 cmt. at 71–72.
[12] ARSIWA, supra note 6, art. 8 cmt. at 72–75 (citing *Nicaragua*, supra note 2, ¶ 115).

of ARSIWA recognises consent as a circumstance precluding wrongfulness, confirming that conduct undertaken with valid State consent cannot constitute an internationally wrongful act.

Although consent was not at issue in the SolarWinds intrusion, this positivist architecture underscores a broader structural point relevant to cyber attribution: in the absence of clearer, collectively accepted evidentiary standards, attribution remains dependent on existing consent-based rules that were not designed with digitally mediated operations in mind. The gap between traditional consent-based doctrines and contemporary cyber realities thus reinforces the paper's central argument regarding the normative and evidentiary limits of ARSIWA in cyberspace.

VII. ATTRIBUTION IN CYBERSPACE – ADAPTATIONS AND CHALLENGES

The Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations, while not legally binding and not reflective of State practice as such, represents the views of an independent group of experts on how existing international law including ARSIWA applies in the cyber domain. It therefore provides persuasive but non-authoritative guidance on the continued applicability of traditional attribution rules to cyberspace.[13]

Rule 15 to 18 of the Tallinn Manual adapt ARSIWA's attribution rules to cyberspace by reaffirming that actions of State organs, including cyber units and intelligence agencies, remain attributable even when they exceed authority or act anonymously. The rules further extend attribution to private actors performing delegated sovereign cyber functions, while also applying the *Nicaragua*-based "effective control" test to the proxy-driven cyber landscape. The Tallinn Manual acknowledges that technical indicators like IP addresses, malware signatures, infrastructure reuse, or coding patterns commonly relied upon in cyber investigations are inherently fragile and

[13] Micheal N. Schmitt, ed., (2017) *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (Cambridge Univ. Press 2017), rule 14, cmt. at 87–88 (affirming ARSIWA's secondary rules apply without modification to cyber operations, rejecting domain exceptionalism).

insufficient on their own to conclusively establish attribution, while exposing the evidentiary fragility of cyber attribution.

Although ARSIWA provides a legal basis for holding States responsible for cyber operations, it is hard to apply in practice and cannot be operationalized under the current evidentiary conditions.

The traditional attribution tests under ARSIWA do not map cleanly onto the digital landscape. Even though the ARSIWA rules apply to cyberspace, cyber operations strain ARSIWA's factual threshold[14]. ARSIWA currently faces three major challenges in the cyber domain, which are anonymity, proxy use, and evidentiary subjectivity. These factors directly undermine Article 2's requirement that attribution be established through clear factual evidence. Cyber operations are structurally designed to obscure the identity of the real actor, making technical traces unreliable and allowing States to deny involvement[15].

This problem is compounded by proxy actors, like private hackers and contractors, who exploit the gap between Article 4 (State organs), Article 5 (delegated authority), and Article 8 (control over specific operations), through whom it becomes easy for States to claim plausible deniability. Alongside these structural barriers, evidentiary subjectivity remains a central obstacle; the Tallinn Manual 2.0 itself recognises that cyber indicators are easily manipulated[16], and rarely meet ARSIWA's requirement under Article 2 of establishing attribution through clear and solid factual evidence[17]. Much of the available intelligence in cyber incidents is therefore, inferential, circumstantial, fragmented, and classified, creating uncertainty in linking conduct to a specific State.

[14] Schmitt, supra note 14, rule 14, cmt. at 87–88 (ARSIWA applies but strains factual thresholds in cyber ops).
[15] Schmitt, supra note 14, rule 17, cmt. para. 3 at 94 (tools like VPNs/spoofing enable imitation/false flags, rendering evidence unreliable).
[16] Schmitt, supra note 14, at 131 (evidentiary challenges from manipulated trails create "difficulty of attribution," clouding ARSIWA application).
[17] ARSIWA, supra note 6, art. 2 cmt. para 2 at 32 (requiring conduct attributable under IL + breach of obligation, demanding solid factual links).

The practical consequence of this, leads to attributions being made on probabilities, and not certainties. Therefore, the governments in these cases use words and say "high probability" and not "conclusive proof".

As Mikanagi and Macak argue, these hybrid actors blur the line between State and non-State conduct, undermining the architecture of ARSIWA attribution[18].

Where State organs are denied and delegation is informal, attribution inevitably shifts to Article 8. This article states that attribution requires "effective control" over the specific operation, since mere funding, or encouragement, or ideological support is not enough to establish attribution[19]. This makes it challenging for ARSIWA, since in these cyber contexts, proving that the State gave such specific instructions is extremely difficult because, communications are encrypted, tasking more often happens on private channels, and malware access is shared by multiple actors. Tallinn further accepts that digital clues such as, malware families or coding style or infrastructure reuse, suggest control, but still do not satisfy the *Nicaragua*'s strict "effective control" standard[20]. As a result, Article 8 becomes the default gateway for cyber attribution and the point at which most claims fail.

The Park Jin Hyok case illustrates the evidentiary gap between political attribution and ARSIWA-grade legal proof. In 2018, the United States Department of Justice indicted Park Jin Hyok, a North Korean national allegedly associated with the Lazarus Group, for his role in major cyber operations including the Sony Pictures hack and the WannaCry ransomware attack. While the indictment publicly attributed the conduct to actors linked to the Democratic People's Republic of Korea, it relied heavily on technical forensics and intelligence assessments. As analysed by Mikanagi and Mačák, the case demonstrates that although the political attribution was forceful and detailed,

[18] Yoshiki Mikanagi & Kubo Mačák, Attribution of Cyber Operations: An International Law Perspective on the Park Jin Hyok Case, 9 CAMBRIDGE INT'L L.J. 51, 52–54 (cyber ops involve blurred actors like contractors/patriotic groups, complicating state/non-state distinction).
[19] ARSIWA, supra note 6, art. 8, cmt. para ¶ 2 at 47 (attribution for private actors requires effective control over specific operation, excluding mere funding/support).
[20] Schmitt, supra note 14, rule 17 cmt. para. 5, at 95–96 (digital clues like malware reuse suggest but do not meet *Nicaragua*'s strict effective control under ARSIWA Art. 8); *see Military and Paramilitary Activities in and Against Nicaragua (Nicar. v. U.S.)*, 1986 I.C.J. 14, ¶ 115 (June 27).

the publicly available evidence did not establish the level of "effective control" required under Article 8 of ARSIWA for State responsibility.[21]

Cyber evidence is classified and technical. An ex-ante decision, for example, the countermeasures or sanctions often apply lower evidentiary thresholds, but international litigation, in the ICJ or ICC, requires near certainty, and this mismatch results in uneven State practices, a weak opinio juris, and ultimately politicized attribution[22].

These challenges clearly expose the gaps in ARSIWA's fitness when it comes to cyber operations. In the next segment of the paper, the author indicates exactly how SolarWinds reflects this, wherein the forensic indicators point towards SVR, but Russia denies it and evidence is insufficient for ICJ-level attribution.

In this part, the three landmark cases are discussed, where cyber incidents reflect a recurring global pattern, where in the public and political attributions are made rather quickly and confidently by States. There is no formal international legal action that follows, since there are no ICJ cases, and no ARSIWA-based responsibility, domestic action does happen, but it is more often than not, politicized, and finally, States rely on sanctions, statements, and indictments, which is not formal international law mechanisms. SolarWinds shows exactly this pattern repeating[23].

Eichensehr in her article, talks about how "public blame" is different from "legal bite"[24], since States increasingly issue joint public attributions, and in these announcements, they often cite words like, "high confidence", "technical analysis", and "intelligence assessments". But States often withhold detailed evidence proving the same, citing national and security concerns. In her article, Eichensehr, also states that there is ,"no international legal duty to release evidence". Legally, it does not meet

[21] Mikanagi & Mačák, supra note 23, at 55–58 (Park's patterns linked to DPRK but lacked direct instructions, insufficient for ARSIWA Art. 8, illustrating political-legal gap).
[22] Kristen E. Eichensehr, The Law and Politics of Cyberattack Attribution, 67 UCLA L. REV. 520, 551–53 (2020) (ex-ante probabilistic thresholds for sanctions vs. near-certainty for ICJ create weak opinio juris and politicization).
[23] Id. at 550–51 (describing "coordinated attributions" as recurring but non-legal pattern).
[24] Id. at 550 (coining "public blame" for joint statements vs. "legal bite" of enforceable responsibility).

ARSIWA's requirements for attribution, since there is no solid factual link per Article 2, no proven organ or proxy control per Articles 4 and 8, and no legal forum invoked[25].

Stuxnet, WannaCry, and NotPetya collectively show how major cyber incidents receive strong public attributions yet never trigger formal legal responsibility under ARSIWA. Stuxnet, which targeted Iran's Natanz nuclear facility, was widely attributed on technical and investigative grounds to the United States and Israel, yet no State acknowledged responsibility and Iran did not bring up any international claim, leaving attribution in a purely political space[26].

Similarly, 2017 WannaCry ransomware attack was forensically linked to North Korea's Lazarus Group[27], prompting coordinated public attribution by several States and a domestic indictment, but no proceedings were initiated before any international tribunal, and the evidentiary basis remained largely undisclosed, preventing any test of Article 8's effective control threshold. NotPetya followed the same trajectory, although governments publicly attributed the attack to the Russian state-linked actors[28], based on technical and contextual indicators, the attribution remained diplomatic rather than legal[29], with no international adjudicatory mechanism invoked and no evidentiary record released.

In all three cases, attribution relied on technical forensics and intelligence assessments, wherein evidence stayed classified. States acted via sanctions or diplomacy instead of the international law mechanisms, and hence, deniability allowed the States to avoid ARSIWA consequences. These patterns show that, ARSIWA attribution standards are too rigid for cyber operations, since the evidentiary requirements are too high, therefore, cyberspace still remains a "Wild West" with political blame but no actual legal

[25] Id. at 551–53 (no IL duty to disclose evidence, weakening Art. 2 factual links and Arts. 4/8 control proofs).
[26] Id. at 550 (US-Israel leak-based attribution; "neither confirm nor deny" policy avoids ARSIWA invocation)
[27] Id. at 552 (code reuse/IP patterns as "high confidence" indicators; indictments but no formal IL process)
[28] Id. at 554 (malware/geopolitical links to GRU; multinational coordination without substantiation).
[29] Fact Sheet, Imposing Costs for Harmful Foreign Activities by the Russian Government, WHITE HOUSE (Apr. 15, 2021), https://www.whitehouse.gov/briefing-room/statements-releases/2021/04/15/fact-sheet-imposing-costs-for-harmful-foreign-activities-by-the-russian-government/ (labelling NotPetya "reckless" and imposing sanctions, eschewing formal IL).

accountability[30]. These cases collectively demonstrate a consistent global pattern, with strong political attribution, but no international adjudication, and thus, no ARSIWA consequences.

VIII. THE SOLARWINDS CASE STUDY – FACTUAL ATTRIBUTION AND LEGAL GAPS

The SolarWinds incident involved a sophisticated supply-chain cyberattack wherein the attackers gained access to the Orion software build environment. Malicious code, later identified as Malware (SUNBURST) was inserted into legitimate updates. The compromised updates were digitally signed and distributed globally. This infusion of malware went undetected until FireEye uncovered it. US agencies publicly attributed the operation to Russia's SVR/APT29 based on malware lineage, infrastructure reuse, operational tradecraft, and classified intelligence assessments. The attackers operated from within SolarWinds's software build environment, including developer systems, and the operation appears to have been limited to covert intelligence-gathering, with no destructive or disruptive component.

This characterisation raises the contested question of whether espionage per se constitutes a violation of international law. While espionage is widely regarded as unfriendly and unlawful under domestic law, many scholars including Michael Schmitt observe that international law does not clearly prohibit peacetime cyber espionage as such. If SolarWinds is properly characterised as a non-destructive intelligence operation, the threshold question becomes whether any primary rule of international law was breached at all, thereby complicating the Article 2 requirement of an internationally wrongful act.

As analysed by Antonio Coco, Talita Dias, and Tsvetelina van Benthem, the forensic indicators supporting attribution to Russia's SVR are strong and persuasive for political purposes, yet they fall short of the "clear and solid factual" standard that

[30] Eichensehr, supra note 27, at 555 (evidentiary rigidity enables deniability, perpetuating cyber impunity patterns like SolarWinds).

would likely be required before the International Court of Justice under Article 2 of ARSIWA.[31]

Even spectacular, well-documented cyber intrusions leave attribution ambiguities, since political attribution works fast, but legal attribution remains uncertain.

In this part, the author applies the ARSIWA code to the SolarWinds, per Article 4, the conduct of any State organ is automatically attributable to the State. In here, the attribution is to SVR, which is Russia's Foreign Intelligence Service, legally a State organ. Article 7 also negates any claim, even if operatives exceeded instructions, since ultra vires acts are still attributable.

Even if Russia invokes "rogue actors", then attribution must move from Article 4 to 8, which is direction or effective control. Per Article 8 standard of *Nicaragua*, it requires the proof of specific operational over the precise wrongful act. Cyber forensics like, the malware families, TTPs, C2 infrastructure, suggest direction, but no revealed intelligence showing explicit orders, and no intercepts showing tasking. Therefore, attribution under Article 8 remains incomplete, enabling Russia's denial.

US responded, by firstly applying sanctions which were countermeasures and not formal legal proceedings, the White House sanctioned targeting SVR officers, Russian technology companies who were aiding the operations, six individuals and 16 entities. The justification given by US for these sanctions were that it was "imposing costs" for harmful Russian activity. US never invoked ARSIWA initiating any action against Russia in ICJ proceedings. The executive order, which was triggered by this whole incident, mandated the zero-trust architecture demonstrating how domestic cybersecurity reform followed political attribution. GAO reports even notes, that the pre-breach federal system lacked, the multifactor authentication, endpoint detection and response tools, and adequate logging.

Forensics gave "high confidence" but still fell short of ARSIWA's stringent "solid factual requirement" per Article 2. SolarWinds, therefore, shows how political attribution succeeds on probabilistic intelligence, and legal attribution under ARSIWA

[31] Antonio Coco, Talita Dias & Tsvetelina van Benthem, *Illegal: The SolarWinds Hack under International Law* (2022) 33 European Journal of International Law 1275.

struggles because of evidentiary opacity, intelligence secrecy, and the absence of a forum capable of testing classified material.

IX. SUGGESTIONS AND RECOMMENDATIONS

1. Greater clarification of evidentiary standards for cyber attribution should be pursued through multilateral dialogue or interpretative statements at the United Nations level.
2. States should enhance transparency in public attribution practices to strengthen normative consistency and accountability.
3. Development of technical-legal cooperation frameworks may improve the reliability of attribution assessments.
4. Soft-law instruments such as the Tallinn Manual should continue evolving to reflect emerging State practice and technological advancements.

X. CONCLUSION

SolarWinds displays the structural mismatch between ARSIWA's attribution model and the realities of cyber operations. Evidentiary opacity, anonymity, proxy actors, and classified intelligence prevent States from meeting Article 2's threshold. Without clearer procedures, greater transparency in public attribution practices, or the development of cyber-specific evidentiary standards through multilateral engagement, attribution remains politically driven and legal responsibility specifically under ARSIWA remains theoretical rather than operational. These structural limitations underscore the need for the normative and institutional reforms outlined in the Suggestions and Recommendations section.

XI. BIBLIOGRAPHY

A. Primary Sources

1. Draft Articles on Responsibility of States for Internationally Wrongful Acts, in *Report of the International Law Commission on the Work of Its Fifty-Third Session*, U.N. GAOR, 56th Sess., Supp. No. 10, U.N. Doc. A/56/10 (2001).

2. *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (Michael N. Schmitt gen. ed., Cambridge Univ. Press 2017).
3. U.S. Gov't Accountability Office, *Cybersecurity: Federal Responses to SolarWinds and Microsoft Exchange Incidents*, GAO-22-104746 (2022).
4. Antonio Coco, Talita Dias & Tsvetelina van Benthem, Illegal: The SolarWinds Hack Under International Law, 33 *Eur. J. Int'l L.* 1275 (2022).

B. Secondary Sources

1. *Corfu Channel* (U.K. v. Alb.), 1949 I.C.J. 4 (Apr. 9).
2. *Military and Paramilitary Activities in and Against Nicaragua* (Nicar. v. U.S.), 1986 I.C.J. 14 (June 27).
3. Kristen E. Eichensehr, The Law and Politics of Cyberattack Attribution, 67 *UCLA L. Rev.* 520 (2020).
4. Kristen E. Eichensehr, SolarWinds: Accountability, Attribution, and Advancing the Ball, Just Security (Apr. 16, 2021), https://www.justsecurity.org/75779/solarwinds-accountability-attribution-and-advancing-the-ball/.
5. Yoshiki Mikanagi & Kubo Mačák, Attribution of Cyber Operations: An International Law Perspective on the Park Jin Hyok Case, 9 *Cambridge Int'l L.J.* 51 (2020).
6. Fact Sheet: Imposing Costs for Harmful Foreign Activities by the Russian Government, White House (Apr. 15, 2021), https://www.whitehouse.gov/briefing-room/statements-releases/2021/04/15/fact-sheet-imposing-costs-for-harmful-foreign-activities-by-the-russian-government/
7. World Econ. Forum, *Global Cybersecurity Outlook 2025* (2025), https://www.weforum.org/publications/global-cybersecurity-outlook-2025/.