THE ATTRIBUTION DILEMMA IN CYBERSPACE: RETHINKING STATE RESPONSIBILITY FOR MALICIOUS CYBER OPERATIONS UNDER INTERNATIONAL LAW

Murchana Baruah**,** Advocate, Dibrugarh, Assam, India

ABSTRACT

Malicious cyber operations targeting critical infrastructure and governmental systems raise complex questions concerning State responsibility under public international law. Although existing international law applies to State conduct in cyberspace, establishing whether a cyber operation is legally attributable to a State remains difficult. This paper examines the adequacy of the Articles on Responsibility of States for Internationally Wrongful Acts (2001) in addressing these challenges.

The study adopts a doctrinal methodology, examining international legal instruments, International Court of Justice (ICJ) judgments, United Nations reports, State practice, and scholarly literature, including the Tallinn Manual 2.0. It analyses Articles 4, 5, 8 and 11 of the Articles on State Responsibility, with particular reference to *Nicaragua v. United States and Bosnia and Herzegovina v. Serbia and Montenegro*. It also distinguishes technical, political, and legal attribution, demonstrating that technical indicators and public allegations do not automatically establish State responsibility.

The findings indicate that the principal challenge lies in applying existing legal rules to concealed governmental involvement, non-State actors, compromised infrastructure, and inaccessible digital evidence.

The paper recommends greater transparency in public attribution where feasible, stronger international cooperation in preserving and exchanging digital evidence, clearer articulation of States' legal positions, and continued multilateral dialogue. It concludes that the existing framework provides a foundation for accountability, but its effectiveness depends on reliable evidence and consistent State practice.

Keywords: International Law; Cyber Operations; State Responsibility; Legal Attribution; Cybersecurity; Non-State Actors; International Court of Justice.

1. INTRODUCTION

Cyberspace has become an important domain of governmental activity, international competition, economic interaction and national security. States rely on interconnected digital systems for public administration, financial services, healthcare, telecommunications, energy distribution, transportation and defence. These systems can also be targeted by malicious cyber operations capable of disrupting services, compromising information, damaging infrastructure or interfering with governmental functions.[1]

Unlike many conventional acts of State conduct, malicious cyber operations may be carried out through infrastructure distributed across several jurisdictions, using compromised devices, anonymisation techniques, intermediaries or groups whose relationships with governmental authorities are difficult to establish. An operation may pass through infrastructure located in several States before reaching its target. The geographical location of the infrastructure therefore does not, by itself, establish the identity of the responsible actor or the State to which the conduct may legally be attributed.[2]

These characteristics raise a fundamental question of public international law: when does a malicious cyber operation become an internationally wrongful act of a State?

The law of State responsibility provides the starting point for answering that question. Article 1 of the International Law Commission's Articles on Responsibility of States for Internationally Wrongful Acts states that every internationally wrongful act of a State entails the international responsibility of that State. Article 2 identifies two elements: the conduct must be attributable to the State under international law, and it must constitute a breach of an international obligation binding upon that State.[3] The Articles were adopted by the International Law Commission in 2001 and annexed to United Nations General Assembly Resolution 56/83. They were not adopted as a treaty; the General Assembly took note of them and commended them to the attention of Governments without prejudice to their future adoption or other appropriate action. The extent to which individual provisions reflect

[1] U.N. Secretary-General, *Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*, ¶¶ 3–7, U.N. Doc. A/70/174 (July 22, 2015).
[2] Id. ¶ 28(f). The report states that an indication that an ICT activity was launched or originated from the territory or ICT infrastructure of a State may be insufficient, by itself, to attribute the activity to that State.
[3] ILC Articles on State Responsibility, supra note 1, arts. 1–2.

customary international law must be assessed according to the relevant rule and supporting authority.[4]

The distinction between attribution and breach is particularly important in cyberspace. Technical evidence may identify a device, infrastructure, account or suspected operator without establishing that the conduct is attributable to a State under international law. Conversely, conduct attributable to a State does not automatically constitute an internationally wrongful act unless an applicable international obligation has also been breached.

The legal inquiry is therefore not limited to identifying a computer, individual or organisation involved in a cyber incident. It requires an assessment of the legally relevant connection between the conduct and a State, followed by an assessment of whether the conduct breached an international obligation.

The International Court of Justice (ICJ) has developed important principles concerning attribution, particularly in Military and Paramilitary Activities in and against Nicaragua and Application of the Convention on the Prevention and Punishment of the Crime of Genocide. Although neither judgment concerned cyber operations, their treatment of State organs, non-State actors, instructions, direction and control provides relevant legal authority when assessing whether conduct by a non-State actor may be attributed to a State.[5] The precise application of those principles to particular cyber operations, however, requires analysis of the facts and the relevant attribution rule.

The Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations, published in 2017, examines how existing international law applies to cyber operations, including activities below the thresholds of the use of force and armed conflict. It is a non-binding scholarly work prepared by an international group of experts; it is not a treaty and does not, by itself, establish the legal position of States.[6]

Against this background, this paper examines whether the existing international law of State responsibility provides an adequate framework for addressing malicious cyber

[4] G.A. Res. 56/83, annex, ¶ 3 (Dec. 12, 2001); International Law Commission, *Draft Articles on Responsibility of States for Internationally Wrongful Acts*, with Commentaries, general commentary, U.N. Doc. A/56/10 (2001).
[5] *Nicaragua*, 1986 I.C.J. 14, ¶¶ 109–15; *Bosnia Genocide*, 2007 I.C.J. 43, ¶¶ 385–415.
[6] Tallinn Manual 2.0 on the *International Law Applicable to Cyber Operations* (Michael N. Schmitt ed., Cambridge University Press 2017).

operations. It argues that the general rules of attribution remain relevant, while their practical application is complicated by evidentiary limitations, uncertainty surrounding indirect State involvement and the absence of a universally prescribed procedure for publicly demonstrating the basis of an attribution decision. The latter point concerns public attribution practice; it should not be understood to mean that international law contains no rules governing attribution.

The paper does not assume that every cyberattack constitutes a use of force, an armed attack or an internationally wrongful act. Instead, it focuses on the attribution of conduct and the requirements for establishing State responsibility under general international law.[7]

1.1 Research Questions

The paper addresses the following questions:

1. How do the Articles on State Responsibility apply to malicious cyber operations conducted by State organs and non-State actors?

2. How do technical attribution and legal attribution differ, and why is that distinction significant?

3. To what extent do the ICJ's attribution principles assist in assessing indirect State involvement in cyber operations?

4. What legal and institutional measures could improve the practical application of State responsibility in cyberspace?

1.2 Research Objectives

The objectives of this paper are to examine the existing international legal framework governing attribution; analyse the relevance of international judicial decisions to cyber operations; identify the principal evidentiary and institutional difficulties affecting the determination of State responsibility; and propose measures to improve international cooperation and legal accountability.

[7] U.N. Charter arts. 2(4), 51; ILC Articles on State Responsibility, supra note 1, arts. 1–2.

1.3 Research Methodology

This research adopts a doctrinal methodology. It examines primary legal materials, including the Charter of the United Nations, the Articles on State Responsibility, relevant ICJ judgments, United Nations documents concerning international cybersecurity, and publicly available statements of State practice.[8]

Secondary sources, particularly the Tallinn Manual 2.0 and academic commentary, are used to evaluate competing interpretations of international law. The research is qualitative and analytical rather than empirical. It does not purport to independently establish the technical origin of any particular cyber operation or verify classified intelligence assessments.

The paper distinguishes binding international legal obligations from non-binding resolutions, expert commentary and policy recommendations. This distinction is necessary because scholarly interpretations and political declarations do not have the same legal status as treaties, applicable rules of customary international law or binding judicial decisions between the parties in a particular case. The legal significance of any particular source must nevertheless be assessed in context.[9]

2. THE INTERNATIONAL LEGAL FRAMEWORK GOVERNING STATE RESPONSIBILITY

2.1 The General Principles of State Responsibility

The international law of State responsibility establishes the legal consequences arising when a State commits an internationally wrongful act. The International Law Commission completed its Articles on Responsibility of States for Internationally Wrongful Acts in 2001. The United Nations General Assembly took note of the Articles in Resolution 56/83 and commended them to the attention of Governments. The Articles are not, as a whole, a treaty. They are an important codification and progressive-development text; the legal status of an individual provision depends on whether it reflects customary international law, an applicable

[8] U.N. Charter arts. 2(4), 51; ILC Articles on State Responsibility, supra note 1; Nicaragua, 1986 I.C.J. 14; Bosnia Genocide, 2007 I.C.J. 43; U.N. Doc. A/70/174, supra note 3.
[9] Statute of the International Court of Justice arts. 38(1), 59; Tallinn Manual 2.0, supra note 9. The legal effect of a source depends on its nature and the applicable law.

treaty rule or another relevant source of law.

Article 2 establishes two cumulative requirements for an internationally wrongful act: the conduct must be attributable to the State under international law, and it must constitute a breach of an international obligation binding upon that State.[10] In the context of cyber operations, these requirements must be examined separately. For example, suppose a group conducts a cyber operation against another State's electricity infrastructure. Even if a technical investigation establishes that the operation used servers located in a particular country, that fact alone does not establish that the territorial State conducted, directed or controlled the operation. The inquiry must identify the relevant actor, apply the appropriate legal rule of attribution and assess whether the attributable conduct breached an international obligation.

Likewise, attribution of an operation to a State does not, by itself, establish that the operation was unlawful. The applicable obligation must be identified and interpreted in light of the circumstances. Depending on the facts, potentially relevant rules may concern sovereignty, non-intervention, the prohibition on the use of force, international humanitarian law where applicable, or other international obligations. These rules have distinct elements and thresholds; they should not be treated as interchangeable.

This distinction matters because identifying a suspected State actor is not the same as establishing State responsibility. A legally sound analysis must establish both attribution and breach, subject to any other relevant rules of international responsibility.

2.2 The UN Charter and Cyber Operations

The Charter of the United Nations establishes the principal legal framework governing international peace and security. Article 2(4) requires Member States to refrain from the threat or use of force against the territorial integrity or political independence of any State, or in any other manner inconsistent with the purposes of the United Nations. Article 51 preserves the inherent right of individual or collective self-defence if an armed attack occurs, subject to the applicable requirements of international law.[11]

[10] ILC Articles on State Responsibility, supra note 1, art. 2.
[11] U.N. Charter arts. 2(4), 51.

These provisions may be relevant to cyber operations, but their application depends on the circumstances of the particular operation. The legal characterisation of a cyber operation requires an assessment of its nature, scale, effects and context, together with the relevant rules of international law.

A cyber operation causing physical destruction or injury may raise different legal questions from an operation involving espionage, data theft, temporary service disruption or interference with computer systems. Such distinctions are relevant to the legal analysis, but no single consequence automatically resolves every question under the Charter. In particular, the threshold for a use of force under Article 2(4) and the threshold for an armed attack under Article 51 should not be conflated.[12]

The UN Charter does not contain a separate, comprehensive code governing cyber operations. States have nevertheless considered the application of existing international law to information and communications technologies through United Nations processes, including the Group of Governmental Experts (GGE) and the Open-ended Working Group (OEWG) on developments in the field of information and telecommunications in the context of international security.[13]

The 2015 GGE report stated that international law, particularly the Charter of the United Nations, is applicable to the use of information and communications technologies by States. It also addressed sovereignty, non-intervention and the responsibilities of States in connection with internationally wrongful acts attributable to them. The report further observed that the fact that an ICT activity originated from the territory or infrastructure of a State may be insufficient, by itself, to attribute the activity to that State. Subsequent UN processes have continued to consider international law and responsible State behaviour in cyberspace.

These developments support the proposition that State use of information and communications technologies must be assessed within the existing international legal order. They do not eliminate disagreement among States over the interpretation or application of particular rules to specific cyber activities.

[12] U.N. Charter arts. 2(4), 51; *Nicaragua*, 1986 I.C.J. 14, ¶ 191.
[13] U.N. Doc. A/70/174, supra note 3; U.N. Secretary-General, *Report of the Open-ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security*, U.N. Doc. A/75/816 (Mar. 18, 2021).

2.3 Attribution as a Distinct Legal Requirement

Attribution determines whether conduct is treated as an act of a State for the purposes of international responsibility. It is not identical to identifying the technical origin of an operation, establishing its political motivation or determining which State may have benefited from it. Technical evidence may inform the legal inquiry, but the legal conclusion must be reached by applying the relevant rules of international law to the facts.[14]

The Articles on State Responsibility address attribution principally in Articles 4 to 11. Article 4 concerns the conduct of State organs. Article 5 concerns persons or entities empowered by the law of the State to exercise elements of governmental authority, where they act in that capacity in the particular instance. Article 8 concerns conduct carried out on the instructions of, or under the direction or control of, a State. Article 11 addresses conduct that was not otherwise attributable to the State but that the State subsequently acknowledges and adopts as its own.

These provisions may be relevant where cyber operations are conducted by military or intelligence agencies, entities exercising delegated governmental authority, private contractors or other non-State actors. The correct provision depends on the actor's status and the circumstances in which the conduct occurred; the mere involvement of a private entity does not automatically make Article 8 the applicable rule.

Attribution under Article 8 requires more than political sympathy, geographical proximity, a shared strategic interest or general contacts between a group and a government. The ICJ has interpreted Article 8 by reference to instructions, direction or control in relation to the conduct at issue. Its Nicaragua and Bosnia Genocide judgments are particularly important to the distinction between support for a non-State group and legal attribution of that group's specific conduct to a State.[15]

Attribution must therefore be assessed by applying the relevant legal rule to the available evidence, rather than by relying solely on the perceived character, political orientation or location of the suspected actor.

[14] ILC Articles on State Responsibility, supra note 1, arts. 4–11; U.N. Doc. A/70/174, supra note 3, ¶ 28(f).
[15] *Nicaragua*, 1986 I.C.J. 14, ¶ 115; *Bosnia Genocide*, 2007 I.C.J. 43, ¶¶ 398–407.

3. STATE ATTRIBUTION IN MALICIOUS CYBER OPERATIONS

3.1 Cyber Operations Conducted by State Organs

Article 4 of the Articles on State Responsibility provides that the conduct of any State organ is considered an act of that State under international law, whether the organ exercises legislative, executive, judicial, or other functions.[16] This principle applies irrespective of whether the State organ conducts its activities through conventional means or digital infrastructure. If members of a State's military or intelligence service conduct a cyber operation in their official capacity, the legal question is generally one of identifying the conduct and establishing the status and capacity in which the actors operated.

Cyber operations may make that inquiry more difficult in practice because the individuals responsible may use concealed identities, third-party infrastructure, or intermediaries. Nevertheless, the technological means employed do not themselves remove the conduct from the ordinary rules governing State organs.

The legal difficulty lies primarily in establishing the relevant facts. Public evidence may be incomplete, while technical reports may identify indicators associated with a particular actor without establishing the actor's official status or the capacity in which the conduct occurred.[17] Article 4 therefore provides a relatively clear legal starting point, but its practical application depends on the quality of the evidence available.[18]

3.2 Governmental Authority and Article 5

Article 5 addresses the conduct of persons or entities that are not State organs under Article 4 but are empowered by the law of the State to exercise elements of governmental authority, provided that they act in that capacity in the particular instance. This provision may be relevant where a State entrusts a private entity with a legally recognised governmental

[16] International Law Commission, *Draft Articles on Responsibility of States for Internationally Wrongful Acts, with Commentaries*, art. 4, U.N. Doc. A/56/10 (2001), reprinted in *Yearbook of the International Law Commission*, 2001, vol. II, pt. 2. Official UN text and commentaries.

[17] U.N. General Assembly*, 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, para. 28(f) (July 22, 2015). UN Digital Library record. This report recognises that the fact that ICT activity originated from or passed through a State's territory or infrastructure may be insufficient, by itself, to attribute the activity to that State.

[18] ILC, *Draft Articles*, supra note 1, art. 4 and commentary to art. 4, paras. 1–2. The commentary identifies attribution of the conduct of State organs as the basic rule while recognising that application depends on the relevant facts.

function involving cybersecurity or digital infrastructure. However, a private cybersecurity company does not become an organ of the State merely because it provides services to a government. Nor does a contractual relationship automatically establish that every act of the contractor is attributable to the State.

The legal inquiry must examine whether the entity was empowered to exercise governmental authority and whether the conduct in question occurred in that capacity. The distinction is important because governments frequently rely on private technology companies, consultants, and contractors for digital services. Treating every activity of a government contractor as State conduct would extend attribution beyond the conditions established by international law.

Conversely, the private status of an entity does not necessarily prevent attribution where the legal requirements of Article 5 or another applicable attribution rule are satisfied.

3.3 Non-State Actors and Article 8

Article 8 provides that conduct of a person or group of persons shall be considered an act of a State under international law if the person or group is in fact acting on the instructions of, or under the direction or control of, that State in carrying out the conduct.[19] This provision is central to cases involving cyber operations conducted by groups outside the formal governmental structure. A State may benefit from the activities of a private group without having directed those activities. A group may also share a State's political objectives while operating independently. Neither circumstance automatically establishes attribution under Article 8.[20]

The relevant question is whether the necessary connection between the State and the conduct has been established under the applicable legal standard.[21]

In cyberspace, such a connection may be difficult to demonstrate because

[19] Id. art. 8.
[20] Id. art. 8; *Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States of America*), Merits, Judgment, 1986 I.C.J. Rep. 14, paras. 109–15. Official ICJ judgment.
[21] *Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Bosnia and Herzegovina v. Serbia and Montenegro*), Judgment, 2007 I.C.J. Rep. 43, paras. 398–407. Official ICJ judgment. The Court considered Article 8 and its prior jurisprudence, including the standard applied in Nicaragua. These judgments concerned non-cyber conduct; they are cited for the general attribution rule, not as decisions on cyber operations.

communications, instructions, payments, operational planning, and other evidence may be concealed or unavailable to outside investigators. A group may also conduct several operations independently while receiving support from a State in other respects. These circumstances require careful differentiation between different forms of State involvement.

Financial assistance, technical assistance, political support, and the provision of infrastructure may be relevant evidence, but their legal significance depends on the circumstances and the applicable rule. Support for a group does not necessarily establish that the State instructed, directed, or controlled the particular operation. This does not mean that indirect State involvement is legally irrelevant. It means that the relationship must be evaluated against the requirements of international law rather than inferred solely from the existence of support.[22]

3.4 Adoption of Conduct under Article 11

Article 11 concerns conduct that would not otherwise be attributable to a State under the preceding provisions but that the State acknowledges and adopts as its own.[23] This provision may be relevant where a government subsequently endorses or adopts an operation initially conducted by a non-State actor. However, public approval, political praise, or expressions of sympathy do not necessarily amount to adoption of the conduct as the State's own. The provision requires a sufficiently clear acknowledgement and adoption of the conduct.

In a cyber context, a State might publicly claim responsibility for an operation, but the legal consequences would depend on the nature and circumstances of the statement and the conduct concerned.

Article 11 illustrates that attribution is not limited to the relationship existing at the time an operation begins. Subsequent State conduct may also become legally significant. Nevertheless, the provision should not be interpreted so broadly that every expression of political approval becomes an admission of international responsibility.

[22] *Nicaragua*, 1986 I.C.J. Rep. 14, paras. 109–15; Bosnia Genocide, 2007 I.C.J. Rep. 43, paras. 398–407. These judgments support the need to apply the relevant attribution test to the facts rather than infer attribution solely from a general relationship between a State and a non-State group.
[23] ILC, *Draft Articles*, supra note 1, art. 11.

4. JUDICIAL APPROACHES TO ATTRIBUTION AND THEIR RELEVANCE TO CYBERSPACE

4.1 Nicaragua v. United States

In Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States of America), the International Court of Justice (ICJ) examined the responsibility of the United States in connection with its support for the contras in Nicaragua.[24] The judgment is important for its treatment of State involvement in the conduct of non-State actors. The Court distinguished between the extent of United States support for the contras and the degree of control necessary to attribute particular conduct to the United States. The Court considered the United States' financing, organising, training, supplying, and equipping of the contras, as well as its participation in planning certain activities. It concluded that this involvement did not, by itself, establish that all acts committed by the contras were attributable to the United States. In relation to the violations under consideration, the Court examined whether the United States exercised effective control over the operations in the course of which the alleged violations occurred.

The judgment is therefore closely associated with the effective-control standard. The decision is relevant to cyber operations because it distinguishes general support for a group from control over the particular conduct sought to be attributed to a State. A State's provision of resources, equipment, training, or other assistance to a cyber group would not, without more, establish that every operation conducted by that group is attributable to the State. The relevant legal inquiry must focus on the relationship between the State and the conduct in question.[25]

This analogy must nevertheless be used carefully. The ICJ was not considering digital infrastructure, technical attribution, or the specific characteristics of contemporary cyber operations. Its judgment provides general principles relevant to the analysis, rather than a complete answer to every question of cyber attribution.

---

[24] *Military and Paramilitary Activities* in and against *Nicaragua (Nicaragua v. United States of America*), Merits, Judgment, 1986 I.C.J. Rep. 14, paras. 109–15 (June 27, 1986). Official ICJ judgment.

[25] International Law Commission, *Draft Articles on Responsibility of States for Internationally Wrongful Acts, with Commentaries*, art. 8 and commentary, U.N. Doc. A/56/10 (2001). Official ILC text and commentaries; *Nicaragua*, 1986 I.C.J. Rep. 14, para. 115. Article 8 concerns conduct carried out on State instructions or under State direction or control; the application of this rule to cyber operations is an application of the general rule, not a specific holding in *Nicaragua*.

4.2 Bosnia and Herzegovina v. Serbia and Montenegro

In Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Bosnia and Herzegovina v. Serbia and Montenegro), the ICJ considered whether acts committed by persons and groups associated with the Federal Republic of Yugoslavia could be attributed to that State.[26] The Court examined the effective-control test applied in Nicaragua and compared it with the broader overall-control approach discussed by the International Criminal Tribunal for the former Yugoslavia (ICTY) in Prosecutor v. Tadić. The ICJ declined to adopt the overall-control test as the general standard for attributing conduct to a State for the purposes of State responsibility. It reaffirmed the requirement of effective control over the relevant conduct.

This distinction is relevant to cyber operations involving groups that receive substantial support or coordination from a State but may retain operational independence. A general relationship between a government and a cyber group may be relevant evidence, but it does not necessarily establish the degree of control required under Article 8 of the Articles on State Responsibility.[27] The effective-control standard should not, however, be misunderstood as requiring a State official personally to perform every technical step of an operation. The question is whether the relevant conduct satisfies the applicable legal test, assessed in light of the evidence and circumstances.

The judgment also demonstrates the importance of distinguishing State responsibility from other legal inquiries. In Tadić, the ICTY's overall-control approach concerned whether an armed conflict was international in character. The ICJ did not accept that test as a substitute for the attribution standard governing State responsibility. The two inquiries serve different legal purposes and should not be treated as interchangeable.[28]

4.3 The Limits of Applying Traditional Jurisprudence to Cyber Operations

The ICJ's decisions provide an established doctrinal foundation for analysing State

[26] *Bosnia Genocide*, 2007 I.C.J. Rep. 43, paras. 385–415. The Court considered, among other issues, whether the acts of Bosnian Serb forces could be attributed to Serbia under the rules of State responsibility.
[27] International Law Commission, *Draft Articles*, supra note 5, art. 8; Bosnia Genocide, 2007 I.C.J. Rep. 43, paras. 398–406. These sources support the distinction between general support and the attribution of specific conduct.
[28] *Bosnia Genocide*, 2007 I.C.J. Rep. 43, paras. 403–06; *Tadić*, Case No. IT-94-1-A, paras. 120–45. The ICJ's discussion expressly distinguished the overall-control approach used by the ICTY for conflict classification from the standard applicable to State attribution.

attribution. However, cyber operations raise evidentiary and technical difficulties that cannot be resolved merely by repeating the applicable legal tests. Digital activity may originate from or pass through infrastructure located in a particular State without establishing that the State itself conducted or directed the operation. The UN Group of Governmental Experts expressly recognised that the location of the originating activity or ICT infrastructure may be insufficient, by itself, to attribute the activity to a State. It also stated that accusations of organising and implementing wrongful acts should be substantiated.[29]

Cyber incidents may also involve several actors and technical systems, making it necessary to distinguish evidence identifying the infrastructure or apparent operator from evidence establishing the legally relevant connection to a State. The UN report recognises the importance of considering the broader context and the challenges of attribution in the ICT environment.[30]

These difficulties do not, by themselves, establish a need for a new substantive attribution standard. They do, however, underscore the importance of applying existing rules carefully and assessing the evidence relevant to the particular case. A public allegation by one State that another State is responsible does not, by itself, establish legal attribution. Conversely, the absence of publicly disclosed technical evidence does not necessarily establish that an attribution is incorrect. The allegation, the evidence available to support it, and the legal standard applicable to State responsibility must be considered separately.

The principal challenge is therefore to maintain the legal discipline of attribution while recognising the distinctive evidentiary environment in which cyber operations occur.

5. Technical Attribution, Political Attribution, and Legal Attribution

5.1 Technical Attribution

Technical attribution concerns identifying the systems, infrastructure, tools, methods, or actors associated with a cyber operation. Investigators may examine malicious software,

[29] U.N. General Assembly, *Report 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, para. 28(f) (July 22, 2015). UN Digital Library record.

[30] Id. para. 28(f). The report recognises attribution challenges in the ICT environment and states that the origin of ICT activity or the location of the infrastructure involved may be insufficient, by itself, to attribute the activity to a State.

network traffic, command-and-control infrastructure, indicators of compromise, operational patterns, and other technical evidence. Such information can help establish how an operation was conducted and may support an assessment of who was involved. However, technical attribution has limitations. Attackers may use compromised third-party systems, reuse tools associated with other actors, or employ techniques intended to obscure the origin of their activity.[31] Consequently, identifying the location from which a cyber operation appears to originate does not necessarily identify the responsible person or State.

Technical findings can be relevant to a legal inquiry, but they do not independently determine legal responsibility.

5.2 Political Attribution

Political attribution occurs when a government publicly identifies another State or actor as responsible for a cyber operation.

Public attribution can serve several purposes, including communicating a security assessment, informing other States, signalling opposition, coordinating diplomatic responses, or explaining a government's policy decision.[32] However, a public attribution statement is not equivalent to a binding judicial determination. Governments may rely on evidence that is not fully disclosed, and their assessments may be disputed by other States.[33]

Political attribution may provide evidence of a State's official position or contribute to an assessment of State practice. Nevertheless, its legal significance depends on the circumstances and the applicable rules. A government cannot establish another State's international responsibility merely by asserting that the State was responsible.[34]

---

[31] *Cyber Attribution: Technical and Legal Approaches and Challenges*, 31 *European Journal of International Law* 941 (2020). Oxford Academic article. These sources discuss the technical methods and limitations involved in tracing malicious cyber activity. The examples in the text should be understood as possible attribution challenges, not as features established in every incident.

[32] Foreign, Commonwealth & Development Office, Application of International Law to States' Conduct in Cyberspace: UK Statement paras. 13–14 (June 3, 2021). Official UK government statement. The statement explains that public attribution involves technical and diplomatic considerations and that the decision to attribute publicly is a matter of policy.

[33] Id. paras. 14–15. The statement distinguishes the decision to make a public attribution from the question of disclosing the information underlying it. This supports the distinction between a governmental attribution and an adjudicated finding; it does not establish that every public attribution is disputed or unsupported.

[34] International Law Commission, *Draft Articles on Responsibility of States for Internationally Wrongful Acts, with Commentaries*, art. 2 and commentary, U.N. Doc. A/56/10 (2001). Official ILC text and commentaries.

5.3 Legal Attribution

Legal attribution concerns whether the conduct satisfies the relevant rules of international law for treating it as an act of a State. It requires the application of the relevant legal standard to the facts. In cases involving State organs, Article 4 of the Articles on State Responsibility may apply. In cases involving entities exercising governmental authority, Article 5 may be relevant. Where non-State actors are involved, Article 8 or another applicable provision may provide the relevant framework.[35]

The distinction between these three forms of attribution is fundamental. Technical attribution may establish facts about the operation's infrastructure, methods, or apparent operators. Political attribution may express a government's assessment. Legal attribution determines whether the conditions established by international law for attributing conduct to a State have been satisfied.

These processes may inform one another, but they are not interchangeable. A cyber incident can be technically investigated and publicly attributed without a final judicial determination of State responsibility.

5.4 The Evidentiary Challenge

The Articles on State Responsibility establish substantive rules for determining State responsibility, including attribution, but do not prescribe a single universal evidentiary procedure for every cyber-attribution decision.[36] The applicable evidentiary requirements may depend on the forum, the legal claim, the nature of the proceedings, and the applicable procedural rules. The ICJ has recognised that the standard of proof may vary with the case and the gravity of the allegations.[37] It would therefore be inaccurate to assert that one universal standard of proof governs every cyber-attribution decision.

Article 2 requires both conduct attributable to the State under international law and a breach of an international obligation for an internationally wrongful act to exist.

[35] Id. arts. 4, 5, 8, 11. These provisions set out distinct rules for attribution of the conduct of State organs, entities exercising governmental authority, persons or groups acting on State instructions or under State direction or control, and conduct subsequently acknowledged and adopted by a State as its own.

[36] International Law Commission, supra note 10, arts. 2–3. These provisions establish substantive elements and the international-law characterisation of wrongful conduct; they do not set out a universal procedural code for evidentiary assessment in all forums.

[37] *Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Bosnia and Herzegovina v. Serbia and Montenegro*), Judgment, 2007 I.C.J. Rep. 43, paras. 209–10 (Feb. 26, 2007). Official

Nevertheless, a State seeking to establish international responsibility must substantiate the relevant factual and legal elements of its claim. Where a dispute reaches an international court or tribunal, the claim must be evaluated in accordance with the applicable procedural framework.

The problem becomes more difficult where relevant evidence consists of classified intelligence or information held by private service providers in different jurisdictions. Cyber-attribution scholarship recognises that States may withhold information to protect intelligence sources, collection methods, or other sensitive capabilities.[38] This creates a tension between the protection of sensitive information and the need to explain the basis of an international legal claim. Greater disclosure may enable independent scrutiny, but the United Kingdom's published position, for example, is that international law does not generally require a State to publicly disclose the underlying information on which its attribution decision rests.

The absence of a general public-disclosure obligation should not be confused with the proposition that evidence is unnecessary. The questions are distinct: one concerns the substantiation of responsibility; the other concerns the extent to which supporting information must be made publicly available.[39]

6. IS THE EXISTING FRAMEWORK ADEQUATE?

6.1 The Case for Retaining Existing Attribution Rules

The existing framework offers general rules capable of applying across different forms of State conduct, including cyber operations. The Articles on State Responsibility distinguish between conduct attributable to State organs, entities exercising governmental authority, non-State actors acting under State instructions or control, and conduct subsequently adopted by

ICJ judgment. The Court discusses burden of proof, standard of proof, and methods of proof, including its requirement of fully conclusive evidence for allegations of exceptional gravity involving genocide. The case does not establish a universal cyber-attribution standard.

[38] *Cyber Attribution: Technical and Legal Approaches and Challenges*, supra note 3. The article discusses how the withholding of attribution methods, sources, or underlying evidence can affect external verification and the assessment of reliability.

[39] U.N. General Assembly, supra note 4, para. 28(f); Foreign, Commonwealth & Development Office, supra note 7, paras. 13–15. The UN report states that accusations of organising and implementing wrongful acts should be substantiated, while the UK statement distinguishes substantiation from a general obligation to disclose the underlying information publicly.

the State.[40]

The framework also distinguishes attribution from breach: a cyber operation's connection to a State does not, by itself, establish that the operation violates international law. Where an internationally wrongful act is established, the Articles address its legal consequences, including cessation and reparation, subject to the applicable conditions.

Accordingly, the technological novelty of cyber operations does not by itself demonstrate that existing attribution rules are inadequate. The key question is whether the rules can be applied coherently to the facts and whether the available mechanisms are sufficient to establish those facts.

6.2 The Case for Clarification and Development

Although the substantive framework remains relevant, its application to cyber operations raises practical concerns. These include how technical evidence should be assessed against legal attribution standards; how indirect State involvement should be evaluated; and how States can cooperate when evidence is held by private companies or authorities in different jurisdictions.[41]

Transparency presents a related challenge. Public explanations may help other States evaluate the legal basis of an attribution claim, while disclosure may be limited by legitimate security and confidentiality concerns. Continued international dialogue can help clarify areas of agreement and disagreement concerning the application of international law to cyberspace. These concerns support further institutional and procedural development, but do not necessarily establish that the existing attribution rules should be replaced.

[40] International Law Commission*, Draft Articles on Responsibility of States for Internationally Wrongful Acts, with Commentaries,* arts. 4–5, 8, 11, U.N. Doc. A/56/10 (2001). Official ILC text and commentaries.

[41] U.N. General Assembly, *Report 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, para. 28(f) (July 22, 2015). Official UN Digital Library record. The report recognises that the origin of ICT activity or the location of infrastructure may be insufficient, by itself, to attribute activity to a State. For the broader international discussion of responsible State behaviour and cooperation, see U.N. General Assembly, *Report of the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security*, U.N. Doc. A/76/135 (July 14, 2021). Official UN Digital Library record.

6.3 The Importance of State Practice

International law concerning cyber operations continues to develop through State practice, official legal statements, multilateral negotiations, and the application of existing rules to particular incidents. Government statements concerning sovereignty, non-intervention, due diligence, the prohibition on the use of force, and State responsibility can help identify States' legal positions.[42]

However, a statement expressing a preferred policy or legal interpretation does not automatically establish a rule of customary international law. Customary law requires a general practice accepted as law.[43] Similarly, UN reports and General Assembly resolutions can provide important evidence of international discussion and agreement, but their significance depends on their content, context, and legal character. A rigorous assessment should therefore distinguish established rules from disputed interpretations and proposals for future development.

7. PROPOSED MEASURES TO IMPROVE ACCOUNTABILITY

7.1 Transparency and International Cooperation

States should, where reasonably possible, provide a reasoned public explanation when attributing a serious malicious cyber operation to another State. Such explanations could identify the legal basis of the attribution and describe the general categories of evidence relied upon, without disclosing sensitive intelligence. This is a recommendation for greater accountability, not a claim that international law generally requires the publication of all supporting intelligence.[44]

International cooperation should also be strengthened to facilitate the preservation and lawful exchange of cyber incident evidence among competent authorities and relevant technical

[42] U.N. Doc. A/76/135, supra note 4; see also U.N. General Assembly, *Developments in the Field of Information and Telecommunications in the Context of International Security,* G.A. Res. 70/237 (Dec. 23, 2015). Official UN Digital Library record. These sources document multilateral consideration of responsible State behaviour in cyberspace. Individual government statements should be assessed separately before drawing conclusions about a particular State's legal position.

[43] Statute of the International Court of Justice art. 38(1)(b). Official ICJ Statute. Article 38(1)(b) refers to "international custom, as evidence of a general practice accepted as law." The assessment of a customary rule therefore requires attention to both State practice and acceptance as law (opinio juris).

[44] UK Foreign, Commonwealth & Development Office, Application of International Law to States' Conduct in Cyberspace: UK Statement ¶¶ 13–15 (June 3, 2021).

or private-sector organisations. Such cooperation should respect applicable international obligations, domestic law, privacy protections, and confidentiality requirements. The location of infrastructure involved in an operation should not, by itself, be treated as proof of the responsibility of the State in which it is located.[45]

7.2 Continued Clarification through the United Nations

The United Nations provides an established forum for discussing the application of international law to information and communications technologies. Further dialogue could clarify how existing rules apply to cyber operations involving State organs, private contractors, proxy groups, and subsequent State adoption of conduct. Such discussions should distinguish clarification of existing law from proposals for new obligations and acknowledge that States continue to differ on some legal questions.

7.3 Separating Attribution from the Legality of a Response

States should distinguish the attribution of a cyber operation from the legal justification for responding to it. Diplomatic measures, retorsion, countermeasures, and self-defence are distinct categories governed by different legal conditions. Countermeasures are subject to requirements including a prior internationally wrongful act, the purpose of inducing compliance, and proportionality; they are not a general authorisation for any response against a suspected State.[46] Self-defence under Article 51 of the UN Charter is governed by its own requirements, including the occurrence of an armed attack. A disputed technical assessment should therefore not be treated, without further legal analysis, as sufficient justification for a particular response.

7.4 Avoiding Premature Claims of International Wrongfulness

Not every harmful or politically hostile cyber operation necessarily violates international law. Its legal character depends on the applicable international obligation and the facts. An operation may raise distinct questions concerning sovereignty, non-intervention, the prohibition on the use of force, international humanitarian law, or human rights law. Each claim

[45] U.N. Secretary-General, Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security, U.N. Doc. A/70/174, ¶ 28(f) (July 22, 2015); U.N. Doc. A/75/816 (Mar. 18, 2021).

[46] Int'l Law Comm'n, Articles on Responsibility of States for Internationally Wrongful Acts, arts. 22, 49–53, U.N. Doc. A/56/10 (2001); UK Statement, supra note 1, ¶¶ 16–17.

must be assessed under the relevant rules rather than inferred solely from technical harm or political hostility.[47]

8. FINDINGS

The study establishes five principal findings:

First, the Articles on State Responsibility provide a general framework applicable to malicious cyber operations.

Second, attribution and breach are distinct requirements: technical evidence linking an operation to an actor does not automatically establish State responsibility, nor does attribution alone prove a violation of international law.

Third, the ICJ judgments in Nicaragua and Bosnia and Herzegovina v. Serbia and Montenegro remain relevant to determining when non-State conduct may be attributed to a State, although their principles must be applied in the context of cyber operations.

Fourth, attribution difficulties arise not only from legal standards but also from challenges in obtaining, verifying, interpreting, and disclosing digital evidence.

Finally, effective accountability requires continued application of existing international law alongside stronger evidence-sharing mechanisms, international cooperation, greater transparency, and multilateral clarification. A new treaty may be warranted if specific legal gaps are demonstrated, but technological complexity alone does not establish the need for an entirely new regime.

9. CONCLUSION

Malicious cyber operations challenge international accountability by making it difficult to identify responsible actors and establish their connections with States. Nevertheless, cyberspace is not beyond the reach of international law. The Articles on State Responsibility, particularly Articles 4, 5, 8 and 11, provide the principal framework for assessing attribution, while the ICJ's decisions in Nicaragua and Bosnia and Herzegovina v. Serbia and Montenegro

[47] U.N. Charter arts. 2(4), 51; *Articles on Responsibility of States for Internationally Wrongful Acts*, supra note 4, arts. 2, 12–15.

offer important guidance on the attribution of non-State conduct.

The study highlights the need to distinguish technical attribution, political attribution, and legal attribution. Technical indicators and governmental allegations may inform an assessment, but legal responsibility depends on applying the relevant international rules to sufficiently established facts. Attribution must also remain separate from determining whether an international obligation has been breached or whether a proposed response is legally justified.

Accordingly, the existing framework should be strengthened through reliable evidence collection, international cooperation, transparent attribution practices where feasible, and continued multilateral dialogue. Any proposal for new legal instruments should address clearly identified gaps rather than presume that existing rules are inadequate. Ultimately, effective cyber accountability depends on the consistent application of international law, sound evidentiary analysis, and responsible State practice.

BIBLIOGRAPHY

I. INTERNATIONAL INSTRUMENTS

1. Charter of the United Nations art. 2(4), June 26, 1945, 1 U.N.T.S. XVI, https://www.un.org/en/about-us/un-charter/full-text (last visited August 06, 2026).

2. Statute of the International Court of Justice art. 38, June 26, 1945, https://www.icj-cij.org/statute (last visited August 06, 2026).

3. G.A. Res. 56/83, annex, Responsibility of States for Internationally Wrongful Acts (Dec. 12, 2001), https://digitallibrary.un.org/record/454412 (last visited September 13, 2026).

II. INTERNATIONAL JUDICIAL DECISIONS

4. Military and Paramilitary Activities in and Against Nicaragua (Nicar. v. U.S.), Judgment, 1986 I.C.J. 14 (June 27), https://www.icj-cij.org/case/70 (last visited August 14, 2026).

5. Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Bosn. & Herz. v. Serb. & Montenegro), Judgment, 2007 I.C.J. 43 (Feb. 26), https://www.icj-cij.org/node/103164 (last visited August 15, 2026).

6. Prosecutor v. Tadić, Case No. IT-94-1-A, Appeals Chamber Judgment (Int'l Crim. Trib. for the Former Yugoslavia July 15, 1999), https://www.icty.org/case/tadic (last visited September 20, 2026).

III. UNITED NATIONS REPORTS AND OFFICIAL DOCUMENTS

7. Int'l Law Comm'n, Draft Articles on Responsibility of States for Internationally Wrongful Acts, with Commentaries (2001), https://legal.un.org/ilc/texts/instruments/english/commentaries/9_6_2001.pdf (last visited September 24, 2026).

8. U.N. Secretary-General, 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), https://digitallibrary.un.org/record/799853 (last visited September 24, 2026).

9. U.N. Secretary-General, Open-Ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security: Final Substantive Report, U.N. Doc. A/75/816 (Mar. 18, 2021), https://digitallibrary.un.org/record/3908015 (last visited October 13, 2026).

IV. BOOKS AND SCHOLARLY ARTICLES

10. Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations (Michael N. Schmitt ed., Cambridge Univ. Press 2017), https://ccdcoe.org/research/tallinn-manual/ (last visited October 13, 2026).

11. Nicholas Tsagourias & Michael Farrell, Cyber Attribution: Technical and Legal Approaches and Challenges, 31 Eur. J. Int'l L. 941 (2020), https://doi.org/10.1093/ejil/chaa057 (last visited October 23, 2026).

12. Andraz Kastelic, Non-Escalatory Attribution of International Cyber Incidents: Facts, International Law and Politics (United Nations Institute for Disarmament Research 2022), https://unidir.org/publication/non-escalatory-attribution-of-international-cyber-incidents-facts-international-law-and-politics/ (last visited October 20, 2026).

V. OFFICIAL GOVERNMENT STATEMENT

13. UK Foreign, Commonwealth & Development Office, Application of International Law to States' Conduct in Cyberspace: UK Statement (June 3, 2021), https://www.gov.uk/government/publications/application-of-international-law-to-states-conduct-in-cyberspace-uk-statement (last visited October 26, 2026).