



Research Article

The Attribution Problem in Cyber Conflict: Implications For Deterrence, International Law and Nigerian Response

Nura Umar Manya Manya, Isa Maina

School of Postgraduate Studies, Institute of Governance and Development Studies, Nasarawa State University, Keffi, Nigeria

Corresponding Author, E-mail; umarmanyamanyanura@gmail.com  (Nura Umar Manya Manya)



Copyright © 2026 by Authors, Published by JUSTICES: Journal of Law. This is an open access article under the CC BY License <https://creativecommons.org/licenses/by/4.0/>

Received : June 13, 2026
Accepted : August 15, 2026

Revised : July 17, 2026
Available online : September 03, 2026

How to Cite: Nura Umar Manya Manya, & Isah Maina. (2026). The Attribution Problem in Cyber Conflict: Implications For Deterrence, International Law and Nigerian Response. *JUSTICES: Journal of Law*, 5(3), 64-78. <https://doi.org/10.58355/justices.v5i3.226>

Abstract. The attribution of malicious cyber operations remains a major challenge to effective deterrence, international legal accountability and national cybersecurity. This study examines the attribution problem in cyber conflict and assesses its implications for deterrence, international law and Nigeria's cybersecurity response. The study adopted a qualitative documentary research design based on systematic analysis of scholarly literature, international legal instruments, policy documents, official cybersecurity reports and selected cyber incidents, including Stuxnet, NotPetya and SolarWinds. Documents were analysed thematically around technical attribution, legal attribution, political attribution, deterrence and Nigeria's institutional capacity. The findings indicate that cyber attribution is rarely a purely technical exercise because attackers can employ compromised infrastructure, proxy networks, false flags and other concealment techniques. Attribution uncertainty weakens deterrence by punishment, complicates the application of state responsibility and creates difficulties in determining appropriate responses under international law. The study further finds that Nigeria has developed important cybersecurity institutions and legal frameworks, but gaps remain in digital forensics, intelligence integration, inter-agency coordination, specialist expertise and

international cooperation. The study concludes that Nigeria should adopt a national cyber-attribution framework integrating technical forensics, intelligence assessment and legal analysis while strengthening regional and international cooperation.

Keywords: Cyber Conflict, Cyber Attribution, Cyber Deterrence, International Law, Cybersecurity, Nigeria, State Responsibility, Digital Forensics, Cyber Warfare.

INTRODUCTION

Cyberspace has become an important domain of contemporary international security, economic activity and political interaction. The increasing dependence of governments, financial institutions, telecommunications systems, energy networks and other critical infrastructures on digital technologies has simultaneously increased the strategic consequences of cyber insecurity. Cyber operations can be conducted remotely, rapidly and across national borders, while the identity and location of the actors responsible may remain uncertain. This combination of connectivity, speed and anonymity creates a distinctive security problem: the difficulty of determining who conducted a cyber operation, whether the operation was state-sponsored, and whether sufficient evidence exists to hold the responsible actor accountable. This challenge is commonly described as the cyber attribution problem. Attribution involves more than identifying the computer or infrastructure from which malicious activity originated. A compromised computer may merely be an intermediary controlled by an attacker, while malware may contain deliberately misleading indicators. Consequently, attribution requires the integration of technical evidence with intelligence, contextual information and, where necessary, legal analysis (Rid & Buchanan, 2015; Lindsay, 2015; Tsagourias & Farrell, 2020). The strategic importance of attribution is illustrated by major cyber incidents. Stuxnet demonstrated the possibility of highly sophisticated cyber operations against strategically important infrastructure. NotPetya demonstrated how an operation directed at one geographical target could generate extensive international disruption. SolarWinds further illustrated the difficulty of identifying sophisticated state-sponsored cyber activity operating through a legitimate software supply chain. The United Kingdom, for example, publicly attributed NotPetya to the Russian government and specifically assessed that the Russian military was responsible. Similarly, United States agencies publicly attributed the SolarWinds compromise to Russia's Foreign Intelligence Service (SVR). Attribution has therefore become closely connected with cyber deterrence. Classical deterrence assumes that an adversary can be identified and that credible consequences can subsequently be imposed. In cyberspace, however, uncertainty concerning the identity of an attacker can make punishment difficult. Lindsay (2015) demonstrates that the attribution problem affects the feasibility of deterrence, while Nye (2017) argues that cyber deterrence should not be reduced to retaliation but should incorporate denial, resilience, norms and other forms of strategic influence. The problem also has an important international legal dimension. Under the law of state responsibility, conduct must satisfy applicable rules of attribution before responsibility can be imposed on a state. The International Law

Commission's Articles on Responsibility of States for Internationally Wrongful Acts provide the principal general framework for state responsibility. Yet cyber operations frequently involve proxies, non-state actors and compromised third-party infrastructure, making it difficult to establish the required connection between an operation and a state.

Africa has increasingly developed its own position on these questions. The African Union Peace and Security Council adopted the Common African Position on the Application of International Law to the Use of Information and Communication Technologies in Cyberspace on 29 January 2024, and the AU Assembly subsequently endorsed it in February 2024. The position addresses sovereignty, due diligence, non-intervention, the use of force, international humanitarian law, human rights and attribution.

For Nigeria, the issue is particularly significant because the country's expanding digital economy and dependence on information and communication technologies increase its exposure to cyber threats. Nigeria's National Cybersecurity Policy and Strategy 2021 identifies governance and coordination, protection of critical national information infrastructure, incident management, legal and regulatory strengthening and capacity development among its strategic priorities. The Cybercrimes (Prohibition, Prevention, etc.) (Amendment) Act 2024 further amended the 2015 cybercrime legislation, including provisions relating to national cybersecurity coordination and sectoral CERTs/Security Operations Centres. Despite these developments, Nigeria's ability to conduct sophisticated attribution remains an important area for further research. Existing Nigerian cybersecurity literature tends to concentrate on cybercrime, financial fraud, cybercrime legislation and general cybersecurity awareness, while comparatively less attention has been given to the intersection between technical attribution, cyber deterrence, international law and Nigeria's national security strategy. This study therefore examines the attribution problem in cyber conflict and its implications for deterrence, international law and Nigeria's cybersecurity response.

Objectives of the Study

The study seeks to:

1. examine the nature and dimensions of the attribution problem in contemporary cyber conflict;
2. Analyse the implications of cyber attribution uncertainty for deterrence and national security;
3. Examine the application and limitations of international legal rules relating to attribution and state responsibility in cyberspace;
4. Assess Nigeria's institutional, legal and technical capacity for cyber attribution;
5. Examine the relevance of the African Union Common African Position to Nigeria's cyber-attribution and international-law posture; and
6. Propose policy measures for strengthening Nigeria's cyber attribution, deterrence and response capabilities.

Research Questions

The study addresses the following questions:

1. What are the principal technical, legal and political challenges associated with cyber attribution?
2. How does attribution uncertainty affect cyber deterrence?
3. To what extent does existing international law provide an adequate framework for attributing cyber operations to states?
4. What institutional and technical capabilities does Nigeria possess for cyber attribution?
5. What gaps exist in Nigeria's cyber-attribution and deterrence architecture?
6. How can Nigeria strengthen its cyber-attribution capacity through national, regional and international cooperation?

METHODOLOGY

Research Design

This study adopted a qualitative documentary research design. The design was selected because the study concerns legal rules, strategic concepts, institutional arrangements, cybersecurity policies and documented cyber incidents rather than variables requiring primary survey or experimental measurement. Documentary research enables researchers to systematically examine existing textual and documentary evidence to understand a phenomenon within its institutional, historical and theoretical context. In this study, the approach was used to integrate evidence from cybersecurity scholarship, international law, government policy documents, international organisations and documented cyber incidents. The study does not claim to establish statistical causality between attribution and deterrence. Instead, it analyses the mechanisms through which attribution uncertainty can influence deterrence, legal accountability and national security decision-making.

Sources of Data

The documentary corpus consisted of five principal categories:

1. Peer-reviewed academic literature: journal articles and scholarly books on cyber attribution, cyber conflict, deterrence and international law.
2. International legal materials: International Law Commission materials, United Nations documents, international judicial decisions and relevant legal instruments.
3. Regional African documents: African Union cybersecurity and international-law instruments, particularly the Common African Position adopted in 2024.
4. Nigerian policy and legal documents: the National Cybersecurity Policy and Strategy 2021, Cybercrimes (Prohibition, Prevention, etc.) Amendment Act 2024 and relevant institutional materials.
5. Documented cyber incidents: Stuxnet, NotPetya and SolarWinds were selected as illustrative cases because they demonstrate different attribution circumstances and strategic consequences.

The Nigerian National Cybersecurity Coordination Centre describes the national cybersecurity architecture as incorporating incident response, digital

forensics and capacity-building functions, demonstrating the institutional importance of these capabilities.

Documentary Selection Criteria

Documents were selected using the following criteria:

- relevance to cyber attribution, cyber conflict, deterrence or international law
- publication by recognized academic, governmental, regional or international institutions
- direct relevance to Nigeria or international cyber-security practice
- sufficient bibliographic information for verification
- Publication within the relevant contemporary period, while retaining seminal earlier works necessary for theoretical and legal foundations.

Documents that were purely promotional, lacked identifiable authorship or did not provide sufficient information for academic verification were excluded.

Method of Data Analysis

The collected documents were subjected to qualitative thematic analysis. Four principal analytical themes were developed:

Theme 1: technical attribution

Theme 2: deterrence and strategic consequences

Theme 3: international law and state responsibility

Theme 4: Nigeria's institutional and policy response

The analysis compared arguments across the literature and examined how the theoretical propositions correspond with documented cyber incidents and Nigeria's policy environment.

Theoretical Framework

The study is principally anchored in Deterrence Theory, complemented by the theory of state responsibility under international law.

Deterrence Theory

Deterrence theory proposes that an actor can discourage an adversary from undertaking undesirable behaviour by threatening consequences or reducing the expected benefits of the behaviour. In cyber conflict, however, the traditional logic of deterrence by punishment is complicated by attribution uncertainty. If the victim cannot confidently identify the attacker, retaliation becomes more difficult and potentially dangerous. Nye (2017) therefore argues for a broader conception of cyber deterrence incorporating deterrence by denial, resilience, norms and punishment. Harknett and Nye (2017) similarly question whether traditional deterrence concepts adequately capture the dynamics of cyberspace.

State Responsibility

The second framework concerns the attribution of conduct to states under international law. The International Law Commission's Articles on State

Responsibility provide rules concerning when conduct may be attributed to a state. In cyberspace, this framework becomes particularly difficult when operations involve proxies, private groups or non-state actors.

The theoretical framework therefore assumes that the effectiveness of cyber deterrence is partly conditioned by the ability to establish credible attribution, while the legal consequences of a cyber operation depend on whether sufficient evidence exists to connect the conduct to a responsible state or other legally relevant actor.

LITERATURE REVIEW

Concept of Cyber Conflict

Cyber conflict refers to hostile or adversarial activities conducted through cyberspace to obtain strategic, political, economic or military objectives. Such activities may include espionage, disruption, sabotage, information manipulation, ransomware and attacks against critical infrastructure.

Cyber conflict differs from conventional conflict because physical distance does not necessarily constrain the attacker. An operation can be launched from one jurisdiction, routed through several others and affect systems located in another country. This geographical complexity contributes directly to the attribution problem. Nye (2017) observes that cyberspace has altered the strategic environment because states can employ cyber capabilities below the threshold traditionally associated with armed conflict. Consequently, the distinction between espionage, criminality, coercion and warfare can become blurred.

Concept of Cyber Attribution

Cyber attribution is the process of determining who conducted or sponsored a cyber operation. Rid and Buchanan (2015) emphasise that attribution should be understood as a multidimensional process rather than merely a technical exercise. Their analysis remains particularly important because attribution can involve technical evidence, intelligence assessment and political judgment.

Technical Attribution

Technical attribution involves examining malware, infrastructure, network traffic, command-and-control systems, timestamps, tactics, techniques and procedures and other digital indicators. However, technical indicators may be manipulated. An attacker may use compromised computers belonging to innocent third parties or deliberately plant misleading indicators.

Legal Attribution

Legal attribution concerns whether the conduct can be legally connected to a state or another actor under applicable international law. This requires consideration of the International Law Commission's rules on attribution and relevant judicial approaches.

Mačák (2016) argues that Article 8 of the Articles on State Responsibility contains important concepts relating to instructions, direction and control when considering conduct of non-state actors.

Political Attribution

Political attribution occurs when a government publicly identifies a suspected perpetrator. Such attribution may be based on classified intelligence that cannot be publicly disclosed. Consequently, political attribution may achieve strategic or diplomatic objectives even when the complete evidentiary basis cannot be revealed.

The Attribution Problem

The attribution problem arises because the apparent source of a cyber operation may not correspond to the actual actor responsible.

- ❖ Attackers may employ
- ❖ compromised servers
- ❖ botnets
- ❖ proxy networks
- ❖ virtual private networks
- ❖ encrypted communications
- ❖ stolen credentials
- ❖ false technical indicators
- ❖ third-party infrastructure
- ❖ False-flag techniques.

Lindsay (2015) demonstrates that the attribution problem is directly relevant to deterrence because uncertainty about the identity of the attacker affects both the probability and credibility of retaliation. Recent scholarship further demonstrates that false flags can deliberately manipulate the attribution process by planting misleading indicators. Baram and Lin's recent study of the Olympic Destroyer case illustrates how deception can influence forensic analysis and political decision-making.

Attribution and Cyber Deterrence

Deterrence by punishment depends heavily on credible attribution. A state cannot reasonably threaten retaliation against an unidentified adversary. This does not mean that attribution makes deterrence impossible. Rather, it means that cyber deterrence requires a broader strategy. Nye (2017) distinguishes among different mechanisms of deterrence and emphasises the importance of denial and resilience in addition to punishment. Lindsay (2015) similarly demonstrates that the relationship between attribution and deterrence is more complex than the simple proposition that anonymity eliminates deterrence.

Therefore, the central strategic implication is that Nigeria should not construct cyber deterrence entirely around retaliatory punishment. Instead, it should develop a layered deterrence model consisting of:

1. deterrence by denial;
2. Deterrence by resilience;
3. Deterrence by intelligence;
4. Deterrence by attribution;
5. Deterrence by lawful punishment; and

6. Deterrence through international cooperation.

International Law and Cyber Attribution

The application of international law to cyberspace has developed significantly, although important uncertainties remain. The International Law Commission's Articles on State Responsibility establish general principles for determining when conduct is attributable to a state. The Nicaragua judgment is particularly important because the International Court of Justice developed the effective-control approach in considering responsibility for conduct involving non-state actors. The ICTY's Tadić jurisprudence subsequently developed an overall-control approach in a different legal context. These approaches should not be treated as interchangeable because they arose in different institutional and legal circumstances. In cyberspace, the difficulty is that a state may employ a proxy actor while maintaining sufficient distance to create plausible deniability. Mačák (2016) identifies instructions, direction and control as important aspects of Article 8 attribution. Tsagourias and Farrell (2020) further demonstrate that cyber attribution involves both technical and legal methodologies and that uncertainty can produce responsibility gaps. Finlay and Payne (2019) likewise argue that attribution is particularly important when determining whether a cyber operation could constitute an armed attack and whether a state may invoke self-defence.

Tallinn Manual 2.0 and Cyber Attribution

The Tallinn Manual 2.0 provides one of the most comprehensive scholarly treatments of international law applicable to cyber operations. It addresses sovereignty, due diligence, jurisdiction, state responsibility and attribution of cyber operations. However, the Tallinn Manual is not a treaty and does not itself create binding international law. It represents expert analysis of how existing international law may apply to cyber operations. This distinction is important for Nigeria because policy-makers should not treat every Tallinn Manual rule as universally accepted law. Rather, the Manual should be used as an important interpretive resource alongside treaties, customary international law, state practice, United Nations processes and the African Union's Common African Position.

African Union Common African Position

A major development for African cybersecurity governance occurred in 2024. The African Union Peace and Security Council adopted the Common African Position on 29 January 2024 and the AU Assembly endorsed it in February 2024. The Common African Position addresses:

1. sovereignty
2. due diligence
3. non-intervention
4. peaceful settlement of disputes
5. prohibition of the use of force
6. international humanitarian law
7. international human rights law

8. attribution

9. Capacity building.

This development is important because it provides African states with a common regional platform for engaging international debates on responsible state behaviour in cyberspace. For Nigeria, the Common African Position creates an opportunity to harmonise national cyber diplomacy, legal interpretation and attribution practices with broader African positions.

Nigeria's Cybersecurity Framework

Nigeria has developed an increasingly sophisticated cybersecurity governance structure. The National Cybersecurity Policy and Strategy 2021 provides a national framework centred on cybersecurity governance, critical national information infrastructure protection, incident management, legal and regulatory frameworks and capacity development. The Cybercrimes Amendment Act 2024 further amended the 2015 Act. Among other changes, it introduced language concerning sectoral CERTs and Security Operations Centres and modified incident-reporting requirements. Nigeria's current institutional architecture also includes the National Cybersecurity Coordination Centre, ngCERT and digital-forensics capabilities. The NCCC identifies incident response, digital forensics and capacity building among its capabilities. These developments demonstrate significant progress. Nevertheless, the existence of institutions and legislation does not automatically guarantee sophisticated attribution capacity.

Challenges to Nigeria's Cyber Attribution Capacity

Several challenges remain.

1. Limited Specialist Capacity

Advanced attribution requires specialists in malware analysis, digital forensics, network intelligence, reverse engineering, threat intelligence and cyber law.

2. Institutional Fragmentation

Cybersecurity responsibilities cut across law enforcement, intelligence, military, telecommunications and regulatory institutions. Without effective information sharing, fragmented institutional responsibilities can reduce attribution speed and accuracy.

3. Technical Infrastructure

Sophisticated attribution requires forensic laboratories, secure intelligence systems, malware-analysis platforms and advanced cyber-threat intelligence capabilities.

4. Intelligence Integration

Technical evidence alone may be insufficient. Nigeria therefore requires mechanisms for integrating technical evidence with intelligence from relevant national security institutions.

5. International Cooperation

Cyber operations routinely cross borders. Nigeria cannot effectively attribute sophisticated foreign cyber operations without cooperation involving foreign governments, technology companies, cybersecurity firms and international organisations.

Empirical Review

The international literature demonstrates substantial scholarly agreement that attribution is central to cyber conflict, but disagreement remains regarding its precise implications for deterrence. Rid and Buchanan (2015) conceptualise attribution as a multidimensional process involving technical, intelligence and political assessments. Lindsay (2015), using a formal model, demonstrates that attribution uncertainty does not simply eliminate deterrence but alters the conditions under which punishment and denial can operate. Nye (2017) argues that cyber deterrence should incorporate denial, resilience, entanglement, norms and punishment rather than simply reproducing Cold War models.

Tsagourias and Farrell (2020) examine the technical and legal dimensions of attribution and identify responsibility gaps created by the difficulty of connecting malicious cyber activities to states. Finlay and Payne (2019) demonstrate the significance of attribution in determining the legal consequences of cyber operations that may reach the threshold of armed attack. Mačák (2016) examines attribution of non-state cyber operations under Article 8 of the Articles on State Responsibility. Recent research further indicates that false flags complicate attribution by intentionally introducing misleading evidence into cyber operations. The literature therefore demonstrates three major findings. First, attribution is inherently multidimensional. Second, attribution uncertainty affects both deterrence and legal accountability. Third, international law has not developed a universally accepted cyber-specific attribution procedure.

Research Gap

Although existing scholarship has examined cyber attribution, deterrence and international law separately, relatively fewer studies integrate the three dimensions within the context of Nigeria. International studies have extensively examined technical attribution, state responsibility and cyber deterrence (Rid & Buchanan, 2015; Lindsay, 2015; Nye, 2017; Tsagourias & Farrell, 2020). Legal scholarship has also analysed the application of the International Law Commission's rules and the Tallinn Manual to cyber operations (Mačák, 2016; Finlay & Payne, 2019). However, a contextual gap remains concerning how these international debates relate to Nigeria's institutional cybersecurity architecture, national security interests and African regional legal position.

This study addresses that gap by integrating:

Cyber Attribution → Deterrence → International Law → Nigerian Institutional Capacity → National Cybersecurity Response.

The study therefore contributes a Nigeria-focused analytical framework that connects technical attribution with strategic deterrence and legal responsibility.

DISCUSSION OF FINDINGS

Attribution Is a Multidimensional Security Process

The study finds that cyber attribution cannot reliably be reduced to identifying an IP address or examining malware characteristics. Technical evidence represents only one component of a broader attribution process.

A credible attribution assessment may require the combination of:

Technical evidence + threat intelligence + behavioural analysis + geopolitical context + human intelligence + legal assessment.

This explains why sophisticated attribution can take considerable time.

Attribution Uncertainty Weakens Deterrence by Punishment

The study finds that attribution uncertainty reduces the credibility of punishment-based deterrence.

Where the identity of the aggressor remains uncertain, a victim state faces three risks:

1. failure to respond;
2. Retaliation against the wrong actor; and
3. Escalation based on inaccurate intelligence.

Therefore, attribution uncertainty can create strategic hesitation.

However, this does not mean that deterrence becomes impossible. Denial and resilience can operate even when attribution remains uncertain.

International Law Contains Attribution Mechanisms but No Cyber-Specific Universal Procedure

The study finds that existing international law provides principles relevant to cyber attribution but does not establish a universally accepted cyber-attribution institution or procedure. The Tallinn Manual contributes significant scholarly guidance, while the Articles on State Responsibility provide the general framework for attribution. However, difficult questions remain regarding proxy actors, standards of evidence, due diligence and the relationship between technical and legal attribution. Tsagourias and Farrell (2020) identify precisely this problem as a source of responsibility gaps.

Nigeria Has Developed Important Cybersecurity Institutions but Requires Stronger Attribution Integration Nigeria has established an important institutional foundation through its national cybersecurity strategy, cybercrime legislation, incident-response mechanisms and digital-forensics capabilities. The principal weakness is therefore not simply the absence of institutions. Rather, the greater challenge is ensuring that technical, intelligence, law-enforcement and diplomatic capabilities are integrated into a coherent national attribution process.

African Regional Cooperation Provides an Opportunity

The AU Common African Position provides Nigeria with a regional framework for developing its cyber diplomacy and international-law posture.

The endorsement of the Common African Position by the AU Assembly provides an important basis for African states to participate more coherently in international cyber governance debates.

Nigeria can therefore use the AU framework to strengthen:

- ❖ regional cyber intelligence sharing
- ❖ legal cooperation
- ❖ cyber diplomacy
- ❖ joint training
- ❖ digital forensic cooperation
- ❖ Coordinated responses to significant cyber incidents.

CONCLUSION

The attribution problem represents one of the central strategic challenges of contemporary cyber conflict. The study demonstrates that attribution is not simply a technical exercise but a multidimensional process involving digital forensics, intelligence assessment, legal analysis and political decision-making. The findings indicate that attribution uncertainty can weaken deterrence by punishment because states may be unable to identify an aggressor with sufficient confidence to justify retaliation. At the same time, the problem does not make deterrence impossible. Deterrence by denial, resilience, intelligence, international cooperation and credible attribution can complement punishment-based approaches. The study further finds that international law provides important principles for addressing cyber responsibility but does not yet provide a universally accepted cyber-specific attribution mechanism. The African Union's Common African Position represents a significant regional development and provides Nigeria with an opportunity to strengthen its position on international cyber law.

Nigeria has made substantial progress through the National Cybersecurity Policy and Strategy 2021, the Cybercrimes Amendment Act 2024 and the development of national cybersecurity coordination and digital-forensics capabilities. Nevertheless, further investment is required in specialist expertise, intelligence integration, forensic infrastructure, inter-agency coordination and international cooperation. The central conclusion is therefore that Nigeria should move from a predominantly incident-response approach toward an integrated national cyber-attribution and deterrence architecture.

RECOMMENDATIONS

1. Establish a National Cyber Attribution Framework: Nigeria should develop a formal national framework specifying procedures for technical, intelligence, legal and political attribution.
2. Strengthen Digital Forensic Infrastructure: Government should increase investment in advanced digital forensic laboratories, malware analysis, threat intelligence platforms and secure evidence-management systems.

3. Establish an Inter-Agency Cyber Attribution Mechanism: Relevant security, intelligence, law-enforcement and cybersecurity institutions should operate through a structured attribution mechanism that facilitates rapid exchange of technical and intelligence information.
4. Develop National Attribution Standards: Nigeria should establish confidence levels and evidentiary thresholds for technical, intelligence and public attribution.
5. Strengthen Cyber Intelligence
 Investment should be increased in cyber threat intelligence, signals analysis, malware intelligence and other capabilities capable of linking technical indicators to responsible actors.
6. Strengthen Public-Private Partnerships: Nigeria should deepen cooperation with telecommunications companies, financial institutions, technology companies and cybersecurity firms because private organisations often possess important technical evidence concerning cyber incidents.
7. Enhance AU and ECOWAS Cooperation: Nigeria should use the AU Common African Position and regional mechanisms to strengthen joint cyber exercises, intelligence sharing, digital-forensics cooperation and legal coordination.
8. Develop Cyber-Diplomatic Capacity: Nigeria should strengthen the capacity of diplomats, lawyers and national-security officials to participate in international negotiations on responsible state behaviour in cyberspace.
9. Adopt a Layered Cyber Deterrence Strategy: Nigeria should combine deterrence by denial, resilience, intelligence, attribution, lawful punishment and international cooperation rather than relying exclusively on retaliation.
10. Establish an Academic-Government Cyber Research Network: Universities, research institutions, cybersecurity agencies and security organisations should collaborate on research into cyber attribution, artificial intelligence, digital forensics, cyber deterrence and international cyber law.

REFERENCES

- African Union. (2014). African Union Convention on Cyber Security and Personal Data Protection (Malabo Convention). African Union.
- African Union. (2024). Common African Position on the Application of International Law to the Use of Information and Communication Technologies in Cyberspace. African Union.
- Baram, G., & Lin, H. (2025). Navigating uncertainty in cyber conflict: Incorporating false flags in the attribution process of offensive cyber operations. *Information, Communication & Society*. <https://doi.org/10.1080/1369118X.2025.2604662>
- Boutin, B. (2019). Shared responsibility for cyber operations. *AJIL Unbound*, 113, 197–201. <https://doi.org/10.1017/aju.2019.31>
- Chircop, L. (2018). A due diligence standard of attribution in cyberspace. *International & Comparative Law Quarterly*.
- Crawford, J. (2002). *The International Law Commission's articles on state responsibility: Introduction, text and commentaries*. Cambridge University Press.

- Efrony, D. (2026). Rethinking the legal status quo in cyberspace to legally attribute state responsibility, and enhance accountability and deterrence. *International Law Studies*, 108.
- Finlay, L., & Payne, C. (2019). The attribution problem and cyber armed attacks. *AJIL Unbound*, 113, 202–206. <https://doi.org/10.1017/aju.2019.35>
- Harknett, R. J., & Nye, J. S., Jr. (2017). Is deterrence possible in cyberspace? *International Security*, 42(2), 196–199. https://doi.org/10.1162/ISEC_c_00290
- International Court of Justice. (1986). Military and paramilitary activities in and against Nicaragua (Nicaragua v. United States of America). ICJ Reports.
- International Law Commission. (2001). Articles on responsibility of states for internationally wrongful acts, with commentaries. United Nations.
- Kadlecová, L. (2018). State responsibility in the cyber age: The course towards indirect evidence. *Czech Journal of International Relations*, 53(4), 35–46. <https://doi.org/10.32422/mv.1585>
- Lindsay, J. R. (2015). Tipping the scales: The attribution problem and the feasibility of deterrence against cyberattack. *Journal of Cybersecurity*, 1(1), 53–67. <https://doi.org/10.1093/cybsec/tyv003>
- Libicki, M. C. (2009). Cyberdeterrence and cyberwar. RAND Corporation.
- Mačák, K. (2016). Decoding Article 8 of the International Law Commission's Articles on State Responsibility: Attribution of cyber operations by non-state actors. *Journal of Conflict and Security Law*, 21(3), 405–428. <https://doi.org/10.1093/jcsl/krw014>
- Nye, J. S., Jr. (2017). Deterrence and dissuasion in cyberspace. *International Security*, 41(3), 44–71. https://doi.org/10.1162/ISEC_a_00266
- Rid, T., & Buchanan, B. (2015). Attributing cyber attacks. *Journal of Strategic Studies*, 38(1–2), 4–37. <https://doi.org/10.1080/01402390.2014.977382>
- Schmitt, M. N. (Ed.). (2017). *Tallinn Manual 2.0 on the international law applicable to cyber operations* (2nd ed.). Cambridge University Press. <https://doi.org/10.1017/9781316822524>
- Tsagourias, N., & Farrell, M. (2020). Cyber attribution: Technical and legal approaches and challenges. *European Journal of International Law*, 31(3), 941–967. <https://doi.org/10.1093/ejil/chaao57>
- United Nations General Assembly. (2001). Responsibility of states for internationally wrongful acts: Resolution 56/83. United Nations.
- United Nations. (2021). Developments in the field of information and telecommunications in the context of international security. United Nations.
- Federal Republic of Nigeria. (2021). National Cybersecurity Policy and Strategy 2021. Office of the National Security Adviser.
- Federal Republic of Nigeria. (2024). Cybercrimes (Prohibition, Prevention, etc.) (Amendment) Act, 2024. Federal Government of Nigeria.
- Manya Manya, N. U., & Maina, I. (2026). Assessment of cybersecurity challenges and their implications for national security in Nigeria. *Interkoneksi: Journal of Computer Science and Digital Business*, 4(1), 191–207. <https://doi.org/10.61166/interkoneksi.v4i1.92>

- Manya Manya, N. U. (2026). The role of private security organizations on national security. *SRAI Journal of Linguistics and Social Sciences*, 6(2), 17–26. <https://doi.org/10.5281/zenodo.21204646>
- Manya, N. U. (2025). Response and efforts at combating terrorism in Nigeria. *Shodh Sari-An International Multidisciplinary Journal*, 4(2), 15–23. <https://doi.org/10.59231/SARI7805>
- Manya Manya, N. U. (2026). The Paradox of Force: A qualitative analysis of armed banditry and its implications for Nigeria's national security (2010–2025). *Academos Journal*, 2(1), 33–43. <https://doi.org/10.65921/9gopvf65>
- Manya-Manya, N. U. (2024). The role of agricultural economy cooperative societies in combating insecurity in Nigeria. *Journal of Fintech, Business, and Development*, 1(1), 7–16. <https://doi.org/10.62762/JFBD.2024.000000>
- Manya Manya, N. U. (2025). The role of Islamic Sharia in safeguarding the rights and lives of non-Muslims in Zamfara State, Nigeria. *MAQOLAT: Journal of Islamic Studies*, 3(4), 525–537. <https://doi.org/10.58355/maqolat.v3i4.215>
- Manya Manya, N. U. (2025). Assessing Nigeria's national livestock policy and its role in enhancing protein security: A qualitative policy and food-security assessment. *Public Management and Service*, 1(1), 32–39. <https://doi.org/10.64229/6wjftau>
- Manya-Manya, N. U. (2023). Prison reforms and national security in Nigeria (2010–2020): A study of Gusau Medium Security Correctional Facility. *ResearchGate*. <https://doi.org/10.13140/RG.2.2.17860.81285>
- Manya-Manya, N. U. (2024). The use of system theory in national system with reference to the behaviour of any country in crisis: A study of Libya. *IOSR Journal of Humanities and Social Science*, 29(10), 6–10.