stratbase INSTITUTE

OCCASIONAL PAPER

JANUARY 2026
ISSUE 19.01

ADVOCATING FOR PHILIPPINE CYBER SOVEREIGNTY AND LEGAL FRAMEWORKS

OCCASIONAL PAPER JANUARY 2026
02

ADVOCATING FOR PHILIPPINE CYBER SOVEREIGNTY AND LEGAL FRAMEWORKS

The Philippines must adopt a National Position on international law in cyberspace and formalize a Cyber Attribution Framework to address escalating cyber threats, strengthen deterrence, protect sovereignty, and enhance its role in shaping global cybersecurity norms

The Philippines stands at a critical inflection point in its cyber sovereignty. As the nation confronts an increasingly hostile cyber threat environment—marked by state-sponsored intrusions, ransomware attacks on critical infrastructure, and persistent espionage campaigns—the absence of a formal National Position on the Application of International Law in Cyberspace and a codified Cyber Attribution Framework leaves the country strategically exposed among the many other holes that the country needs to plug.

This paper advocates for the current administration to (1) adopt and publish a National Position articulating the Philippines' views on how international law applies to State conduct in cyberspace; and (2) formalize a Philippine Cyber Attribution Framework through an Executive Order, institutionalizing the methodology, governance, and decision-making processes for attributing malicious cyber operations.

These measures are not merely technical or bureaucratic—they are strategic imperatives that will strengthen deterrence against state-sponsored cyber threats, enable lawful responses under international law, demonstrate responsible State behavior in UN and ASEAN forums, and protect Philippine sovereignty in the cyber domain.

The time for action is now. The Philippines cannot afford to remain silent while adversaries operate with impunity in our cyberspace.

THE EVOLVING THREAT LANDSCAPE

The Philippines faces a cyber threat environment of unprecedented complexity and severity. State-sponsored actors conduct persistent espionage campaigns against government networks. Criminal organizations deploy ransomware against critical infrastructure. Hacktivist groups target electoral systems.[1] The 2016 COMELEC data breach exposed 55 million voter records. The 2023 PhilHealth ransomware attack compromised sensitive health data of millions of Filipinos.[2] These are not isolated incidents—they are symptoms of a systemic vulnerability.

Yet despite this reality, the Philippines lacks two foundational elements that peer nations have already established.

THE POLICY GAP

The National Security Policy (NSP) 2023-2028 recognizes that: "The Philippines shall ensure the inviolability of its national territory, including land, seas, air, space, and cyberspace."[3]

The NSP further commits the Philippines to: "Building up the country's military capability on cyber defense... in response to the rapidly shifting and continuously evolving international landscape and to ensure cyber sovereignty."[4]

However, these policy commitments remain unfulfilled without the legal and institutional frameworks to operationalize them. Sovereignty without the capacity to defend it is merely aspirational.

PURPOSE OF THIS POLICY PAPER

This paper provides the Marcos Jr. administration with:

1. A compelling case for adopting a National Position on International Law in Cyberspace
2. A detailed framework for formalizing Philippine cyber attribution methodology
3. Actionable recommendations for implementation

WHY THE PHILIPPINES NEEDS A NATIONAL POSITION ON INTERNATIONAL LAW IN CYBERSPACE

THE INTERNATIONAL CONTEXT

The question of how international law applies to cyberspace has been the subject of sustained multilateral deliberation. The UN Group of Governmental Experts (GGE) affirmed in 2013, 2015, and 2021 that:

> *"International law, and in particular the Charter of the United Nations, is applicable and is essential to maintaining peace and stability and promoting an open, secure, stable, accessible and peaceful ICT environment."*[5]

The ongoing UN Open-Ended Working Group (OEWG) 2021-2025 continues to develop norms of responsible State behavior in cyberspace.[6] The Philippines participates in these processes but has not articulated a comprehensive national position.

Among ASEAN Member States, only Singapore has published a comprehensive national position. The Philippines, as a founding member of ASEAN and an active participant in UN cyber discussions, should not lag behind.

STRATEGIC BENEFITS OF A NATIONAL POSITION

The adoption of a National Position on the Application of International Law in Cyberspace delivers immediate and tangible strategic benefits for the Philippines. First and foremost, it provides legal clarity—establishing the doctrinal foundation for determining when cyber operations against Philippine interests constitute violations of international law, whether as breaches of sovereignty, prohibited intervention, or unlawful uses of force. This legal clarity, in turn, unlocks a spectrum of response options previously unavailable or legally ambiguous: from retorsion and diplomatic protests to countermeasures and, in the most severe cases, the exercise of the inherent right of self-defense under Article 51 of the UN Charter. Without a clearly articulated position, the Philippines remains constrained—unable to invoke international law with precision or credibility when responding to malicious cyber operations targeting our critical infrastructure, government systems, or citizens.

TABLE 1 . POLICY GAPS AND CONSEQUENCES IN PHILIPPINE CYBERSECURITY FRAMEWORK

GAP	CONSEQUENCE
No formal National Position on international law in cyberspace	Inability to articulate legal basis for responses; weakened diplomatic posture
No codified attribution framework	Ad hoc, inconsistent attribution processes; limited deterrence capability

SOURCE: AUTHOR'S DATA MANAGEMENT

Beyond the immediate legal and operational benefits, a National Position elevates the Philippines' diplomatic leverage in multilateral forums, particularly the UN Open-Ended Working Group (OEWG) and ASEAN cybersecurity dialogues, where the absence of a formal position has rendered our voice muted and our influence diminished. Equally critical is the deterrence signal such a position transmits: it communicates unambiguously to potential adversaries that the Philippines will identify, attribute, and hold States accountable for malicious cyber conduct—a posture that raises the cost-benefit calculus for those contemplating operations against us. Furthermore, a codified position facilitates alliance coordination with key partners—the United States, Australia, Japan, and other like-minded nations—enabling interoperability in threat intelligence sharing, coordinated attribution, and joint responses. Finally, and perhaps most consequentially for the long term, the Philippines' articulation of its position contributes to norm development from a Global South perspective, ensuring that the rules governing State behavior in cyberspace are not shaped exclusively by major powers but r eflect the interests, values, and strategic realities of developing nations like ours.

CORE ELEMENTS OF A PHILIPPINE NATIONAL POSITION

A Philippine National Position on the Application of International Law in Cyberspace must be anchored on the foundational premise of (1) general applicability—the unequivocal affirmation that international law, including the United Nations Charter, governs State conduct in cyberspace just as it does in the land, sea, air, and outer space domains. This is not a novel or contested proposition; it has been repeatedly affirmed by the UN Group of Governmental Experts and the Open-Ended Working Group, and the Philippines must add its voice to this consensus. Building upon this foundation, the National Position must articulate the Philippines' view on (2) sovereignty as a binding rule of international law—not merely a principle or policy preference—such that cyber operations causing effects on Philippine territory, systems, or persons may constitute violations of sovereignty warranting appropriate response. Equally essential is the principle of (3) non-intervention: cyber operations that coercively interfere in matters within the Philippines' *domaine reserve*[7] [8] —including our electoral processes, governmental functions, and internal political affairs—constitute prohibited intervention under international law, regardless of whether such interference is achieved through kinetic or digital means.

The National Position must further address the critical thresholds governing the (4) use of force and the (5) right of self-defense. The Philippines should adopt the widely accepted "scale and effects" test: cyber operations may constitute a use of force prohibited under Article 2(4) of the UN Charter if their scale and effects are comparable to those of conventional kinetic operations. Where a cyber operation rises to the level of an (6) armed attack—causing destruction, death, or significant physical damage equivalent to a kinetic armed attack—the Philippines reserves its inherent right of self-defense under Article 51, whether exercised individually or collectively with our treaty allies. This position aligns with the views of like-minded States and provides the legal basis for proportionate responses to the most severe cyber threats against our nation. Complementing these principles is (7) State responsibility: under the International Law Commission's Articles on State Responsibility, States bear international responsibility for cyber operations attributable to them, whether conducted by State organs, entities exercising governmental authority, or non-State actors acting under State direction or control.

Finally, the National Position must address three additional principles critical to responsible State behavior in cyberspace. The (8) due diligence obligation requires that States not knowingly allow their territory or cyber infrastructure to be used for cyber operations that cause serious adverse consequences to other States—a principle of particular importance given the transboundary nature of cyber threats and the use of compromised infrastructure across multiple jurisdictions. In the context of armed conflict, International Humanitarian Law (IHL) applies to cyber operations as it does to kinetic operations; the principles of distinction, proportionality, and precaution must govern cyber conduct during hostilities, protecting civilian populations and infrastructure from the effects of cyber warfare. And transcending both peacetime and armed conflict, (9) international human rights law applies online as it does offline—the rights to privacy, freedom of expression, and access to information do not diminish simply because they are exercised through digital means. Together, these nine principles constitute the doctrinal core of a Philippine National Position—a framework that asserts our sovereign rights, defines the boundaries of lawful State conduct, and positions the Philippines as a responsible and credible voice in the ongoing development of international cyber norms.

THE PHILIPPINE CYBER ATTRIBUTION FRAMEWORK: A COMPREHENSIVE PROPOSAL

WHAT IS CYBER ATTRIBUTION?

Attribution is the process of identifying the perpetrator(s) of a cyber operation and, where applicable, establishing State responsibility. As Rid and Buchanan observe:

> *"Attribution is not binary—it is a spectrum of confidence levels based on technical, intelligence, and contextual analysis."*[9]

The Digital Society Foundation (DSF) study on Official Public Political Attribution (OPPA) defines it as:

> *"A government entity's public disclosure of information tying malicious cyber operations to another state through official channels."*[10]

Attribution enables States to:

- Pursue appropriate legal, diplomatic, and operational responses

- Support international cooperation and information sharing
- Contribute to deterrence by demonstrating attribution capability
- Fulfill due diligence obligations under international law
- Inform national security decision-making

CURRENT PHILIPPINE ATTRIBUTION LANDSCAPE

The Philippines currently lacks a formalized attribution framework. Attribution activities are conducted on an ad hoc basis by multiple agencies without standardized methodology or clear decision-making authority, as can be gleaned on Table 2.

The result: Fragmented capabilities, inconsistent methodologies, and no clear authority for public attribution decisions.

LEGAL AND POLICY FOUNDATIONS

The proposed framework builds upon existing legal and policy instruments, as shown in Table 3.

INTERNATIONAL LAW BASIS FOR ATTRIBUTION

Under the ILC Articles on State Responsibility, attribution of cyber operations to a State requires demonstrating that the conduct is:

1. Attributable to the State under international law; and
2. Constitutes a breach of an international obligation of that State

Attribution may be established when cyber operations are conducted by: (see Table 4)

TABLE 2 . CURRENT ROLES AND LIMITATIONS OF PHILIPPINE CYBERSECURITY AGENCIES

AGENCY	CURRENT ROLE	LIMITATIONS
DICT-CICC (Department of Information and Communications Technology-Cybercrime Investigation & Coordination Center)	Cybercrime investigation; incident response	Limited to criminal investigation; no State attribution mandate
PNP-ACG (Philippine National Police-Anti-Cybercrime Group)	Cybercrime investigation	Law enforcement focus; limited international law expertise
NBI-CCD (National Bureau of Investigation-Cyber Crime Division)	Cybercrime investigation	Domestic criminal focus
AFP Cyber Command	Military cyber operations	Defense-focused; limited civilian coordination
NICA (National Intelligence Coordinating Agency)	Intelligence collection and analysis	Expanded mandate under EO 54, s. 2024, but no formal attribution framework
DFA (Department of Foreign Affairs)	Diplomatic engagement	Legal expertise but limited technical capability

SOURCE: AUTHOR'S DATA MANAGEMENT

TABLE 3 . LEGAL AND POLICY INSTRUMENTS GOVERNING PHILIPPINE CYBERSECURITY EFFORTS

INSTRUMENT	ATTRIBUTION-RELEVANT PROVISIONS
RA (Republic Act) 10175 (Cybercrime Prevention Act)	Sec. 10 – Law enforcement authorities; Sec. 21 – Extraterritorial application; Sec. 22 – International cooperation
RA 10844 (DICT Act)	Mandates DICT to coordinate cybersecurity efforts and establish protocols
RA 10173 (Data Privacy Act)	Protection of personal data; relevant to evidence handling
EO 189, s. 2015	Created NCIAC as policy coordination body
EO 95, s. 2019	Reorganized NCIAC; DICT Secretary as Co-Chair with Executive Secretary and the National Security Adviser; authorized Technical Working Groups
EO 54, s. 2024	Expanded NICA mandate to include cyber intelligence; established Cyber Intelligence Directorate
EO 58, s. 2024	Adopted NCSP 2023-2028
NSP 2023-2028	Recognizes cyberspace as domain of national sovereignty; mandates cyber defense capability

SOURCE: AUTHOR'S DATA MANAGEMENT

TABLE 4 . CATEGORIES OF STATE RESPONSIBILITY FOR CYBER OPERATIONS UNDER INTERNATIONAL LAW

CATEGORY	ILC ARTICLE	DESCRIPTION
State organs	Article 4	Conduct of any State organ, regardless of function or position
Delegated authority	Article 5	Persons or entities empowered to exercise governmental authority
Directed or controlled	Article 8	Persons acting on instructions, direction, or control of a State
Acknowledged and adopted	Article 11	Conduct subsequently acknowledged and adopted by a State

SOURCE: AUTHOR'S DATA MANAGEMENT

TABLE 5 . PHILIPPINE ATTRIBUTION METHODOLOGY

PHASE 1	PHASE 2	PHASE 3	PHASE 4
Technical Forensics DICT-CICC AFP/PNP/NBI	**All-Source Analysis** National Intelligence Board (NIB)/National Intelligence Committee (NIC)/National Security Council (NSC)/NICA	**Legal Assessment** Department of Justice (DOJ)/DFA	**Policy Decision** NCIAC[11]/Office of the Executive Secretary/NSC

SOURCE: AUTHOR'S DATA MANAGEMENT

TABLE 6 . KEY ELEMENTS AND INDICATORS FOR TECHNICAL FORENSIC ANALYSIS IN CYBER ATTRIBUTION

ELEMENT	DESCRIPTION	INDICATORS
Malware Analysis	Reverse engineering of malicious code	Code signatures, compiler artifacts, language settings, timestamps
Infrastructure Mapping	Identification of command-and-control (C2) infrastructure	IP addresses, domain registrations, hosting providers, VPN/proxy usage
TTPs Analysis	Analysis of adversary behavior patterns	MITRE ATT&CK framework mapping, operational patterns
Digital Artifacts	Collection and preservation of evidence	Log files, network traffic captures, memory dumps, file metadata
Vulnerability Exploitation	Analysis of exploited vulnerabilities	Zero-day vs. known vulnerabilities, exploitation methods

SOURCE: AUTHOR'S DATA MANAGEMENT

PROPOSED PHILIPPINE ATTRIBUTION METHODOLOGY

The Philippine Attribution Methodology follows a multi-phase, multi-source approach that integrates technical forensics, intelligence analysis, and legal assessment: (see Table 5)

Phase 1: Technical Forensic Analysis
Lead Agencies: DICT-CICC, AFP Cyber Command, PNP Anti-Cybercrime Group, NBI Cybercrime Division (see Table 6)

Phase 2: All-Source Intelligence Analysis
Lead Agency: NICA (Cyber Intelligence Division), in coordination with NIB and NIC members (see Table 7)

Analytical Framework:

The Analysis of Competing Hypotheses (ACH)[12] [13] methodology shall be employed to:

1. Identify potential actors (State actors, State-sponsored groups, criminal organizations, hacktivists, insiders)
2. List evidence and arguments for and against each hypothesis
3. Assess consistency of evidence with each hypothesis
4. Refine hypotheses based on new evidence
5. Assess sensitivity of conclusions to key evidence
6. Report conclusions with confidence levels and caveats

Phase 3: Legal Assessment
Lead Agencies: DOJ, DFA (Office of Legal Affairs) (see Table 8)

Evidentiary Standards Matrix: (see Table 9)

Phase 4: Policy Decision

Lead Bodies: NCIAC, OES, NSC, DICT (see Table 10)

The Technical Attribution Working Group (TAWG) shall prepare an Attribution Assessment Report for consideration by the NCIAC, which shall include:

1. Executive Summary – Key findings and confidence levels
2. Technical Analysis – Summary of forensic findings
3. Intelligence Assessment – All-source analysis and competing hypotheses
4. Legal Assessment – International and domestic law implications
5. Response Options – Recommended courses of action
6. Dissemination Recommendations – Classification level and information-sharing guidance

Decision Matrix: (see Table 10)

DECISION MATRIX FOR CYBER ATTRIBUTION AND RESPONSE

The decision to attribute a cyber operation and determine the appropriate response must be guided by a structured framework that balances confidence level in the attribution assessment against the severity of the incident—ensuring that responses are proportionate, legally defensible, and strategically sound.[14]

When attribution confidence is high and the incident is of critical severity—threatening national security, governmental functions, or the safety of the Filipino people—the full spectrum of response options is warranted: public attribution naming the responsible State or actor, formal diplomatic response through appropriate channels, and where legally justified, the consideration of countermeasures or the exercise of self-defense in accordance with Article 51 of the UN Charter.[15] Where confidence remains high, but the severity is significant—such as attacks on critical infrastructure that do not

TABLE 7 . SOURCE TYPES AND CONTRIBUTING AGENCIES FOR ALL-SOURCE INTELLIGENCE ANALYSIS

SOURCE TYPE	DESCRIPTION	CONTRIBUTING AGENCIES
SIGINT	Signals intelligence	AFP, NICA
HUMINT	Human intelligence	NICA, NBI, PNP
OSINT	Open-source intelligence	All agencies
GEOINT	Geospatial intelligence	AFP, NAMRIA (National Mapping & Resource Information Authority), PhilSA (Philippine Space Agency)
FININT	Financial intelligence	AMLC (Anti-Money Laundering Council), BSP (Bangko Sentral ng Pilipinas
Allied Intelligence	Intelligence from partner nations	NICA, DFA, DND (Department of National Defense)

SOURCE: AUTHOR'S DATA MANAGEMENT

TABLE 8 . LEGAL ASSESSMENT ELEMENTS AND THEIR DESCRIPTIONS

ASSESSMENT ELEMENT	DESCRIPTION
International Law Classification	Determine if the cyber operation constitutes a violation of sovereignty, prohibited intervention, use of force, or armed attack
State Responsibility Analysis	Assess whether the conduct is attributable to a State under ILC Articles
Domestic Law Violations	Identify violations of Philippine law (RA 10175, RA 10173, etc.)
Evidentiary Standards	Evaluate whether evidence meets applicable legal standards
Response Options	Legal assessment of available response options

SOURCE: AUTHOR'S DATA MANAGEMENT

TABLE 9 . EVIDENTIARY STANDARDS MATRIX FOR CYBER ATTRIBUTION AND RESPONSE

PURPOSE	STANDARD	DESCRIPTION
Criminal prosecution	Beyond reasonable doubt	Highest standard; required for domestic or international criminal proceedings
Diplomatic protest	Reasonable basis	Sufficient credible evidence to support a formal diplomatic communication
Countermeasures	Clear and convincing	Evidence must clearly establish the prior wrongful act and the responsible State
Self-defense	Reasonable belief	Evidence sufficient to support a reasonable belief that an armed attack has occurred or is imminent
Public attribution	Preponderance of evidence	Evidence shows it is more likely than not that the attributed actor is responsible

SOURCE: AUTHOR'S DATA MANAGEMENT

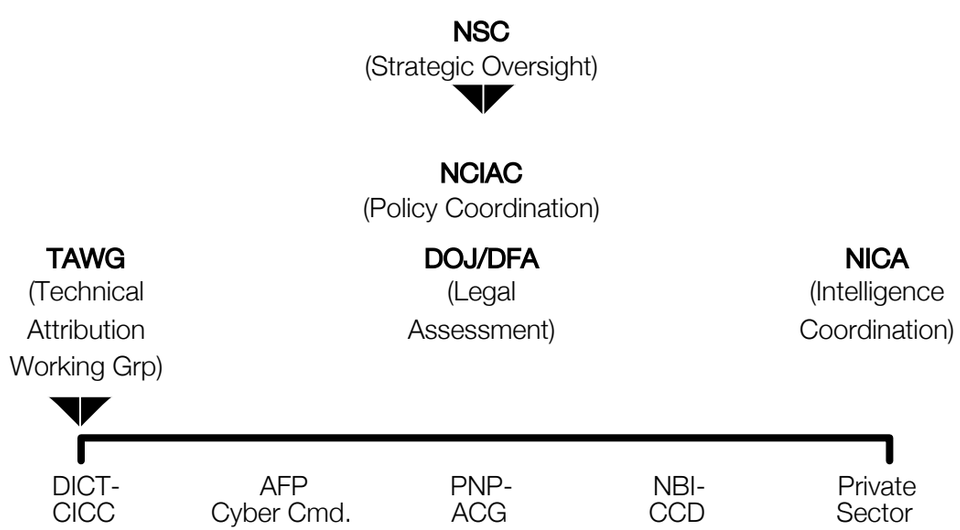
TABLE 10 . DECISION MATRIX FOR CYBER ATTRIBUTION AND RECOMMENDED ACTIONS

CONFIDENCE LEVEL	SEVERITY OF INCIDENT	RECOMMENDED ACTION
High	Critical (national security)	Public attribution; diplomatic response; potential countermeasures/self-defense
High	Significant (critical infrastructure)	Diplomatic engagement; potential public attribution; law enforcement action
Moderate	Critical	Confidential diplomatic engagement; continued investigation
Moderate	Significant	Information sharing with allies; continued investigation
Low	Any	Continued investigation; no public attribution

SOURCE: AUTHOR'S DATA MANAGEMENT

TABLE 10 . DECISION MATRIX FOR CYBER ATTRIBUTION AND RECOMMENDED ACTIONS

ATTRIBUTION GOVERNANCE STRUCTURE



SOURCE: AUTHOR'S DATA MANAGEMENT

rise to the level of national security emergencies—the appropriate response includes diplomatic engagement with the responsible State, potential public attribution where national interest is served, and coordination with law enforcement authorities for investigation and potential prosecution.[16]

When attribution confidence is moderate and the incident is critical, prudence counsels a more measured approach: confidential diplomatic engagement through bilateral or multilateral channels, coupled with continued investigation to strengthen the evidentiary foundation before any public attribution is considered.[17] For incidents of moderate confidence and significant severity, the recommended course of action is information sharing with trusted allies and partners—leveraging collective intelligence capabilities to validate findings—while sustaining investigative efforts to resolve remaining uncertainties. Finally, where attribution confidence remains low, regardless of the severity of the incident, no public attribution should be made; the appropriate action is continued investigation, evidence collection, and coordination with intelligence partners until sufficient confidence is achieved to support a defensible attribution judgment.[18]

This matrix ensures that the Philippines responds to cyber threats in a manner that is calibrated, credible, and consistent with our obligations under international law—avoiding premature attribution that could damage diplomatic relations or undermine our credibility, while ensuring that high-confidence, high-severity incidents receive the decisive response they demand.

INSTITUTIONAL FRAMEWORK FOR ATTRIBUTION

GOVERNANCE STRUCTURE

Technical Attribution Working Group (TAWG)
Establishment: Under the authority of NCIAC pursuant to EO 95, s. 2019 [19]

Functions:

1. Conduct technical forensic analysis of significant cyber incidents
2. Coordinate all-source intelligence analysis with NICA
3. Prepare Attribution Assessment Reports for NCIAC
4. Maintain situational awareness of cyber threat landscape
5. Develop and maintain attribution methodology standards[20]
6. Coordinate with international partners on attribution matters

PUBLIC ATTRIBUTION POLICY

The decision to publicly attribute a cyber operation to a State or State-sponsored actor is among the most consequential determinations a government can make—carrying profound implications for diplomatic relations, international credibility, and the broader normative development of responsible State behavior in cyberspace.[21] Accordingly, the Philippines must establish clear and rigorous criteria governing when public attribution is appropriate. Public attribution should proceed only when confidence is high, grounded in comprehensive technical forensic analysis corroborated by all-source intelligence; when the national interest is served by disclosure—whether to achieve deterrence, demonstrate international solidarity with affected partners, or inform the Filipino public of threats to their security; when diplomatic considerations have been thoroughly assessed, including the potential impact on bilateral relations and the availability of international support for the attribution; when operational security is maintained, ensuring that sources, methods, and intelligence partnerships are protected from compromise; and when legal review confirms that the attribution meets applicable evidentiary standards sufficient to withstand scrutiny in international forums and, where relevant, domestic legal proceedings.[22]

CONCLUSION

The Philippines stands at a crossroads. The cyber domain is now inextricably linked to our national security, our economic prosperity, and the daily lives of 115 million Filipinos. Our critical infrastructure—power grids, telecommunications networks, financial systems, transportation, and government services—depends upon the security and resilience of cyberspace. Yet our legal and institutional frameworks have not kept pace with the threat. We lack a formally articulated position on the application of international law in cyberspace. We lack a comprehensive framework for attributing malicious cyber operations to the States and actors responsible. And we lack the doctrinal clarity necessary to respond—lawfully, effectively, and credibly—when our sovereignty is violated through digital means.

The Marcos Jr. administration has an opportunity—and an obligation—to act. Adopting a National Position on the Application of International Law in Cyberspace will articulate the Philippines' sovereign rights in the cyber domain, provide the legal foundation for proportionate responses to malicious cyber operations, strengthen our voice in the United Nations Open-Ended Working Group and ASEAN regional forums, and demonstrate to the international community that the Philippines is a responsible State committed to a rules-based order in cyberspace.

Formalizing a Philippine Cyber Attribution Framework will enable the identification and accountability of cyber threat actors—whether State-sponsored, criminal, or hacktivist—enhance deterrence by signaling that malicious conduct will not go unanswered, support international cooperation with our allies and partners in collective defense and threat intelligence sharing, and ultimately protect Philippine critical infrastructure and the Filipino people from the escalating dangers of the cyber domain.

The cost of inaction is clear: continued vulnerability to malicious cyber operations, eroded sovereignty as foreign actors operate with impunity against Philippine systems and interests, and diminished credibility in the international community as a nation unable or unwilling to defend itself in the domain that now defines modern statecraft. The path forward is equally clear: decisive action to establish the legal, institutional, and technical foundations for Philippine cyber sovereignty. The time to act is now.

ENDNOTES

[1] GMA News Online. (2016, April 11). 55 million registered voters' data now public. GMA News. https://www.gmanetwork.com/news/topstories/nation/562547/comelec-data-breach-exposes-55-million-voters-personal-information/story/.

[2] Department of Information and Communications Technology. (2023). DICT Statement on PhilHealth Ransomware Incident. Republic of the Philippines. https://dict.gov.ph/.

[3] National Security Council. (2023). National Security Policy 2023-2028, p. 19. Republic of the Philippines. https://nsc.gov.ph/.

[4] Ibid.

[5] United Nations General Assembly. (2015). Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (A/70/174), para. 24. https://documents-dds-ny.un.org/doc/UNDOC/GEN/N15/228/35/PDF/N1522835.pdf.

[6] United Nations Office for Disarmament Affairs. (2023). Open-ended Working Group on security of and in the use of information and communications technologies 2021-2025. https://meetings.unoda.org/open-ended-working-group-on-security-of-and-in-the-use-of-icts-2021-2025.

[7] Domaine réservé (French for "reserved domain") refers to matters that international law recognizes as falling essentially within the exclusive domestic jurisdiction of a State, where external interference—including through cyber means—is prohibited under the principle of non-intervention.1 These reserved matters typically include a State's political system, electoral processes, economic policies, and governmental functions—areas in which each State retains sovereign authority free from coercive external influence.

[8] International Court of Justice. (1986). Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States of America), Merits, Judgment, I.C.J. Reports 1986, p. 14, para. 205. https://www.icj-cij.org/case/70.

[9] 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.

[10] Rupp, C., & Paulus, A. (2023). Official Public Political Attribution of Cyber Operations: State of Play and Policy Options, p. 3. Digital Society Foundation. https://digitalsociety.berlin/.

[11] The National Cybersecurity Inter-Agency Committee, the Philippines' highest policymaking body for cybersecurity.

[12] Analysis of Competing Hypotheses (ACH) is a structured analytical methodology developed by the U.S. Central Intelligence Agency to evaluate multiple potential explanations for observed evidence by systematically assessing the consistency of available data against each hypothesis, identifying which hypotheses are most—and least—supported by the evidence, and explicitly surfacing assumptions, information gaps, and the potential for deception or denial.1 In the context of cyber attribution, ACH enables analysts to rigorously compare competing explanations for a cyber operation—whether attributable to a particular State actor, State-sponsored group, criminal organization, hacktivist collective, or insider threat—by weighing technical forensic indicators, intelligence reporting, and contextual factors against each hypothesis, thereby reducing cognitive bias and enhancing the defensibility of attribution judgments.

[13] Heuer, R. J., Jr. (1999). Psychology of Intelligence Analysis, Chapter 8: Analysis of Competing Hypotheses. Central Intelligence Agency, Center for the Study of Intelligence. https://www.cia.gov/resources/csi/books-monographs/psychology-of-intelligence-analysis-2/

[14] Schmitt, M.N. (Ed.). (2017). Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations (2nd ed.). Cambridge University Press. Rule 6–9 (State Responsibility and Attribution). https://doi.org/10.1017/9781316822524.

[15] United Nations. (1945). Charter of the United Nations, Article 51. https://www.un.org/en/about-us/un-charter/full-text.

[16] International Law Commission. (2001). Draft Articles on Responsibility of States for Internationally Wrongful Acts, Articles 22, 49–54 (Countermeasures). UN Doc. A/56/10. https://legal.un.org/ilc/texts/instruments/english/draft_articles/9_6_2001.pdf.

[17] Efrony, D., & Shany, Y. (2018). A Rule Book on the Shelf? Tallinn Manual 2.0 on Cyberoperations and Subsequent State Practice. American Journal of International Law, 112(4), 583–657. https://doi.org/10.1017/ajil.2018.86.

[18] Rid, T., & Buchanan, B. (2015). Attributing Cyber Attacks.

[19] Office of the President of the Philippines. (2019). Executive Order No. 95, s. 2019: Creating the National Cybersecurity Inter-Agency Committee. Official Gazette of the Republic of the Philippines. https://www.officialgazette.gov.ph/downloads/2019/10oct/20191014-EO-95-RRD.pdf.

[20] NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE). (2022). Tallinn Manual Process. https://ccdcoe.org/research/tallinn-manual/.

[21] Finnemore, M., & Hollis, D.B. (2016). Constructing Norms for Global Cybersecurity. American Journal of International Law, 110(3), 425–479. https://doi.org/10.1017/S0002930000016894.

[22] United Nations General Assembly. (2021). Report of the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security. UN Doc. A/76/135, paras. 71–73. https://documents-dds-ny.un.org/doc/UNDOC/GEN/N21/075/86/PDF/N2107586.pdf.

Picture Credits:

[1] *Cover page: stock.adobe.com/ph: AdobeStock_557389202*

[2] *Page 2: stock.adobe.com/ph: AdobeStock_136375846*

19.01
VOLUME

ABOUT

Francisco Ashley L. Acedillo

most recently served as Deputy Director General for Cyber and Emerging Threats at the Philippines' National Intelligence Coordinating Agency (NICA), where he directed national counterintelligence strategies against cybersecurity threats and weapons of mass destruction. A former Representative during the 16th Congress of the Philippines—ranked among the "Most Productive Partylist Representatives"—he helped pass seven bills into national law, including Republic Act 10844, which created the Department of Information and Communications Technology (DICT). A decorated former military pilot with the Philippine Air Force and he holds a Master of Management degree as W. Sycip GSB full scholar from the Asian Institute of Management and a Bachelor of Science in Management from the Philippine Military Academy, where he was an AGFO (Association of Generals and Flag Officers) awardee

STRATBASE INSTITUTE
is an independent international and strategic research organization with the principal goal of addressing the issues affecting the Philippines, and IndoPacific

The Financial Tower
6794 Ayala Avenue, Makati City
Philippines 1226

V 7005.3779
V 7000.2748

www.stratbase.ph