stratbase INSTITUTE

OCCASIONAL PAPER

AUGUST 2026
ISSUE 19.08

CONVERGENT FOUNDATIONS: THE PHILIPPINES' EMERGING CYBER DEFENSE ARCHITECTURE AND ITS IMPLICATIONS FOR ALLIANCE CREDIBILITY AND REGIONAL SECURITY

OCCASIONAL PAPER AUGUST 2026
02

CONVERGENT FOUNDATIONS: THE PHILIPPINES' EMERGING CYBER DEFENSE ARCHITECTURE AND ITS IMPLICATIONS FOR ALLIANCE CREDIBILITY AND REGIONAL SECURITY

This paper examines the Philippines' evolving cyber defense architecture, highlighting new policies, legislative reforms, and alliance initiatives. It underscores the need for implementation, institutional resilience, and regional cooperation to transform policy convergence into operational capability and strengthen national and Indo-Pacific security.

THE STRATEGIC IMPERATIVE OF CYBER CONVERGENCE

The Philippines is no longer a peripheral actor in Indo-Pacific security competition. Geographic position, alliance value, and the contested waters of the South China Sea have thrust Manila into the center of great-power dynamics. Yet the instruments of competition have evolved. Coercion no longer arrives exclusively in the form of naval vessels or aircraft - it manifests in the disruption of undersea cables, the compromise of government networks, the manipulation of public information ecosystems, and the degradation of logistics and command systems that underpin both civilian governance and military operations.[1]

This paper proceeds from a foundational premise: cyber defense is no longer a technical specialty to be delegated to IT departments; it is a core element of national sovereignty and alliance credibility. A Philippines that cannot defend its networks, protect its critical infrastructure, and sustain communications under pressure is a Philippines that cannot fully exercise sovereignty - and an alliance partner whose vulnerabilities become shared liabilities.

The convergence now underway is both real and fragile. It is real because the policy pieces are finally aligning: the Marcos administration has articulated a clear strategic direction; the legislature has enacted the Self-Reliant Defense Posture (SRDP) Revitalization Act with explicit cyber provisions; the executive has institutionalized the executive has institutionalized the National Cybersecurity Plan (NCSP) through an executive order; and the U.S. Congress has authorized historic levels of security assistance specifically designed to build Philippine resilience. It is fragile because convergence on paper does not automatically produce capability in practice - and because the hardest work of implementation, institutionalization, and sustainment lies ahead.

This paper examines the emerging Philippine cyber defense architecture through three lenses: the domestic policy and legislative foundation, the alliance dimension, and the theoretical framework that explains why this architecture matters for deterrence and regional stability. It concludes with recommendations designed to transform convergence into operational readiness.

THE MARCOS ADMINISTRATION AND THE STRATEGIC RECALIBRATION OF PHILIPPINE SECURITY

FROM HEDGING TO ALIGNMENT

The May 2022 election of President Ferdinand Marcos Jr. marked a decisive inflection point in Philippine foreign and security policy. The preceding Duterte administration had pursued what scholars characterized as a "hedging" strategy – maintaining (albeit barely) the formal alliance with the U.S. while cultivating closer ties with China and, at times, publicly questioning the value of the Mutual Defense Treaty.[2] This approach generated significant uncertainty regarding Philippine strategic orientation and complicated alliance planning.

President Marcos Jr. has charted a different course. While rhetorically maintaining a "friend to all, enemy to none" posture, the administration has in practice moved decisively toward alliance consolidation. The President's repeated assertions that the Philippines "will not give up a single square inch" of territory signal a departure from the ambiguity that characterized the previous government.[3] More substantively, the administration has:

- Approved expanded access to Philippine bases under the Enhanced Defense Cooperation Agreement (EDCA), adding four new sites in 2023;
- Endorsed the Comprehensive Archipelagic Defense Concept (CADC),[4] which reorients the Armed Forces of the Philippines (AFP) toward external defense;
- Elevated the rhetorical and operational priority of South China Sea disputes; and
- Embraced a "whole-of-nation" approach to security that explicitly incorporates cyber and information domains.

CYBERSPACE AS A DOMAIN OF SOVEREIGNTY

The Marcos administration's strategic documents reflect an understanding that sovereignty is defended across multiple domains simultaneously. The CADC envisions a Philippines capable of monitoring, controlling, and defending its archipelagic waters and airspace - but this vision is unachievable without secure, resilient communications and information systems.[5]

This recognition has translated into policy action. Executive Order (EO) No. 58, signed on April 4, 2024, formally adopts the National Cybersecurity Plan 2023–2028 as "the whole-of-nation roadmap for the integrated development and strategic direction of the country's cybersecurity."[6] The order directs all national government agencies and instrumentalities, including government-owned or controlled corporations, to formulate and implement cybersecurity plans aligned with the NCSP. Local government units are encouraged to do likewise. The Department of Information and Communications Technology (DICT) is tasked with establishing an implementation, monitoring, and review system, and must submit bi-annual progress reports to the President through the National Cybersecurity Inter-Agency Committee (NCIAC).[7]

The significance of EO 58 lies not in its creation of new institutions - it does not - but in its transformation of the NCSP from a planning document into a mandatory alignment framework. Government agencies can no longer treat cybersecurity as optional or peripheral; they are now required to demonstrate conformity with a national strategic direction.

DOMESTIC LEGISLATIVE FOUNDATIONS: RA 12024 AND THE SELF-RELIANT DEFENSE POSTURE

THE SRDP REVITALIZATION ACT: CYBER AS AN UNCONVENTIONAL THREAT

Republic Act No. 12024, or the Self-Reliant Defense Posture Revitalization Act, represents the legislative anchor for Philippine defense modernization—and it explicitly incorporates cyber capabilities into the national defense industrial framework.[8]

Section 9 of the Act addresses the development of technology and systems to counter unconventional threats. The statute is unambiguous in its scope:

> *"The SRDP Programs shall include materiel, capital equipment, spare parts and accessories essential to and designed to effectively counter and address chemical, biological, radiological, nuclear, and cyberattacks or incidents."*[9]

The section further mandates that the Department of National Defense (DND), the AFP, and other relevant government agencies enhance the capacity of special units tasked with emergency response and risk mitigation "by promoting technology transfer, and locally sourcing labor and production of materiel, capital equipment, spare parts or accessories."[10]

This provision accomplishes several things simultaneously. First, it classifies cyberattacks alongside chemical, biological, radiological, and nuclear (CBRN) threats as "unconventional" - elevating cyber from a technical concern to a national security contingency. Second, it links cyber capability to the broader defense industrial base, creating a statutory basis for cyber-related procurement, technology transfer, and local production. Third, it emphasizes sustainment: the focus on "spare parts and accessories"[11] signals recognition that cyber capability requires ongoing maintenance, not one-time purchases.

Section 10 extends this framework to emerging technologies:

> *"The DND shall develop programs and projects on emerging and evolving technologies necessary for national defense and security wherever located which shall include, but not be limited to, artificial intelligence, advanced defense equipment, military robotics and autonomous systems, internet of military things, cyber warfare, immersive technologies, additive manufacturing, big data and analytics, independent military 5G connectivity, and blockchain."*[12]

The enumeration is striking. “Cyber warfare” appears explicitly alongside the enabling technologies that modern cyber operations require: AI for threat detection and response, military IoT for networked operations, independent 5G for resilient communications, and big data analytics for situational awareness. The statute thus provides not merely authorization but direction: the DND is mandated to develop programs in these areas.

THE GAP: A NATIONAL CYBERSECURITY AGENCY REMAINS A PROPOSAL

While RA 12024 and EO 58 provide policy direction and defense industrial integration, a critical institutional gap persists. The Philippines lacks a centralized authority with the mandate, resources, and enforcement powers to compel cybersecurity compliance across Critical Information Infrastructure (CII).

A proposed Cybersecurity Act, currently pending in Congress, would address this gap by creating a National Cybersecurity Agency (NCSA) attached to the DICT.[13] [14] The proposed legislation would authorize CII protection, define agency powers, and appropriate dedicated funding. However, as of this writing, the bill has not been enacted.

The absence of an NCSA means that Philippine cybersecurity governance remains fragmented. The DICT holds coordination responsibilities but lacks robust enforcement authority. Sector regulators operate independently. Incident reporting remains inconsistent. Critical infrastructure operators - in telecommunications, energy, finance, and transport - face no mandatory baseline security standards with meaningful consequences for non-compliance.

This gap is not merely administrative. It represents a structural vulnerability that adversaries can exploit and that undermines the effectiveness of both EO 58 and RA 12024. A national cybersecurity plan without an implementing agency risks becoming aspirational; a defense modernization law without civilian infrastructure protection creates a military capability dependent on brittle foundations.

THE ALLIANCE DIMENSION: FROM MUTUAL DEFENSE TO INTEGRATED DETERRENCE

THE BILATERAL DEFENSE PLANNING GUIDELINES

The U.S.-Philippines alliance has undergone its most significant transformation since the post-Cold War retrenchment of the 1990s. The Bilateral Defense Planning Guidelines, released in May 2023 during Secretary of Defense Lloyd Austin’s visit to Manila,formally updated the operational framework of the alliance for contemporary threats.[15]

The Guidelines are notable for several features. First, they explicitly address “all domains” - including cyberspace - as areas requiring interoperability and combined planning. Second, they acknowledge that an armed attack triggering the Mutual Defense Treaty could include attacks conducted through or in cyberspace. Third, they emphasize “deterrence by denial”: the objective of making aggression too costly and too unlikely to succeed, rather than relying solely on the threat of punishment after the fact.[16]

The cyber dimension of the Guidelines reflects a strategic reality: modern military operations depend on networked systems, and those systems are vulnerable. An adversary need not sink a ship to degrade Philippine or allied combat effectiveness; disrupting logistics networks, compromising communications, or manipulating sensor data can achieve similar effects with plausible deniability. The Guidelines acknowledge this by treating cyber resilience as a precondition for alliance effectiveness, not an afterthought.

THE 2+2 MINISTERIAL DIALOGUE: INSTITUTIONALIZING STRATEGIC COORDINATION

The U.S.-Philippines 2+2 Ministerial Dialogue - convening the secretaries of defense and foreign affairs of both countries - has become the premier venue for alliance strategic coordination. The April 2023 dialogue produced commitments to accelerate Philippine defense modernization, enhance interoperability, and deepen cooperation across multiple domains including cyber.[17]

Subsequent dialogues have built on this foundation. The 2024 and 2025 sessions have emphasized:

- Combined exercises incorporating cyber scenarios;
- Information-sharing arrangements for threat intelligence;[18]
- Capacity-building programs focused on critical infrastructure protection; and
- Coordination on supply chain security for defense-relevant technologies.[19]

The 2+2 mechanism matters because it elevates cyber from a technical working-group topic to a ministerial priority. When defense and foreign affairs principals discuss cyber resilience alongside basing access and maritime security, it signals that all three are understood as interconnected elements of alliance credibility.

THE NDAA FY 2026: HISTORIC SECURITY ASSISTANCE

The U.S. National Defense Authorization Act (NDAA) for Fiscal Year 2026 authorizes unprecedented levels of security assistance for the Philippines. The legislation includes approximately USD1.5 billion in security assistance for FY 2026 as part of a broader multi-year package exceeding USD3.5 billion.[20] This funding, substantially driven by the Philippines Enhanced Resilience Act (PERA) provisions embedded within the NDAA, is explicitly designed to build Philippine “deterrence by denial” capabilities.[21]

The implications for cyber defense are significant. NDAA FY 2026 assistance can be directed toward:

- Hardened communications infrastructure;
- Secure logistics and command-and-control systems;
- Cyber defense equipment and training;
- Critical infrastructure protection programs; and
- Interoperability investments enabling combined operations.

Importantly, the NDAA assistance is not a one-time windfall. The multi-year authorization provides a planning horizon that enables the Philippines to design programs with sustainment in mind - addressing the chronic challenge of modernization efforts that acquire capabilities without ensuring their long-term viability.

THEORETICAL FRAMEWORK: DETERRENCE IN THE GRAY ZONE

THE LIMITS OF DETERRENCE BY PUNISHMENT

Classical deterrence theory, rooted in the nuclear standoffs of the Cold War, emphasized deterrence by punishment: the threat of unacceptable retaliation to prevent aggression.[22] This model assumed identifiable attackers, attributable actions, and credible retaliatory capabilities.

Cyber operations challenge each of these assumptions. Attribution is often difficult, delayed, or contested. Many cyber activities fall below the threshold of “armed attack,” complicating legal and policy responses. And the asymmetry between offense and defense - where attackers need find only one vulnerability while defenders must protect everything - undermines confidence in proportionate retaliation.[23]

For countries like the Philippines facing a larger and more capable potential adversary, deterrence by punishment is particularly problematic. Manila cannot credibly threaten to impose equivalent costs on an adversary with greater resources and more extensive cyber capabilities. This asymmetry has led scholars and practitioners to emphasize an alternative framework: deterrence by denial.

DETERRENCE BY DENIAL AND THE RESILIENCE IMPERATIVE

Deterrence by denial operates through a different logic: rather than threatening retaliation, it aims to convince adversaries that their operations will not succeed.[24] If a potential attacker concludes that

Philippine networks are sufficiently hardened, monitored, and resilient - that disruptions will be detected quickly, contained effectively, and restored rapidly - the expected utility of cyber coercion declines.

Stephen Mazarr and his colleagues at RAND have argued that denial strategies are particularly relevant for gray-zone competition, where adversaries pursue incremental gains through ambiguous, deniable actions designed to stay below thresholds that would trigger decisive responses.[25] In this context, resilience becomes a form of deterrence: the ability to absorb, adapt, and recover from disruption reduces the coercive leverage that cyber operations provide.

For the Philippines, this framework suggests that cyber defense is not merely about preventing intrusions - it is about demonstrating that intrusions will not achieve their intended effects. This requires:

- Visibility: the ability to detect malicious activity promptly;
- Hardening: baseline security controls that raise the cost and complexity of successful attacks;
- Segmentation: architectures that limit the blast radius of successful compromises;
- Redundancy: backup systems and processes that enable continuity of operations;
- Recovery: tested, exercise-simulated restoration capabilities that minimize downtime; and
- Communication: the ability to maintain credible public messaging during and after incidents.

INTEGRATED DETERRENCE AND ALLIANCE VALUE

The U.S. government's concept of "integrated deterrence" extended the denial framework to alliance relationships.[26] Deterrence is strengthened when adversaries face not a single defender but a coalition with complementary capabilities, shared intelligence, and coordinated responses. An attack on Philippine networks becomes more costly if it triggers alliance mechanisms, engages U.S. capabilities, and generates broader international consequences.

For integrated deterrence to function in cyberspace, however, alliance partners must have achieved genuine interoperability. This required:

- Compatible technical standards for systems that must connect during operations;
- Shared procedures for incident coordination and information sharing;
- Combined exercises that test and refine joint responses; and
- Mutual understanding of thresholds, escalation dynamics, and decision-making processes

The Bilateral Defense Planning Guidelines and 2+2 Dialogue outcomes reflected movement in this direction. But interoperability is not achieved through declarations; it is built through practice. The Philippines and the U.S., therefore, must continue to translate policy commitments into operational routines.

THE OPERATIONAL REALITY: GAPS BETWEEN POLICY AND CAPABILITY

THE AFP CYBER COMMAND: NASCENT INSTITUTIONALIZATION

The elevation of cyber to a dedicated command within the AFP represents institutional recognition that cyber is not merely a support function - it is operational one. However, a Cyber Command does not automatically produce cyber power.

The AFP Cyber Command faces the same challenges that confront cyber organizations globally: doctrine development, force generation, talent acquisition and retention, and integration with conventional operations.[27] Specific gaps include:

- Doctrine: The command requires clear articulation of missions, authorities, and integration with intelligence, communications, and joint operations.
- Personnel: Cyber forces cannot be surged. They require years of training and experience to reach proficiency. Recruitment competes with private sector opportunities; retention requires career paths and incentives that government salary structures often cannot match.
- Training infrastructure: Realistic preparation requires cyber ranges, simulation environments, and exercise programs that allow operators to practice without risking operational networks.
- Sustainment: Tools and capabilities require continuous updating. A cyber capability procured in 2025 may be obsolete by 2027 without sustained investment in maintenance, upgrades, and adaptation.

CRITICAL INFORMATION INFRASTRUCTURE: THE UNDEFENDED FLANK

Perhaps the most significant vulnerability lies outside military networks. Philippine Critical Information Infrastructure (CII) - telecommunications, energy, financial services, transportation, water systems, and healthcare - operates largely without mandatory security baselines or regulatory enforcement.[28] [29] [30]

The proposed Cybersecurity Act would address this gap by empowering an NCSA to designate CII, establish security requirements, mandate incident reporting, and conduct compliance audits. Without such legislation, CII protection remains a matter of voluntary best practices - which, experience suggests, produces uneven results.

The consequences of CII vulnerability extend beyond individual sectors. A disruption to telecommunications affects everything that depends on communications. A compromise of energy systems cascades to all sectors requiring electricity. Financial system disruptions undermine economic stability and public confidence. In a crisis, these interdependencies become force multipliers for adversary coercion.

THE IMPLEMENTATION DEFICIT

Across all dimensions - EO 58 compliance, SRDP utilization, Cyber Command development, and CII protection - the Philippines faces a common challenge: implementation.

Philippine governance has historically struggled with follow-through. Plans are adopted but not resourced. Laws are enacted but not enforced. Institutions are created but not empowered. This pattern poses a particular risk for cybersecurity, where capability depends on continuous, disciplined execution rather than episodic initiatives.

The bi-annual reporting requirement in EO 58 provides a mechanism for accountability - but only if reports are substantive, if non-compliance carries consequences, and if the political will exists to act on findings. The SRDP's cyber provisions provide statutory authority - but only if procurement programs are designed for sustainment, technology transfer produces genuine capability, and local production is economically viable rather than performative.

REGIONAL IMPLICATIONS: PHILIPPINE CYBER RESILIENCE AS A PUBLIC GOOD

The Philippines' cyber defense posture is not merely a domestic concern. In an interconnected region, vulnerabilities in the Philippines create risks that extend beyond national borders.

SUPPLY CHAIN INTERDEPENDENCIES

The Philippines occupies a significant position in regional and global supply chains. Disruptions to Philippine logistics, ports, or communications systems affect trade flows throughout Southeast Asia and beyond. Cyber incidents that degrade these systems impose costs on regional partners and trading relationships.[31]

ALLIANCE CREDIBILITY AND REGIONAL STABILITY

The credibility of the U.S.-Philippines alliance has implications for the broader Indo-Pacific security architecture. If the Philippines is perceived as the weak link - unable to sustain operations, protect shared information, or maintain communications during a crisis - the deterrent value of the alliance diminishes. Conversely, a Philippines that demonstrates cyber resilience reinforces the message that alliance commitments are operationally meaningful.[32]

DEMONSTRATION EFFECTS

How the Philippines addresses its cyber challenges will be observed by other regional states facing similar dilemmas. Success in building effective CII protection, professionalizing cyber forces, and operationalizing alliance cooperation could provide a model for ASEAN partners. Failure would reinforce perceptions that cyber governance in developing democracies is inherently fragmented and ineffective.

CONCLUSION: THE STAKES OF CONVERGENCE

The Philippines has arrived at a moment of genuine opportunity. The policy foundations are stronger than at any previous point: EO 58 provides executive direction; RA 12024 integrates cyber into defense industrial planning; the Bilateral Defense Guidelines and 2+2 Dialogue embed cyber in alliance frameworks; and NDAA FY 2026 offers historic resources.

But opportunity is not outcome. The convergence of policy instruments creates potential that can be realized or squandered depending on implementation choices over the coming years. Five conclusions emerge from this analysis:

First, cyber defense has become inseparable from national sovereignty. The Philippines cannot fully exercise sovereignty - over its territory, its maritime zones, or its information environment - if its networks are vulnerable to disruption and manipulation. This is not a technical observation; it is a strategic reality that should inform resource allocation and institutional priorities.

Second, the alliance dimension is now essential to Philippine cyber defense. The Philippines lacks the resources and capabilities to build comprehensive cyber resilience independently. Alliance cooperation - through interoperability, capacity building, intelligence sharing, and combined exercises - is not a luxury but a necessity. However, alliance value depends on Philippine contributions: a partner that cannot sustain basic cyber hygiene becomes a liability rather than an asset.

Third, legislation matters. The absence of a National Cybersecurity Agency leaves a critical institutional gap that executive action cannot fully address. Until Congress enacts legislation creating an NCSA with adequate authorities and resources, Philippine cybersecurity governance will remain fragmented, voluntary, and ultimately inadequate.

Fourth, military cyber capability requires sustained investment in people, not just technology. The AFP Cyber Command will succeed or fail based on its ability to recruit, train, and retain skilled personnel - and to integrate cyber into the broader joint force. This requires career paths, compensation structures, training infrastructure, and doctrinal clarity that cannot be achieved through procurement alone.

Fifth, implementation is the decisive variable. The Philippines has demonstrated the ability to produce impressive policy documents. It has less consistently demonstrated the ability to translate policy into sustained operational capability. The coming years will test whether the current convergence produces genuine resilience or merely another chapter in the national tradition of elaborate planning without follow-through.

RECOMMENDATIONS

Based on the foregoing analysis, this paper offers five actionable recommendations:

Recommendation 1: Operationalize the National Cybersecurity Plan 2023–2028 Through Enforceable Compliance Mechanisms

EO 58 requires agency alignment with the NCSP but does not specify consequences for non-compliance. The DICT should develop and publish:

- Measurable indicators for each NCSP objective;
- Agency scorecards reported through the bi-annual reporting process;
- Escalation procedures for persistent non-compliance; and
- Budget alignment requirements linking cybersecurity planning to ICT appropriations

The bi-annual reports to the President should be substantive assessments, not bureaucratic formalities. Agencies failing to meet NCSP baselines should face consequences ranging from public identification to budget restrictions for non-essential ICT expansion.

Recommendation 2: Implement RA 12024 Cyber Provisions Through Sustainment-First Procurement

The DND should establish procurement guidelines for SRDP cyber-related programs that prioritize:

- Lifecycle sustainment plans including spares, updates, maintenance, and training;
- Technology transfer requirements with measurable outputs (certifications, local maintenance capability, documentation);
- Interoperability standards ensuring compatibility with alliance systems; and
- Realistic total cost of ownership (TCO)[33] assessments rather than acquisition cost alone

Pilot programs under Section 10 of the SRDP law should focus on capabilities where local sustainment provides genuine strategic value: secure communications, cyber range development, and incident response tooling.

Recommendation 3: Expedite Passage and Funding of Legislation Creating a National Cybersecurity Agency

Congress should prioritize the enactment of the pending Cybersecurity Act with provisions that:

- Establish the NCSA as an attached agency to DICT with operational independence;
- Grant authority to designate CII across sectors;
- Mandate baseline security requirements for CII operators with audit and enforcement powers;
- Require incident reporting within defined timelines with appropriate confidentiality protections;
- Appropriate multi-year funding sufficient for staffing, technical capabilities, and operations; and
- Create a career civil service track for cybersecurity professionals with competitive compensation.

The NCSA should be designed for effectiveness rather than bureaucratic expansion - focused on standard-setting, compliance monitoring, incident coordination, and technical assistance rather than attempting to centralize all cybersecurity functions.

Recommendation 4: Accelerate Institutional Maturation of the AFP Cyber Command

The DND and AFP should:

- Develop and publish cyber operations doctrine defining missions, authorities, and joint integration;
- Establish cyber-specific career tracks with training requirements, promotion criteria, and retention incentives;
- Invest in training infrastructure including dedicated cyber ranges and simulation capabilities;
- Conduct recurring internal exercises and participate in combined exercises with allies;
- Create reserve and auxiliary programs to expand the available talent pool; and
- Define clear requirements and programming for SRDP and NDAA FY 2026 funding relevant to cyber capability development

The Cyber Command should be evaluated not by organizational charts but by operational readiness metrics: detection rates, response times, exercise performance, and personnel retention.

Recommendation 5: Strategically Utilize NDAA FY 2026 Security Assistance for Sustainable Cyber Resilience

The Philippines should approach NDAA FY 2026 assistance not as a procurement opportunity but as a capability-building program. Priority investments should include:

- Hardened communications infrastructure for military and government use;
- Interoperable command-and-control systems compatible with alliance networks;
- CII protection programs developed jointly with the private sector;
- Combined exercise programs with U.S. Cyber Command and Indo-Pacific Command;
- Training and professional development for AFP Cyber Command personnel; and
- Technical assistance for NCSA establishment and CII baseline development.

Utilization planning should emphasize sustainment from the outset, ensuring that capabilities acquired with NDAA assistance can be maintained, updated, and operated independently over time.

STRATEGIC ACTION PLAN

To transition the architecture from a performative policy alignment into an operational capability for the remainder of the Marcos Jr. administration, the following specific lines of effort and must be executed:

Line of Effort 1: Legal Enforceability & CII Hardening (Immediate)

- Action: Issue an administrative joint circular between the DICT and sector regulators utilizing existing regulatory mandates to enforce the NCSP 2023–2028 baselines as a condition of utility franchise retention.

- Integration with Recommendation 1: Operationalize the NCSP 2023–2028 through enforceable compliance mechanisms. The DICT should develop measurable indicators, agency scorecards, escalation procedures, and budget alignment requirements.

- Integration with Recommendation 3: Expedite passage and funding of legislation creating a National Cybersecurity Agency (NCSA). Congress should establish the NCSA as an attached agency to DICT with operational independence, granting authority to designate CII across sectors and mandate baseline security requirements with audit and enforcement powers.

- Metric for Success: 100% of designated Tier-1 CII operators subjected to independent, third-party cybersecurity audits by Q3 2027.

Line of Effort 2: Alliance Fund Architecture Optimization

- Action: Establish a dedicated Project Management Office (PMO) within the DND to oversee NDAA FY 2026 funds (USD1.5 billion allocation). Transition all procurement lines to a “Sustainment-As-A-Service” (Sus-a-a-S) model, mandating 5-year vendor lifecycle maintenance and configuration management within every contract.

- Integration with Recommendation 5: Strategically utilize NDAA FY 2026 security assistance for sustainable cyber resilience. Priority investments should include hardened communications infrastructure, interoperable C2 systems, and CII protection programs developed jointly with the private sector.

- Metric for Success: Obligation of 90% of cyber-allocated NDAA funds under legally binding long-term sustainment terms by Q2 2027.

Line of Effort 3: Asymmetric Force Preservation & Talent Retention

- Action: Leverage the reorganization provisions of the AFP to create a distinct, non-traditional civil-military cyber-reserve pipeline. Establish a system where private sector Tier-1 specialists are commissioned directly into the AFP Cyber Command reserve force for short-term rotational deployments (e.g., 30-day active-duty operational stints).

- Integration with Recommendation 4: Accelerate institutional maturation of the AFP Cyber Command. Establish cyber-specific career tracks with retention incentives, invest in dedicated cyber ranges, and create reserve and auxiliary programs to expand the available talent pool.

- Metric for Success: Standing roster of 250 active cyber reservists integrated into daily joint security operations center (JSOC) shifts by Q1 2028.

Line of Effort 4: Technical Interoperability & Supply Chain Security

- Action: Institutionalize a mandatory National Supply Chain Security standard for all procurement under Sections 9 and 10 of RA 12024. No defense-relevant digital asset may be procured without an audited, verified Software Bill of Materials (SBOM) and automated binary analysis.

- Integration with Recommendation 2: Implement RA 12024 cyber provisions through sustainment-first procurement. Prioritize lifecycle sustainment plans, technology transfer requirements with measurable outputs, and interoperability standards ensuring compatibility with alliance systems.

- Metric for Success: Zero un-vetted firmware deployments across the AFP Cyber Command and DND networks by mid-2028.

“THE PHILIPPINES IS CONSTRUCTING A CYBER DEFENSE ARCHITECTURE. THAT ARCHITECTURE - COMPRISING EO 58, RA 12024, ALLIANCE FRAMEWORKS, AND PROPOSED LEGISLATION - CREATES THE STRUCTURAL CONDITIONS FOR CAPABILITY...”

IMPLEMENTATION TIMELINE MATRIX

Target Milestone	Strategic Objective	Responsible Entity	Verification Mechanism
December 2026	Establishment of the RA 12024 Supply Chain Review Board	DND / DICT	Mandatory SBOM submission protocols operational for all defense tech bids.
June 2027	Completion of Joint US-PH Cyber Interoperability Framework	AFP Cyber Command / U.S. Cyber Command	Successful execution of bilateral live-fire cyber exercises with synchronized C2 nodes.
December 2027	Comprehensive CII Audit & Enforcement Campaign	DICT / Sector Regulators	Penalties or formal notices issued to non-compliant critical infrastructure operators.
June 2028	Full Operational Capability (FOC) of the Integrated JSOC	AFP Cyber Command	Continuous 24/7/365 active threat exposure management across all defense domains.

CLOSING REFLECTION: ARCHITECTURE IS NOT DESTINY

The Philippines is constructing a cyber defense architecture. That architecture - comprising EO 58, RA 12024, alliance frameworks, and proposed legislation - creates the structural conditions for capability. But architecture is not capability, and capability is not resilience.

Resilience is built through the unglamorous disciplines: continuous threat mitigation, training operators, exercising responses, auditing compliance, retaining talent, and learning from failures. It is built through institutional cultures that value security as a continuous practice rather than a checkbox requirement. It is built through leadership that prioritizes implementation over announcement.

The foundations are converging. The question for the Philippines - and for its allies - is whether this convergence will produce a cyber defense posture adequate to the challenges ahead, or whether it will become another monument to plans that looked impressive on paper.

The window is open. It will not stay open indefinitely.

ENDNOTES

[1] Poling, G. B., & Hudes, S. T. (2023, April 11). Deepening the U.S.-Philippines alliance. Center for Strategic and International Studies. https://www.csis.org/analysis/deepening-us-philippines-alliance.

[2] De Castro, R. C. (2018). The Duterte administration's appeasement policy on China and the crisis in the Philippine–US alliance. Asian Affairs: An American Review, 45(3–4), 167–191. https://doi.org/10.1080/00927678.2019.1589664.

[3] Philippine News Agency. (2023, January 23). Marcos says PH won't give up 'single square inch' of territory to any foreign power. https://www.pna.gov.ph/articles/1193557.

[4] Javier, E. N. (2025). Signaling resolve: CADC and Philippine deterrence (Executive Policy Brief No. 2025-05). National Defense College of the Philippines. https://ndcp.edu.ph/wp-content/uploads/2025/09/EPB-2025-05-Signaling-Resolve-CADC-and-Philippine-Deterrence.pdf

[5] Department of National Defense. (2025, December 5). DND launches department circular on IT and cybersecurity standards to strengthen defense-wide cyber resilience [Press release]. https://www.dnd.gov.ph/Release/2025-12-05/2549/DND-Launches-Department-Circular-on-IT-and-Cybersecurity-Standards-to-Strengthen-Defense-Wide-Cyber-Resilience/.

[6] Executive Order No. 58, Adopting the National Cybersecurity Plan 2023–2028, and Directing the Implementation Thereof (2024). https://www.officialgazette.gov.ph/2024/04/04/executive-order-no-58-s-2024/.

[7] Department of Information and Communications Technology. (2024). National Cybersecurity Plan 2023–2028. Republic of the Philippines. https://cms-cdn.e.gov.ph/DICT/pdf/NCSP-2023-2028-FINAL-DICT.pdf.

[8] Republic Act No. 12024, Self-Reliant Defense Posture (SRDP) Revitalization Act (2024). https://www.senate.gov.ph/republic_acts/ra%2012024.pdf.

[9] Republic Act No. 12024, § 9 (2024).

[10] Ibid.

[11] "Spare parts" in a cyber defense sense would mean license renewals, subscription feeds, and patching pipelines - the consumables that keep defensive systems current and functional.

[12] Republic Act No. 12024, § 10 (2024).

[13] Philippine News Agency. (2024, September). House panel OKs bill creating National Cybersecurity Agency. https://www.pna.gov.ph/articles/1232847.

[14] While House Bill (HB) 2026 proposes to create the NCSA under the DICT, the author is of the position that the NCSA and the Director General must operate independently of the DICT and its Secretary, to provide the necessary bifurcated check-and-balance similar to that of the Chief Information Security Officer (CISO) being independent of the Chief Information or Chief Technology Officer (CIO/CTO).

[15] U.S. Department of Defense. (2023, May 3). The United States and the Republic of the Philippines bilateral defense guidelines. https://media.defense.gov/2023/May/03/2003214357/-1/-1/0/THE-UNITED-STATES-AND-THE-REPUBLIC-OF-THE-PHILIPPINES-BILATERAL-DEFENSE-GUIDELINES.PDF.

[16] U.S. Department of Defense. (2023, May 3). The United States and the Republic of the Philippines bilateral defense guidelines (pp. 2–3).

[17] U.S. Department of State. (2023, April 11). Joint statement of the U.S.-Philippines 2+2 ministerial dialogue. https://www.state.gov/joint-statement-of-the-u-s-philippines-22-ministerial-dialogue/.

[18] The November 2024 visit marked Secretary Austin's fourth trip to the Philippines and resulted in the signing of the General Security of Military Information Agreement (GSOMIA) and groundbreaking for the Combined Coordination Center. See U.S. Department of War. (2024, November 19). Joint press release on the visit of U.S. Secretary of Defense Austin to the Philippines. https://www.war.gov/News/Releases/Release/Article/3970660/joint-press-release-on-the-visit-of-us-secretary-of-defense-austin-to-the-phili/

[19] U.S. Embassy in the Philippines. (2024). Joint statement on the Philippines-United States bilateral strategic dialogue. https://ph.usembassy.gov/joint-statement-on-the-philippines-united-states-bilateral-strategic-dialogue/.

[20] LaGrone, S. (2025, December 18). Philippines could receive $2.5 billion in security aid from U.S. defense bill. USNI News. https://news.usni.org/2025/12/18/philippines-could-receive-2-5-billion-in-security-aid-from-u-s-defense-bill.

[21] BusinessMirror. (2025, December 22). PHL secures historic $3.5-B U.S. defense aid via NDAA 2026. https://businessmirror.com.ph/2025/12/22/phl-secures-historic-3-5-b-u-s-defense-aid-via-ndaa-2026/.

[22] Schelling, T. C. (1966). Arms and influence (pp. 69–91). Yale University Press. https://www.jstor.org/stable/j.ctt1nhrj7.

[23] Nye, J. S., Jr. (2017). Deterrence and dissuasion in cyberspace. International Security, 41(3), 44–71. https://doi.org/10.1162/ISEC_a_00266.

[24] Snyder, G. H. (1961). Deterrence and defense: Toward a theory of national security (pp. 14–16). Princeton University Press. https://www.jstor.org/stable/j.ctt183pzm5.

[25] Mazarr, M. J., Heath, T. R., Cevallos, A. S., & Greer, S. (2018). Understanding the emerging era of international competition: Theoretical and historical perspectives. RAND Corporation. https://www.rand.org/pubs/research_reports/RR2726.html.

[26] U.S. Department of Defense. (2022). 2022 national defense strategy of the United States of America (pp. 8–9). https://media.defense.gov/2022/Oct/27/2003103845/-1/-1/1/2022-NATIONAL-DEFENSE-STRATEGY-NPR-MDR.PDF.

[27] Grossman, D. (2023, May). The U.S.-Philippines alliance is back. RAND Blog. https://www.rand.org/blog/2023/05/the-us-philippines-alliance-is-back.html.

[28] Department of Information and Communications Technology. (2024). National Cybersecurity Plan 2023–2028. Republic of the Philippines. https://cms-cdn.e.gov.ph/DICT/pdf/NCSP-2023-2028-FINAL-DICT.pdf.

[29] Section 29 (Performance Audit) of Republic Act No. 11659, Amending Commonwealth Act No. 146 or the Public Service Act, mandates "Administrative agencies must ensure the annual conduct of performance audit by an independent evaluation team to monitor cost, the quality of services provided to the public, and the ability of the public service provider to immediately and adequately respond to emergency cases: Provided, That in the case of critical infrastructure and public utilities, the performance audit shall include risk assessment, emergency response, and cybersecurity, among others. Metrics for various types of services must be established to sustain reliability, security, and safety of the public." The administrative agencies so mandated have yet to publish the requisite standards and metrics pursuant to the conduct of such performance audits of the relevant critical infrastructure and public utilities.

[30] Section 9 (Cybersecurity Certification) of Republic Act No. 12234 or the Konektadong Pinoy Act, requires a Data transmission industry participant (DTIP) to "adopt and comply with national and global best practices and standards on cybersecurity and be subject to a cybersecurity performance audit by the Cybersecurity Bureau of the DICT. Within two (2) years from registration, DTIPs shall secure a cybersecurity certification from a third-party organization based on the prevailing International Organization for Standardization (ISO) standards on information security management or such other minimum security standards identified by the DICT."

[31] Poling, G. B., & Hudes, S. T. (2023, April 11). Deepening the U.S.-Philippines alliance. Center for Strategic and International Studies.

[32] U.S. Embassy in the Philippines. (2024). Joint statement on the Philippines-United States bilateral strategic dialogue.

[33] TCO (Total Cost of Ownership) refers to the comprehensive assessment of all direct and indirect costs associated with acquiring, deploying, operating, and maintaining a cybersecurity solution or system over its entire lifecycle.

Picture Credits:

[1] *Cover page: stock.adobe.com/ph/search?k=cyber+defense&search_type=longtail-carousel-view-results&asset_id=1992445736*

[2] *Page 2: stock.adobe.com/ph/search?k=cyber+defense&search_type=longtail-carousel-view-results&asset_id=2114178613*

[3] *Page 5: stock.adobe.com/ph/search?k=cyber+defense&search_type=longtail-carousel-view-results&asset_id=2070903314*

19.08
VOLUME

ABOUT

Francisco Ashley L. Acedillo

Mr. Acedillo was the Deputy Director General for Cyber and Emerging Threats of the National Intelligence Coordinating Agency (NICA) under the Office of the President – the first to hold the post since its creation via Executive Order (EO) No. 54 s.2024. He previously served as Chief of Staff and Cybersecurity Adviser at the Senate of the Philippines, as well as Asst. Vice President for Cybersecurity Strategy and Innovation at the telecommunications conglomerate PLDT-Smart Communications Inc. He was a Member of the 16th Congress where he, among the seven bills that he authored and were enacted into law, was one of the principal authors of what eventually became Republic Act No. 10844 (An Act Creating the Department of Information and Communications Technology). A graduate of the Philippine Military Academy (Class of 1999), Acedillo served nine years in the Philippine Air Force as an officer and combat helicopter pilot, and was awarded a Gold Cross Medal (for gallantry in action) and a Distinguished Aviation Cross (for extraordinary heroism in aerial flight). He obtained a Master of Management from the Asian Institute of Management (AIM) as a W. Sycip Graduate School of Business full scholar.

stratbase INSTITUTE

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