

STRATEGIC COUNTRY REPORT: PHILIPPINES

Automated Strategic Analyst (v2.2 Parallel)

12 February 2026

Contents

1 Geopolitics	3
Executive Summary	3
1.1 Strategic Alignment and Great Power Competition	3
1.2 Submarine Cable Infrastructure and Physical Connectivity	4
1.3 Network Topology and Digital Sovereignty	4
References	5
2 Infrastructure	6
Executive Summary	6
2.1 Telecommunications Network Status	6
2.2 National Backbone and Submarine Connectivity	7
2.3 The Digital Divide and Socioeconomic Disparities	7
2.4 Regulatory and Investment Environment	7
References	8
3 Market	9
Executive Summary	9
3.1 Market Structure and Competitive Landscape	9
3.2 Network Performance and Connectivity Status	10
3.3 Revenue Dynamics and Economic Indicators	10
3.4 Investment Climate and Regulatory Framework	11
References	11
4 Localization	12
Executive Summary	12
Legislative Framework and Strategic Policy	12
Sovereign Cloud Infrastructure and Partnerships	13
Network Routing and Connectivity Challenges	13
Cross-Border Data Flows and International Standards	14
References	14
5 Security	16
Executive Summary	16
5.1 National Cybersecurity Posture and Preparedness	16
5.2 Threat Landscape and Attack Vectors	17
5.3 Infrastructure Resilience and Protocol Adoption	17
References	18
6 Governance	19
Executive Summary	19
6.1 Legal Framework and Civil Liberties	19

6.2	Telecommunications Regulation and Infrastructure	20
6.3	Digital Rights and Cybersecurity Status	20
	References	21
7	Strategic Synthesis & Roadmap	22
8	Section 7: Strategic Synthesis & Roadmap	23
8.1	Executive Summary: The “Big Picture” Diagnosis	23
8.2	SWOT Analysis: The Strategic Cheat Sheet	23
8.3	Strategic Roadmap: The Policy Agenda	24
8.4	Final Verdict	25

Chapter 1

Geopolitics

Executive Summary

The Philippines' geopolitical stance regarding digital infrastructure is defined by a strategic balancing act between economic pragmatism and national security imperatives, specifically within the context of the United States-China rivalry. While China remains the Philippines' largest trading partner, security concerns regarding territorial disputes in the South China Sea and potential espionage have prompted Manila to pivot toward infrastructure partnerships with the United States, Japan, and the European Union [Source 2]. This shift is evidenced by the cancellation of Chinese-funded projects and increased scrutiny over Chinese-backed vendors like Huawei in 5G deployment [Source 2, Source 3].

The nation's physical connectivity relies heavily on submarine cable systems, most notably the JUPITER system, which connects the Philippines to the U.S. and Japan via the Daet Cable Landing Station [Source 1]. Ownership of this critical infrastructure follows a consortium model involving U.S. and Japanese firms, mitigating the risk of unilateral foreign control [Source 1]. However, vulnerabilities persist in the energy sector—a critical dependency for digital operations—where the National Grid Corporation of the Philippines (NGCP) is 40% owned by the State Grid Corporation of China, raising concerns about potential foreign interference [Source 1]. Internally, the network topology exhibits high centralization, with several domestic Autonomous System Numbers (ASNs) showing 100% dependency scores, indicating significant resilience risks in the event of targeted disruptions [IYP-GRAFH].

1.1 Strategic Alignment and Great Power Competition

The Philippines is navigating a complex “techno-geopolitical” landscape, attempting to leverage international partnerships while mitigating risks associated with over-reliance on any single global power. The government has adopted a cautious approach toward Beijing’s “Digital Silk Road,” driven by fears of surveillance, vendor lock-in, and the potential for critical infrastructure to be used as leverage in territorial disputes [Source 3, Source 4]. Consequently, the Philippines

has sought to diversify its digital alliances, engaging with the European Union to position itself as a “digital connectivity hub,” although this initiative currently focuses on domestic economic resilience rather than regional transit [Source 1].

A focal point of this geopolitical tension is the telecommunications sector. While Huawei equipment offers a cost-effective solution for 5G deployment, its integration has sparked domestic political division and friction with Washington due to espionage concerns [Source 3]. Furthermore, the intersection of energy and digital infrastructure presents a unique strategic vulnerability. The 40% ownership of the NGCP by a Chinese state-owned enterprise creates a potential vector for foreign influence over the power grid that sustains the nation’s digital ecosystem, a situation that has deterred some U.S. investment in cooperative projects [Source 1].

1.2 Submarine Cable Infrastructure and Physical Connectivity

The Philippines’ connectivity to the global internet is primarily maritime, with no significant cross-border terrestrial fiber links confirmed connecting it to immediate neighbors [Source 1, Source 2]. The primary gateway identified is the JUPITER cable system, which lands at the Daet Cable Landing Station. This system is owned and operated by a consortium that includes Philippine Long Distance Telephone Company (PLDT), alongside U.S. tech giants (Amazon, Facebook) and Japanese carriers (NTT Communications, SoftBank) [Source 1]. This ownership structure reflects a strategic alignment with U.S. and Japanese interests rather than Chinese state-backed entities.

Despite its archipelagic geography, the Philippines does not currently serve as a critical digital transit point for landlocked Southeast Asian nations (such as Laos), which rely on alternative corridors through Vietnam and Thailand [Source 1]. However, the Luzon Strait remains a geostrategic bottleneck for regional cables connecting Southeast Asia to North America. While there are discussions regarding the expansion of cable landing points to enhance regional influence, current data does not confirm active investments specifically designed to bolster digital independence through new sovereign cable systems [Source 4].

1.3 Network Topology and Digital Sovereignty

The Philippines’ internal internet topology is characterized by a mix of domestic and foreign operators. Major Internet Exchange Points (IXPs) like PhIX are serviced by a diversity of ASNs, including local telecommunications leaders (PLDT, Converge ICT) and foreign content delivery networks (Cloudflare) [IYP-GRAFH]. Network analysis reveals a high degree of centralization; numerous local ASNs, including those associated with Globe Telecom and Starlink, exhibit a Hegemony Score of 1.0, indicating 100% dependency on upstream peers [IYP-GRAFH]. This topological fragility suggests that specific nodes represent critical points of failure.

From a policy perspective, the Philippines is debating the implementation of digital sovereignty measures. While the Data Privacy Act of 2016 is in force, recent proposals for stricter data

localization have faced opposition from the Global Data Alliance. Critics argue that localization mandates could increase costs, hinder innovation, and paradoxically weaken cybersecurity by restricting visibility, citing negative precedents in Cambodia and Vietnam [Source 3, Source 4]. The government's approach remains fluid, attempting to assert control over data residency without stifling the digital economy or alienating Western technology partners.

References

- [Source 1] Energy Security and the U.S.-Philippine Alliance - CSIS (<https://www.csis.org/analysis/energy-security-and-us-philippine-alliance>)
- [Source 2] Rocking the Boat: The Philippines Trade Strategy Amid Rising ... (<https://www.csis.org/analysis/rocking-boat-philippines-trade-strategy-amid-rising-geoeconomic-tensions>)
- [Source 3] 5G Geopolitics and the Philippines: The Huawei Controversy (<https://www.asiapacific.ca/publications/geopolitics-and-philippines-huawei-controversy>)
- [Source 4] Japan, the U.S., and the Geopolitics of Submarine Cable Security (<https://jsis.washington.edu/news/undersea-alliances-japan-the-u-s-and-the geopolitics-of-submarine-cable-security/>)
- [Source 1] NTT Com to Build Optical Submarine Cable Connecting Japan, U.S. ... (<https://www.gin.ntt.net/ntt-com-to-build-optical-submarine-cable-connecting-japan-u-s-and-philippines-with-large-capacity-and-low-latency/>)
- [Source 1] Global Gateway: EU and ASEAN strengthen their partnership on ... (https://international-partnerships.ec.europa.eu/news-and-events/news/global-gateway-eu-and-asean-strengthen-their-partnership-sustainable-connectivity-2024-02-02_en)
- [Source 3] GDA Comments on Philippine Data Localization Bill and PSAC ... (<https://globaldataalliance.org/wp-content/uploads/2025/09/09022025gdaphdatapsac.pdf>)
- [Source 4] Digital Sovereignty: protectionism or autonomy? | WITA (<https://www.wita.org/wp-content/uploads/2021/09/Digital-sovereignty-protectionism-or-autonomy-Hinrich-Foundation-Deborah-Elms-September-2021.pdf>)
- [Source 4] Economic and social impact of Meta's submarine cable investments ... (https://www.analysysmason.com/contentassets/0c7320380f594f59885246a8918a2fce/analysys_mason_research_economic_and_social_impact_of_meta_s_submarine_cable_investments_2021.pdf)
- [IYP-GRAFH] Internal Knowledge Graph

Chapter 2

Infrastructure

Executive Summary

The Philippines' physical digital infrastructure significantly lags behind regional Southeast Asian peers in terms of reach, capacity, and modernity. As of 2023, only 28 percent of households had access to fixed broadband, a figure substantially lower than Vietnam (79 percent), Thailand (55 percent), and Malaysia (54 percent) [Source 1]. The telecommunications sector is characterized by a massive deficit in cellular tower density and a heavy reliance on 4G technology, with 5G Standalone (SA) adoption remaining nascent at less than 1 percent of mobile connections [Source 5].

Strategic efforts to bridge these gaps are underway, primarily driven by World Bank-funded projects to complete the national fiber optic backbone and regulatory reforms such as the Public Service Act amendment, which aims to liberalize foreign ownership [Source 1]. However, the infrastructure remains vulnerable to natural disasters and climate change, particularly regarding submarine cable landing stations [Source 7]. A widening digital divide persists, heavily correlated with socioeconomic status, where internet penetration for the bottom wealth quintile has seen negligible growth compared to the top quintile [Source 1].

2.1 Telecommunications Network Status

Mobile Network Composition and Density The Philippine mobile network is currently dominated by 4G/LTE technology. Analysis of mobile traffic indicates that 73 percent of connections utilize 4G, while 5G adoption remains low. Only 8 percent of connections utilize 5G Non-Standalone (NSA) networks, and less than 1 percent utilize 5G Standalone (SA) networks [Source 5]. In the second half of 2023, approximately 18,618 new mobile broadband Cell IDs were observed; of these, only 5 percent were 5G-SA, with the operator DITO accounting for over 95 percent of those specific deployments [Source 5].

Infrastructure Deficit A critical bottleneck in network quality is the severe shortage of physical infrastructure. The Philippines operates approximately 22,834 combined cell sites. This is a

fraction of the infrastructure present in neighboring nations with similar or smaller populations; for instance, both Vietnam and Indonesia operate approximately 90,000 cell sites each [Source 3]. This density deficit contributes to the country's low global rankings in internet speeds, placing 89th in mobile and 49th in fixed broadband as of mid-2023 [Source 3]. To address this, the government has adopted a Common Tower Policy to facilitate infrastructure sharing and reduce deployment costs [Source 1].

2.2 National Backbone and Submarine Connectivity

Fiber Optic Backbone Expansion The government is currently executing the Philippines Digital Infrastructure Project to complete the national fiber backbone. This strategic initiative aims to connect the two primary international landing stations located in Baler (Luzon) and Davao City (Mindanao), thereby creating a redundant high-speed pathway across the archipelago [Source 6]. This expansion is critical, as the current infrastructure suffers from a lack of redundancy.

Submarine Cable Vulnerabilities As an archipelagic state, the Philippines relies heavily on submarine cables for domestic and international connectivity. This infrastructure faces significant physical risks: * **Climate and Environmental Threats:** Landing stations and cables are increasingly vulnerable to climate change impacts, including storm surges and underwater landslides [Source 7]. * **Operational Resilience:** There is a lack of route diversity, meaning a single incident can cause widespread disruption. Furthermore, repair capabilities are constrained by the limited global availability of repair vessels and high costs, averaging between \$1 million and \$3 million per repair operation [Source 7].

2.3 The Digital Divide and Socioeconomic Disparities

Access Gaps A profound digital divide exists within the country, driven by wealth and geography. While internet penetration for the top wealth quintile rose from 43 percent in 2019 to 60 percent in 2022, penetration for the bottom quintile stagnated, moving only from 2 percent to 5 percent in the same period [Source 1]. The Philippines accounts for over half of the unconnected mobile broadband population across ASEAN countries [Source 1].

Urban-Rural Disparity While specific “white spot” maps are not publicly available, the disparity follows global trends where urban internet usage (83 percent) significantly outpaces rural usage (48 percent) [Source 8]. The high cost of service relative to income in rural areas remains a barrier, exacerbated by the fact that legacy telecommunications players have historically concentrated on profitable urban centers [Source 3].

2.4 Regulatory and Investment Environment

Investment Trends Despite the clear need for infrastructure upgrades, telecommunications investment in the Philippines has declined, falling from \$2.1 billion in 2019 to less than \$1.8

billion in 2023 [Source 1]. This decline occurs despite the growing digital economy.

Policy Reforms The government has initiated several reforms to stimulate infrastructure development: * **Public Service Act Amendment:** This reform eliminates restrictions on foreign ownership in public services, theoretically allowing greater foreign direct investment into the telecommunications sector [Source 1]. * **Bureaucratic Streamlining:** Efforts are underway to simplify the network rollout process and reduce the permitting obstacles that have historically slowed tower construction [Source 1]. * **Legacy Constraints:** The sector continues to navigate outdated frameworks, such as the Radio Control Law of 1931, which has historically constrained market entry and competition [Source 2].

References

- [Source 1] Unlocking the Philippines' Digital Transformation by Increasing Internet Connectivity (<https://projects.worldbank.org/en/results/2025/07/02/unlocking-the-philippines-digital-transformation-by-increasing-internet-connectivity>)
- [Source 2] Philippines Digital Economy Report 2020 - World Bank Document (<https://documents1.worldbank.org/curated/en/796871601650398190/pdf/Philippines-Digital-Economy-Report-2020-A-Better-Normal-Under-COVID-19-Digitalizing-the-Philippine-Economy-Now.pdf>)
- [Source 3] Philippines - Information and Communications Technology (<https://www.trade.gov/country-commercial-guides/philippines-information-and-communications-technology>)
- [Source 4] The Digital Economy in Southeast Asia - World Bank Document (<https://documents1.worldbank.org/curated/en/328941558708267736/pdf/The-Digital-Economy-in-Southeast-Asia-Strengthening-the-Foundations-for-Future-Growth.pdf>)
- [Source 5] Global Mobile Insights Report - M2Catalyst (<https://www.m2catalyst.com/test-report/philippines-mobiletraffic>)
- [Source 6] More Than 20 million Filipinos to Benefit from Improved Broadband Internet Connectivity (<https://www.worldbank.org/en/news/press-release/2024/10/10/more-than-20-million-filipinos-to-benefit-from-improved-broadband-internet-connectivity>)
- [Source 7] Submarine Cable Security at Risk Amid Geopolitical Tensions (<https://www.recordedfuture.com/cables-face-increasing-threats>)
- [Source 8] Global Internet use continues to rise but disparities remain - ITU (<https://www.itu.int/en/mediacentre/Pages/PR-2024-11-27-facts-and-figures.aspx>)
- [IYP-GRAPH] Internal Knowledge Graph

Chapter 3

Market

Executive Summary

The Philippine telecommunications market is characterized by extreme market concentration, a rapid pivot toward data-driven revenue streams, and a liberalizing regulatory environment designed to court foreign capital. The sector exhibits a Herfindahl-Hirschman Index (HHI) higher than that of Mexico—historically one of the world’s most concentrated markets—indicating a rigid oligopoly with intense competition primarily between incumbent conglomerates rather than new market entrants [Source 1]. Despite high barriers to entry such as infrastructure costs and regulatory constraints that have historically deterred significant “disruptor” operators [Source 2], the market has achieved competitive pricing in mobile data. The average price for 1GB of mobile data is approximately \$0.18 USD, significantly lower than the global average of roughly \$4.00 [Source 3].

Strategic shifts are evident as operators transition from legacy voice and SMS revenues toward mobile data, fixed broadband, and enterprise solutions including cloud computing and IoT [Source 4]. This transition is supported by regulatory reforms, specifically amendments to the Public Service Act (PSA) allowing 100% foreign ownership, and the CREATE Act, which aims to streamline fiscal incentives [Source 5]. However, infrastructure deficiencies and bureaucratic hurdles remain critical challenges to fully realizing the sector’s investment potential [Source 5].

3.1 Market Structure and Competitive Landscape

The competitive landscape of the Philippines is defined by high saturation and consolidation. Intelligence indicates that the market’s concentration levels are exceptionally high, surpassing benchmarks set by other highly concentrated global markets [Source 1]. This structural rigidity is reinforced by significant barriers to entry, including the high cost of digital infrastructure deployment and complex regulatory requirements, which have prevented the emergence of significant “disruptor” operators capable of challenging established players on price or service quality in the near term [Source 2].

While specific recent merger and acquisition (M&A) deals are not detailed in current reporting, the market is following a global trend toward infrastructure consolidation. This includes a strategic focus on the National Fiber Backbone Project and potential infrastructure sharing to optimize capital expenditure for 5G and fiber expansion [Source 6]. The focus has shifted from fragmenting the market to reinforcing existing duopolistic or oligopolistic strongholds through technological upgrades.

3.2 Network Performance and Connectivity Status

Network performance metrics indicate a market in the midst of a technological upgrade cycle, though speeds remain modest by developed market standards. According to the Ookla Speedtest Global Index, the median download speed for mobile connections is 24.74 Mbps, with upload speeds of 7.19 Mbps. Fixed broadband metrics show similar median download performance at 24.74 Mbps [Source 7].

Despite these modest median speeds, infrastructure modernization is progressing. 5G connectivity is now available in major urban centers, with some operators offering speeds up to 300–400 Mbps in specific zones. Furthermore, fiber internet availability has expanded, with plans offering up to 1 Gbps becoming widely available in key metropolitan areas [Source 3]. This infrastructure supports the growing demand for modern applications, although consistency and nationwide coverage remain developmental goals.

3.3 Revenue Dynamics and Economic Indicators

The economic model of Philippine telecommunications is undergoing a fundamental reset. Revenue streams are decisively shifting away from traditional voice and SMS toward data consumption. * **Mobile Data:** Revenue growth is fueled by increasing smartphone penetration and the aggressive promotion of 5G services, which are designed to lift Average Revenue Per User (ARPU) [Source 4]. * **Fixed Broadband:** Operators are focusing on subscriber expansion through fiber lines, utilizing bundling and upselling strategies to maximize value per household [Source 4]. * **Enterprise Solutions:** Telcos are evolving into IT solution providers, leveraging 5G to offer specialized services in edge computing and cloud-based solutions for sectors such as manufacturing and healthcare [Source 8].

Pricing strategies have become highly aggressive to drive adoption. The approximate cost of \$0.18 per GB for mobile data places the Philippines among the most affordable markets in the region for data consumption [Source 3]. However, global trends suggest that mobile ARPU is generally declining or flatlining, forcing operators to rely on volume and value-added services to maintain growth [Source 9].

3.4 Investment Climate and Regulatory Framework

The regulatory environment for telecommunications in the Philippines has become significantly more favorable to foreign direct investment (FDI). Key legislative developments include:

- * **Public Service Act (PSA) Amendments:** This reform effectively opens the telecommunications sector to 100% foreign ownership, removing the 40% foreign equity cap that previously constrained investment [Source 5].
- * **Fiscal Incentives:** The CREATE Act and the establishment of “green lanes” under Executive Order No. 18 aim to expedite permits for strategic investments and reduce corporate income tax burdens [Source 5].

Despite these improvements, the investment climate is tempered by persistent operational challenges. Investors face obstacles related to infrastructure deficiencies, regulatory inconsistencies, and corruption. Furthermore, the dominance of large conglomerates creates a difficult environment for new entrants to navigate without significant local partnerships [Source 5].

References

- [Source 1] Distributional Effects of Competition: A Simulation Approach (<https://docs.iza.org/dp14043.pdf>)
- [Source 2] Philippines Digital Economy Report 2020 - World Bank Document (<https://documents1.worldbank.org/curated/en/796871601650398190/pdf/Philippines-Digital-Economy-Report-2020-A-Better-Normal-Under-COVID-19-Digitalizing-the-Philippine-Economy-Now.pdf>)
- [Source 3] PSA: Internet in the Philippines has massively improved in the past 5 ... (https://www.reddit.com/r/digitalnomad/comments/1ap4slp/psa_internet_in_the_philippines_has_m/)
- [Source 4] Philippines Telecom Operators Intelligence Report 2025 Featuring ... (<https://sg.finance.yahoo.com/news/philippines-telecom-operators-intelligence-report-154200750.html>)
- [Source 5] 2024 Investment Climate Statements: Philippines (<https://www.state.gov/reports/2024-investment-climate-statements/philippines>)
- [Source 6] Key M&A Trends in 2024: A Year in Review of the Philippine ... - PwC (<https://www.pwc.com/ph/en/deals-corporate-finance/deals-publications/2024-ap-ma-report.html>)
- [Source 7] Philippines's Mobile and Broadband Internet Speeds (<https://www.speedtest.net/global-index/philippines>)
- [Source 8] Reshaping business models in the telecom industry - WTW (<https://www.wtaco.com/en-us/insights/2025/02/navigating-the-future-reshaping-business-models-for-new-revenue-streams-in-the-telecom-industry>)
- [Source 9] Perspectives from the Global Telecom Outlook 2024–2028 - PwC (<https://www.pwc.com/gx/en-outlook-perspectives.html>)
- [IYP-GRAFH] Internal Knowledge Graph

Chapter 4

Localization

Executive Summary

The Philippines is actively recalibrating its digital posture, moving toward a framework of “digital sovereignty” characterized by the strategic maxim: “Our data. Our soil. Our rules.” [Source 1 (Q1)]. This shift aims to treat data infrastructure as a strategic national asset, reducing reliance on foreign technologies through a “Diverse-Cloud” strategy that integrates U.S. hyperscalers, Chinese platforms, and domestic sovereign providers [Source 1 (Q1)]. The government’s approach is formalized in the recent passage of Republic Act No. 12254, the E-Governance Act, which mandates unified, secure digital platforms and emphasizes local control and data residency for government networks [Source 3 (Q12)].

However, the drive toward strict data localization faces significant opposition from industry stakeholders. Entities such as the Global Data Alliance (GDA) argue that broad localization mandates could undermine the Business Process Outsourcing (BPO) industry—a critical economic pillar—by impeding cross-border data flows and increasing cybersecurity vulnerabilities [Source 1 (Q3)]. Consequently, the Philippine strategy represents a complex balancing act: promoting sovereign cloud infrastructure and local routing to secure national assets, while maintaining the open data flows necessary for economic competitiveness and international interoperability [Source 1 (Q11)].

Legislative Framework and Strategic Policy

The Philippine government has moved beyond theoretical discussions of sovereignty to legislative action. The cornerstone of this effort is Republic Act No. 12254, the E-Governance Act. This legislation empowers the Department of Information and Communications Technology (DICT) to lead an Integrated Government Network, explicitly prioritizing local control, data residency, and regulatory compliance for cloud infrastructure used by the public sector [Source 3 (Q12)]. This aligns with a broader “Cloud First Policy” that encourages government administration to adopt cloud computing, though specific implementation details regarding hosting percentages

remain fluid [Source 1 (Q2)].

Despite the passage of the E-Governance Act, broader attempts to mandate data localization for the private sector have met resistance. Draft Executive Orders and proposed legislation aiming to enforce localization for cloud services have been challenged by the Global Data Alliance. Critics argue that such measures would degrade local capacity by isolating the Philippines from global threat intelligence, increase costs for Micro, Small, and Medium Enterprises (MSMEs), and potentially reduce GDP by stifling the service exports sector [Source 1 (Q3)]. The government is thus navigating a “Diverse-Cloud” policy, encouraging the use of domestic providers like PLDT/ePLDT alongside international hyperscalers to mitigate the risks of over-centralization [Source 1 (Q1)].

Sovereign Cloud Infrastructure and Partnerships

To operationalize its sovereignty goals, the Philippines is fostering a domestic “Sovereign Data Cloud Infrastructure.” This initiative involves public-private partnerships designed to ensure local data control and operational continuity. Notable collaborations include partnerships between local entities and global IT service providers, such as Tata Consultancy Services (TCS) and NOW Corporation. These alliances aim to build trusted networks and sovereign cloud technologies that reduce dependence on foreign infrastructure while defending against cyber threats [Source 2 (Q12)]. Additionally, firms like CloudSigma and Sover are positioning themselves to provide locally hosted, encrypted infrastructure that complies with Philippine sovereignty requirements [Source 3 (Q12)].

This infrastructure push coincides with a surge in demand; 85% of Philippine businesses expect to be fully cloud-enabled by 2025 [Source 4 (Q2)]. However, the market remains heavily influenced by foreign investment, facilitated by amendments to the Public Service Act that allow up to 100% foreign ownership in telecommunications [Source 1 (Q2)]. This creates a dual-track environment where the state promotes sovereign capacity while simultaneously liberalizing ownership rules to attract necessary capital for data center expansion.

Network Routing and Connectivity Challenges

A critical vulnerability in the Philippines’ localization strategy lies in internet traffic routing. Intelligence indicates that major internet service providers, specifically PLDT, have historically routed local internet traffic through international exchange points, such as the Hong Kong Internet Exchange (HKIX), rather than utilizing the local Philippine Open Internet Exchange (PHOpenIX) [Source 1 (Q7)].

This practice, allegedly maintained to monetize peering and transit, results in “tromboning”—where data originating and terminating within the Philippines traverses international borders. This increases latency, raises costs, and exposes domestic traffic to foreign surveillance and jurisdiction [Source 3 (Q7)]. While the government promotes local hosting, the physical routing

of data through foreign hubs undermines the theoretical benefits of data residency. Effective localization will require not only domestic storage but also the enforcement of local peering to ensure data stays within national borders during transit.

Cross-Border Data Flows and International Standards

Recognizing the economic necessity of cross-border data flows, particularly for the BPO sector, the Philippines maintains active engagement in international privacy forums. The National Privacy Commission (NPC) is a participant in the Global Cross-Border Privacy Rules (CBPR) Forum. This involvement aims to establish interoperability between national regulations and global standards, facilitating safe data transfers without abandoning sovereignty principles [Source 1 (Q11)].

The government's stance is to align with frameworks like the ASEAN Model Contractual Clauses, which standardize data protection for regional transfers [Source 4 (Q11)]. This approach attempts to mitigate the "legal isolation" risks cited by critics of localization, ensuring that while the Philippines builds its sovereign "digital soil," it remains integrated into the global digital economy.

References

- [Source 1 (Q1)] Geopolitics of Data Centers in Southeast Asia: The New Power AI Cockcroft FRGS (<https://www.linkedin.com/pulse/geopolitics-data-centers-southeast-asia-new-power-ai-cockcroft-frgs-w7voc>)
- [Source 1 (Q2)] Philippines - Information and Communications Technology (<https://www.trade.gov/count-commercial-guides/philippines-information-and-communications-technology>)
- [Source 4 (Q2)] Philippines Data Center Market Set for 2030 Surge - ASEAN Briefing (<https://www.aseanbriefing.com/news/rising-demand-for-data-centers-in-the-philippines/>)
- [Source 1 (Q3)] Philippines: Comments on Draft Executive Order relating to Policy (<https://globaldataalliance.org/wp-content/uploads/2023/09/09262023gsadatalocalcloud.pdf>)
- [Source 1 (Q7)] How PLDT Deliberately Keeps Local Internet Traffic Slow and More (https://www.reddit.com/r/Philippines/comments/2aurzq/how_pldt_deliberately_keeps_local_internet/)
- [Source 3 (Q7)] Repost: How PLDT Deliberately Keeps Local Internet Traffic Slow (https://www.reddit.com/r/Philippines/comments/6lbp1m/repost_how_pldt_deliberately_keeps_local/)
- [Source 1 (Q11)] Global Cross-Border Privacy Rules (CBPR) Forum Fall Workshop (<https://www.globalcbpr.org/global-cross-border-privacy-rules-cbpr-forum-fall-workshop-2025-making-waves-shaping-the-future-24-october-2025/>)
- [Source 4 (Q11)] ASEAN Model Contractual Clauses for Cross Border Data Flows (https://asean.org/wp-content/uploads/3-ASEAN-Model-Contractual-Clauses-for-Cross-Border-Data-Flows_Final.pdf)
- [Source 2 (Q12)] TCS Partners with Now Corporation to Power Philippines' Sovereign Data

Cloud (<https://www.tcs.com/who-we-are/newsroom/press-release/tcs-partners-with-now-corporation-power-philippines-sovereign-data-cloud-financial-inclusivity>)

- [Source 3 (Q12)] Philippines passes E-Governance Act, CloudSigma ready to partner (https://www.linkedin.com/posts/sutedjo-tjahjadi-b6b38b4_datasovereignty-e-cloudphilippines-activity-7372098279561445376-Ya-g)
- [IYP-GRAPH] Internal Knowledge Graph

Chapter 5

Security

Executive Summary

The Philippines presents a mixed security profile characterized by significant gaps in national cybersecurity governance and technical preparedness, despite facing an active and evolving threat landscape. The nation ranks 73rd on the National Cyber Security Index (NCSI), a position that trails key regional ASEAN partners such as Singapore and Malaysia [Source 2]. Critical vulnerabilities have been identified in the implementation of cybersecurity strategies and public threat reporting, with indicators in these specific areas showing zero percent fulfillment as of recent assessments [Source 3].

The threat environment is consistent with broader Asia-Pacific trends, dominated by ransomware, phishing, and malicious domain activity [Source 4]. However, the country's resilience is obscured by a lack of definitive public data regarding critical infrastructure protocols such as RPKI and DNSSEC. Adoption of these security measures is reportedly hindered by technical complexity, skill shortages, and cost implications [Source 6]. Furthermore, while the Philippines is situated in a geopolitically sensitive maritime region, specific data regarding ASN "chokepoints" remains opaque, though the security of subsea cable infrastructure remains a high-level concern in the Indo-Pacific theater [Source 8].

5.1 National Cybersecurity Posture and Preparedness

The Philippines' standing in global cybersecurity benchmarks indicates a need for substantial structural improvement. On the National Cyber Security Index (NCSI), the country holds a score of 55.83, placing it 73rd globally. This ranking highlights a disparity in technical preparedness when compared to ASEAN neighbors; for instance, Singapore ranks 27th with a score of 85.00, and Malaysia ranks 51st with a score of 72.50 [Source 2].

Detailed assessments reveal specific implementation gaps. As of March 2021, the Philippines showed significant deficiencies in critical indicators, including a lack of active cybersecurity strategy implementation, the absence of public cyber threat reports, and limited cyber safety

competencies within the education sector [Source 3]. While the ITU Global Cybersecurity Index 2024 acknowledges general challenges such as resource limitations and capacity gaps for nations in this tier, specific scoring breakdowns for the Philippines in the 2024 cycle remain generalized [Source 1].

5.2 Threat Landscape and Attack Vectors

The operational threat landscape facing the Philippines is aligned with observations from the Asia Pacific Computer Emergency Response Team (APCERT). National cybersecurity agencies in the region, including those in the Philippines, actively contend with the following primary vectors:

- **Ransomware and Malware:** Malicious code, specifically ransomware, remains a persistent threat to both public and private sectors [Source 4].
- **Phishing and Social Engineering:** There is a high volume of activity involving phishing sites and malicious domain requests. Incident response drills and training frequently focus on analyzing phishing domains to mitigate this risk [Source 4].
- **Infrastructure Attacks:** Agencies report blocking millions of malicious domain requests and thousands of attacks targeting servers. Denial of Service (DoS) and Distributed Denial of Service (DDoS) attacks are categorized as significant availability threats [Source 5].
- **Hacktivism:** This vector has been identified as a recurring theme in cyber incident drills, indicating its relevance to national security planning [Source 5].

5.3 Infrastructure Resilience and Protocol Adoption

The resilience of the Philippines' internet infrastructure is difficult to quantify due to a lack of specific, up-to-date technical data regarding the adoption of routing security standards.

Routing and DNS Security There is no definitive current data available regarding the validation rates for Resource Public Key Infrastructure (RPKI) or Domain Name System Security Extensions (DNSSEC) specifically for the Philippines. However, regional reports from APNIC indicate that a significant portion of members in the Asia Pacific region (approximately 30%) have no plans for RPKI deployment, and 15% utilize RPKI without performing Route Origin Validation (ROV) [Source 7].

Barriers to Adoption Philippine cybersecurity authorities and industry stakeholders face distinct challenges in securing the nation's routing infrastructure. The primary obstacles to widespread RPKI and DNSSEC adoption include:
* **Complexity and Cost:** The technical complexity of these protocols, combined with the financial costs associated with implementation, serves as a barrier [Source 6].
* **Technical Capacity:** There is a recognized need for enhanced technical skills and knowledge within the workforce to manage these security protocols effectively [Source 6].
* **Market Demand:** A lack of clear customer demand for enhanced security measures further disincentivizes rapid adoption by service providers [Source 6].

Physical Infrastructure Risks While specific Autonomous System Numbers (ASNs) acting as “chokepoints” within the Philippines have not been publicly identified in open-source intelligence, the physical security of subsea cables remains a relevant concern. The Philippines is located in the Indo-Pacific region, where geopolitical tensions place subsea cable infrastructure at risk. General assessments highlight vulnerabilities related to the lack of cable route diversity and limited repair capacity in contested maritime areas [Source 8].

References

- [Source 1] Global Cybersecurity Index 2024 - ITU (https://www.itu.int/en/ITU-D/Cybersecurity/Documents/GCIv5/2401416_1b_Global-Cybersecurity-Index-E.pdf)
- [Source 2] NCSI :: Ranking - National Cyber Security Index (<https://ncsi.ega.ee/ncsi-index/?order=rank>)
- [Source 3] NCSI :: Philippines - National Cyber Security Index (https://ncsi.ega.ee/country/ph_2022/)
- [Source 4] APCERT_Annual_Report_2024.pdf (https://www.apcert.org/documents/pdf/APCERT_Annual_Report_2024.pdf)
- [Source 5] APCERT_Annual_Report_2023.pdf ([http://www.apcert.org/documents/pdf/APCERT_Annual_Report_2023.pdf](https://www.apcert.org/documents/pdf/APCERT_Annual_Report_2023.pdf))
- [Source 6] The politics of internet security: Private industry and the future of the web (<https://www.atlanticcouncil.org/in-depth-research-reports/report/the-politics-of-internet-security-private-industry-and-the-future-of-the-web/>)
- [Source 7] Annual Report - APNIC (https://www.apnic.net/wp-content/uploads/2023/05/APNIC_AR_2023.pdf)
- [Source 8] Safeguarding Subsea Cables: Protecting Cyber Infrastructure ... - CSIS (<https://www.csis.org/analysis/safeguarding-subsea-cables-protecting-cyber-infrastructure-amid-great-power-competition>)

Chapter 6

Governance

Executive Summary

The governance framework of the Philippines regarding the digital and telecommunications sectors is characterized by a dichotomy between robust constitutional protections for expression and structural vulnerabilities in regulatory autonomy. The 1987 Constitution and the Data Privacy Act of 2012 provide a strong legal basis for civil liberties and data protection. However, the primary regulatory body, the National Telecommunications Commission (NTC), lacks operational and budgetary independence, remaining subject to direct executive control. This centralization of power raises strategic concerns regarding the potential for politically motivated interference in the telecommunications sector. Furthermore, while the Philippines has engaged with international cybercrime frameworks, recent domestic policy shifts—specifically the enactment of SIM card registration laws and the utilization of antiterrorism legislation to restrict access to critical media—suggest a tightening of state control over the digital domain, undermining the anonymity and freedom historically afforded to Philippine internet users.

6.1 Legal Framework and Civil Liberties

The foundational legal framework governing freedom of speech and expression in the Philippines is anchored in the **1987 Philippine Constitution**. Article III (Bill of Rights) guarantees these fundamental liberties, aligning with international standards such as Article 19 of the Universal Declaration of Human Rights, which protects the right to hold opinions and impart information without interference [Universal Declaration of Human Rights; Philippines 1987 - Constitute Project].

Regarding data privacy, the Philippines enforces the **Data Privacy Act of 2012 (Republic Act No. 10173)**. This comprehensive legislation applies extraterritorially to entities processing the data of Philippine citizens. It establishes the National Privacy Commission (NPC) and mandates that data processing adhere to principles of transparency, legitimate purpose, and proportionality. While the Act generally requires consent for data collection, it includes exceptions

for national emergencies and legal obligations, which could theoretically be invoked to justify state surveillance, although the Act's overarching principles are designed to limit arbitrary intrusion [Summary: Philippines Data Privacy Act and implementing regulations].

Despite these protections, the legal landscape for internet control remains opaque. Intelligence findings indicate that specific legal provisions governing the blocking or throttling of internet content are not definitively detailed in available open-source data, although the “Bayanihan to Heal as One Act” has been noted for imposing fines related to online content [Chilling Legislation: Tracking the Impact of “Fake News” Laws].

6.2 Telecommunications Regulation and Infrastructure

The primary authority responsible for regulating and supervising telecommunications and broadcast services is the **National Telecommunications Commission (NTC)** [2024 Investment Climate Statements: Philippines].

A critical governance weakness is the NTC's lack of structural independence. The regulator does not possess independent funding or operational autonomy; rather, it is subject to direct presidential or executive control. This lack of budgetary authority renders the NTC susceptible to political pressure, a common characteristic in regulatory bodies where executive powers can restrict independence and create market uncertainty [Governing Infrastructure Regulators in Fragile Environments].

The NTC manages market access through a certification regime. Wireless products intended for the Philippine market require NTC certification (Type Approval or Type Acceptance). The process involves the submission of technical test reports (RF, EMC, Safety) with a typical lead time of 4 to 8 weeks. While the procedural steps for licensing are established, intelligence findings do not confirm whether these processes are perceived as transparent or non-discriminatory by external actors [NTC Type Approval and Certification for Philippines - IB-Lenhardt].

6.3 Digital Rights and Cybersecurity Status

The Philippines faces significant challenges regarding internet freedom. While a specific “Freedom on the Net” score is not available in the current dataset, qualitative indicators suggest a decline in digital rights. Key factors include the government's use of antiterrorism laws to block critical news websites and the implementation of the **SIM Card Registration Law**. The latter is assessed as a measure that undermines anonymous communication, a core component of internet freedom [FREEDOM ON THE NET 2023].

Internationally, the Philippines' commitment to cybercrime cooperation is mixed. The country participated as an observer state in the drafting of the **Budapest Convention on Cybercrime** and is a signatory. However, current intelligence does not definitively confirm whether the Philippines has fully ratified or implemented the Convention [Budapest Convention on Cybercrime - Wikipedia]. Furthermore, the Philippines is not a party to the Malabo Convention

(African Union Convention on Cyber Security), as it is not a member of the African Union [Budapest Convention on Cybercrime - Wikipedia].

References

- [Universal Declaration of Human Rights] Universal Declaration of Human Rights - the United Nations (<https://www.un.org/en/about-us/universal-declaration-of-human-rights>)
- [Philippines 1987 - Constitute Project] Philippines 1987 - Constitute Project (https://www.constituteproject.org/constitution/Philippines_1987)
- [Summary: Philippines Data Privacy Act and implementing regulations] Summary: Philippines Data Privacy Act and implementing regulations (<https://iapp.org/news/a/summary-philippines-data-protection-act-and-implementing-regulations>)
- [Chilling Legislation: Tracking the Impact of “Fake News” Laws] Chilling Legislation: Tracking the Impact of “Fake News” Laws on ... (<https://www.cima.ned.org/publication/chilling-legislation/>)
- [2024 Investment Climate Statements: Philippines] 2024 Investment Climate Statements: Philippines (<https://www.state.gov/reports/2024-investment-climate-statements/philippines>)
- [Governing Infrastructure Regulators in Fragile Environments] Governing Infrastructure Regulators in Fragile Environments (<https://ppp.worldbank.org/sites/default/files/2022-03/Governing-Infrastructure-Regulators-in-Fragile-Environments-Principles-and-Implementation-Manual.pdf>)
- [NTC Type Approval and Certification for Philippines - IB-Lenhardt] NTC Type Approval and Certification for Philippines - IB-Lenhardt (<https://ib-lenhardt.com/type-approval/philippines>)
- [FREEDOM ON THE NET 2023] FREEDOM ON THE NET 2023 (<https://freedomhouse.org/sites/default/10/Freedom-on-the-net-2023-DigitalBooklet.pdf>)
- [Budapest Convention on Cybercrime - Wikipedia] Budapest Convention on Cybercrime - Wikipedia (https://en.wikipedia.org/wiki/Budapest_Convention_on_Cybercrime)
- [IYP-GRAFH] Internal Knowledge Graph

Chapter 7

Strategic Synthesis & Roadmap

Chapter 8

Section 7: Strategic Synthesis & Roadmap

To: The President of the Republic of the Philippines **From:** Office of the Chief Strategy Officer
Date: October 26, 2025 **Subject:** NATIONAL DIGITAL STATECRAFT: SECURING THE ARCHIPELAGO

8.1 Executive Summary: The “Big Picture” Diagnosis

The Narrative: Mr. President, the Philippines stands at a critical juncture. We have successfully liberalized our economy to attract foreign capital (via the Public Service Act), and we have aligned our external connectivity with trusted allies (US/Japan cable consortiums). However, we face a **“Sovereignty Trap.”** While our digital borders are open to investment, our internal physical infrastructure is brittle, under-served, and powered by an energy grid with significant foreign state-owned influence.

The Paradox: “The Open Door, Closed Room.” We have legally opened the door to 100% foreign ownership to solve our connectivity crisis, yet the room itself—our domestic network—is structurally unsound. We rely on American cables to reach the world, but Chinese-affiliated entities hold significant sway over the power grid (NGCP) that keeps those cables running. We export world-class BPO services, yet our domestic internet traffic often “trombones” through Hong Kong before reaching a user in Manila, exposing us to unnecessary latency and surveillance.

8.2 SWOT Analysis: The Strategic Cheat Sheet

STRENGTHS (Internal)	WEAKNESSES (Internal)
<p>Liberalized Market: PSA amendments allow 100% foreign ownership, a massive magnet for capital.</p> <p>Geostrategic Location: Critical gateway between the Pacific (US) and Southeast Asia.</p> <p>Human Capital: English-proficient workforce powering a robust BPO sector.</p>	<p>Infrastructure Deficit: Severe shortage of cell towers and low fiber penetration (28% of households).</p> <p>Energy Vulnerability: 40% Chinese ownership of NGCP creates a “kill switch” risk for digital power.</p> <p>Routing Inefficiency: Domestic traffic routing via foreign IXPs (Hong Kong) increases latency and risk.</p>
OPPORTUNITIES (External)	THREATS (External)
<p>“Friend-Shoring”: US/Japan desire to bypass contested waters makes us a prime cable hub.</p> <p>Satellite Connectivity: Archipelagic geography is perfect for LEO satellite (Starlink) adoption.</p> <p>Data Center Hub: Potential to become the green data center capital of ASEAN if energy is fixed.</p>	<p>Cable Sabotage: High risk of subsea cable cutting in the South China Sea/Luzon Strait.</p> <p>Cyber Warfare: Low national cyber hygiene (Rank 73rd) makes us a soft target for ransomware.</p> <p>Regulatory Capture: NTC’s lack of independence risks politicizing technical decisions.</p>

8.3 Strategic Roadmap: The Policy Agenda

8.3.1 Phase 1: Immediate Actions (Months 1-6) — “Secure the Perimeter”

- **Objective:** Close immediate security gaps without spending billions on new infrastructure.
- **Action 1 (Cyber-Hygiene Mandate):** Issue an Executive Order requiring all Government agencies and Critical Information Infrastructure (CII) providers to implement **RPKI** and **DNSSEC** protocols. We must stop being a “safe harbor” for malicious routing.
- **Action 2 (Stop the “Tromboning”):** Mandate that all domestic ISPs peer at the **PHOpenIX** (local exchange). Domestic traffic must stay on domestic soil. This improves speed for citizens and security for the state without hurting BPO cross-border flows.
- **Action 3 (Energy Audit):** Convene a National Security Council audit of the NGCP’s digital control systems. We must verify that the grid management software is air-gapped from foreign access.

8.3.2 Phase 2: Medium Term (Months 6-24) — “Build the Backbone”

- **Objective:** Leverage the Public Service Act (PSA) to flood the market with infrastructure.
- **Action 1 (The “Common Tower” Blitz):** aggressively enforce the Common Tower Policy. Streamline permitting for new entrants. If the duopoly won’t build rural towers, allow foreign-backed “TowerCos” to do it for them.
- **Action 2 (Cable Landing Diversification):** Incentivize new subsea cable landings away from the Luzon Strait (a geopolitical chokepoint) to **Mindanao and the Visayas**. Create a redundant “Southern Corridor” that bypasses potential conflict zones in the north.
- **Action 3 (Regulatory Independence):** Push for legislation to grant the **National Telecommunications Commission (NTC)** fiscal and operational autonomy, insulating it from political cycles and increasing investor confidence.

8.3.3 Phase 3: Long Term (Years 2-5) — “The Digital Fortress”

- **Objective:** Achieve true Digital Sovereignty and Regional Leadership.
 - **Action 1 (Sovereign Cloud):** Complete the government’s migration to a “Hybrid Sovereign Cloud.” Sensitive citizen data stays on government-owned servers; public services run on secure, localized hyperscaler instances (AWS/Azure/Google) within Philippine borders.
 - **Action 2 (Green Digital Energy):** Decouple the digital economy from the traditional grid. Incentivize data centers to build their own renewable power sources (Solar/Geothermal), reducing reliance on the NGCP.
 - **Action 3 (The “Asian Data Vault”):** Position the Philippines as the “Switzerland of Data” for Asia—a neutral, highly connected, legally secure jurisdiction for data storage, protected by strong privacy laws and robust US-backed physical security.
-

8.4 Final Verdict

Investability Score: HIGH *Explanation:* The legal framework is now world-class due to the PSA amendment allowing 100% foreign ownership. The market is hungry (high data usage, low penetration). The only missing piece is capital to build the physical assets. The door is open; investors just need assurance that the floor won’t collapse (energy/security).

Maturity Score: DEVELOPING *Explanation:* We are a “Mobile-First” nation with “Third-World” infrastructure. While our consumption habits are mature (high social media usage), our physical layer (towers, fiber, 5G SA) and security posture (NCSI ranking) are significantly behind Vietnam and Thailand. We are transitioning from a legacy duopoly to a modern open market.