“NEUTRALITY IN THE DIGITAL AGE: ADAPTING SWISS GOVERNANCE MODELS TO SECURE PAKISTAN’S CRITICAL INFRASTRUCTURE AGAINST GLOBAL CORPORATE HEGEMONY”

Research Paper

Umar Iqbal Butt, SSBM Research, Geneva, Switzerland, omar.iqbal@live.com, ORCID: 0000-0002-8835-9610

“Abstract”

Pakistan legally owns its most consequential national assets yet does not operationally control them. The SCADA systems governing the Reko Diq mining complex and the national energy grid are managed by foreign entities under foreign jurisdictions, a condition this article terms Digital Suzerainty. Using a comparative case study, the article benchmarks Pakistan’s critical infrastructure governance against Switzerland’s National Cyber Strategy. Three findings emerge. First, Pakistan’s Prevention of Electronic Crimes Act lacks data residency mandates, sovereign key management and vendor liability frameworks. Second, both Reko Diq and the CPEC energy grid exhibit dependency configurations associated with state-sponsored operational freeze attacks. Third, the proposed Pakistan Sovereign Stack offers a phased, technically specific blueprint for Strategic Decoupling that is reproducible across resource-dependent Global South economies.

Keywords: Digital Sovereignty, Critical Infrastructure, Pakistan, Switzerland, CPEC, Pakistan Sovereign Stack.

1 Introduction

1.1 The emergence of digital suzerainty

Contemporary geopolitical competition has migrated from territorial control to the governance of digital operational layers. A nation that retains legal title to its natural resources but cannot operate, audit, or protect the software systems governing their extraction has traded substantive sovereignty for a formal shell. This article terms that condition *Digital Suzerainty*: the state in which physical ownership of a strategic asset is legally intact but operationally contingent on the cooperation of foreign-domiciled corporate intermediaries. Pakistan’s critical infrastructure has arrived, through successive procurement decisions made under financial and diplomatic pressure, at precisely this condition.

Musiani (2022) argues that digital sovereignty is not proclaimed through legislation but is materially constructed through infrastructure design choices. Every procurement decision that routes a state’s operational data through a foreign cloud environment, every SCADA deployment that does not include a domestic audit layer, and every service contract that leaves encryption key management with the vendor represents a withdrawal of sovereignty in practice regardless of what the law says in theory. Azevedo et al. (2024) provide empirical grounding: their Domain Name System (DNS)-level analysis demonstrates that critical infrastructure sectors face quantifiable sovereignty risks proportional to their concentration of reliance on foreign-domiciled digital providers.

1.2 The corporate intermediary problem

The mechanism through which sovereign assets become vulnerable is not military but corporate. Clayton, Maggiori and Schreger (2025) formalise what practitioners have observed: the same economic interdependencies that generate gains from integration create the structural conditions for coercion. A

foreign government wishing to inflict operational damage on a rival's strategic assets need not deploy military assets if it can compel its resident technology firms to revoke licences, suspend access, or trigger remote system responses under the guise of compliance with sanctions or export controls. The European Commission's own Economic Security Strategy, cited in Clayton, Maggiori and Schreger (2025), recognises explicitly the "risks of weaponisation of economic dependencies or economic coercion."

The United States Clarifying Lawful Overseas Use of Data (CLOUD) Act provides the paradigmatic legal instrument. Blancato (2023) documents that it requires American cloud service providers to disclose data in their possession to US law enforcement "regardless of where the data is stored" — a geography-agnostic jurisdictional claim that renders physical data localisation meaningless unless combined with domestic key management. Mann and Daly (2020) demonstrate that this mechanism weaponises corporate intermediaries as instruments of state power across international borders. Pakistan, whose strategic assets are operationally managed through systems built on US-aligned cloud infrastructure and Chinese SCADA technology (Hassan, 2025; Menhas et al., 2019), is exposed to both vectors simultaneously.

1.3 Research questions and contributions

This article addresses three research questions: (RQ1) Does Pakistan's existing legislative framework provide adequate protection against corporate-mediated digital coercion of its critical infrastructure? (RQ2) What specific operational vulnerabilities exist in Pakistan's Reko Diq and energy grid architectures? (RQ3) Can the Swiss National Cyber Strategy (NCS) governance benchmark be adapted into a technically actionable framework for Pakistan without requiring constitutional change or foreign capital injection?

The article makes three original contributions. First, it applies Switzerland's NCS as a governance benchmark to a non-European emerging economy for the first time, bridging a gap identified by Qu, Yuan and Xu (2025), who note that cross-national comparative digital sovereignty research has been heavily skewed toward Organisation for Economic Co-operation and Development (OECD) contexts. Second, it provides a legally specific five-dimension gap analysis of Pakistan's PECA against international best practice, drawing on Bokhari's (2023) empirical finding that ambiguity in Pakistan's cybersecurity legislation is a primary obstacle to effective implementation. Third, it proposes the Pakistan Sovereign Stack (PSS) as a modular, phased framework for strategic digital decoupling that is institutionally actionable within Pakistan's existing political economy.

2 Literature Review

2.1 Digital sovereignty: from concept to operational architecture

The concept of digital sovereignty has undergone significant evolution in the academic literature. Pohle, Nanni and Santaniello (2024) trace its migration from a fringe concept associated with Chinese internet governance to a mainstream policy framework embraced by the European Union, India, and Brazil, among others. They document six distinct conceptions deployed simultaneously within European Union (EU) policy discourse alone, ranging from security imperatives to economic protectionism. This conceptual plurality, they argue, risks rendering the term analytically vacuous unless anchored to operational specifics. Adler-Nissen and Eggeling (2024) reach a similar conclusion from their analysis of the Gaia-X European cloud project, identifying three possible trajectories for digital sovereignty discourse: constitutional co-existence, hegemony of a single conception, or collapse from internal contradiction.

Musiani (2022) offers the most rigorous infrastructure-theoretic framework: sovereignty in the digital sphere is embedded in the material choices of procurement, architecture, and operational design, not in legal declarations. A state whose critical systems run on foreign-controlled code, foreign-hosted data, and foreign-managed encryption keys has ceded sovereignty in practice regardless of what its constitution or statute book claims. Azevedo et al. (2024) operationalise this insight at the network layer, demonstrating that sovereignty risks are directly measurable through DNS dependency concentration

ratios. The present article adopts Musiani's infrastructure-theoretic definition and Azevedo's operationalisation logic, applying both to the specific case of Pakistan's strategic resource and energy sectors.

2.2 Critical infrastructure governance: comparative political economy

The governance of critical information infrastructure varies systematically with political economy structures. Calcara and Marchetti (2021) distinguish between public governance ecosystems — characterised by formal state-industry coordination, centralised institutions, and high public investment in security standards — and private governance ecosystems defined by arm's-length regulatory relationships and market-led security provision. Their comparative analysis of France and the United Kingdom demonstrates empirically that public governance ecosystems produce more coherent and effective Critical Information Infrastructure (CII) protection outcomes. Maksan and Leško (2025), writing in this journal, reach a consistent conclusion from a practitioner perspective: because attacks on energy, transport and communication systems can escalate into economic, political and security crises, critical infrastructure protection demands a deliberate national strategy combining modern technology, a legal framework and international cooperation. Switzerland, with its mandatory standards framework, centralised NCSC enforcement, and requirement that all CII vendors submit to state audit, exemplifies the public governance model at its most developed.

The emerging-country dimension of CII governance is directly addressed by Timcke, Gaffley and Rens (2023) in their process-tracing case study of the 2021 ransomware attack on South Africa's Transnet state enterprise. Their key finding — that "cybersecurity policy needs to be a core dimension of contemporary socioeconomic development policy" and that procurement decisions made without sovereignty conditions constitute a "substantial risk to the functioning of the market" — provides direct methodological precedent for the forensic analysis conducted in this article. Malatji, Marnewick and von Solms (2021) similarly demonstrate in their analysis of South Africa's water sector that legislative fragmentation and the absence of sector-specific CII standards create governance vacuums that are structurally equivalent to the gap identified here in Pakistan's PECA. Bokhari (2023), analysing Pakistan directly through a survey of 172 banking and IT sector managers, finds that ambiguity in cybersecurity legislation is a primary independent predictor of implementation failure, with corruption and lack of technical expertise as reinforcing factors.

At the technical layer, Ribas Monteiro, Rodrigues and Zambroni de Souza (2023) provide the most comprehensive survey of cybersecurity vulnerabilities in cyber-physical power systems, establishing that Information Technology/Operational Technology (IT/OT) convergence has created attack surfaces that did not exist in earlier, air-gapped industrial control architectures. Sekonya and Sithungu (2023) synthesise these findings against the SysAdmin, Audit, Network, and Security (SANS) Institute's five critical ICS cybersecurity controls, confirming that the absence of asset inventory management and remote access governance — both absent in Pakistan's CPEC-managed grid — constitutes a critical structural weakness.

2.3 Economic coercion, weaponised interdependence, and the Global South

The formal economic literature on weaponised interdependence has matured rapidly in the period 2023–2025. Clayton, Maggiori and Schreger (2025) demonstrate through a multi-country structural model that hegemonic actors can leverage network centrality in global technology and financial systems to impose costs on dependent states far exceeding what direct military action would achieve, while maintaining plausible deniability. Their model predicts that the optimal target for such coercion is a state with high asset value, high technological dependency, and limited retaliatory capability — a description that applies precisely to Pakistan's situation vis-à-vis both its Western and Chinese technology dependencies.

Qu, Yuan and Xu (2025) provide the most recent cross-national empirical evidence on the pathways to digital sovereignty, using fuzzy-set qualitative comparative analysis (fsQCA) across 30 countries. Their central finding is that international cooperation, legal framework adequacy, and technological capability

must act in combination to achieve digital sovereignty — no single factor is sufficient. Critically, they find that countries relying on external cooperation alone without domestic legal framework or technical capability enter an "externally dependent pathway" characterised by persistent vulnerability. This finding directly characterises Pakistan's current trajectory: participation in CPEC digital infrastructure without corresponding domestic sovereignty architecture creates not protection but structured dependency.

Maxigas and ten Oever (2023) extend the coercion literature to physical infrastructure, demonstrating through their analysis of 5G vendor politics that infrastructure ideologies — the sociotechnical imaginaries embedded in technology choices — function as long-term geopolitical binding agents. Once a nation's critical infrastructure is built on a specific vendor's ecosystem, the cost of extraction creates a de facto lock-in that persists for decades. This analysis applies directly to Reko Diq's Engineering, Procurement, Construction, and Management (EPCM) architecture and the CPEC energy grid's SCADA deployment.

3 Methodology

3.1 Comparative case study design

This article employs a comparative case study methodology grounded in the comparative political economy framework of Calcara and Marchetti (2021). The case pair — Switzerland and Pakistan — is selected through the most-different-systems design logic of Przeworski and Teune (1970): the two cases are maximally different on observable dimensions of institutional capacity, economic development, and geopolitical position, but share the theoretically crucial structural characteristic that both are unable to rely on military deterrence or market power to enforce digital security. Switzerland's commitment to armed neutrality and Pakistan's formal non-alignment policy constitute the shared posture dimension that makes the comparison analytically meaningful.

The most-different-systems design provides strong inferential warrant for policy transfer: if a governance principle is sufficient to achieve effective CII sovereignty in the most institutionally demanding case (Switzerland, a small federal state managing four official languages, a complex federal-cantonal governance structure, and membership of no military alliance), then its core principles are robust candidates for adaptation to other small-state contexts. Switzerland's NCS is thus treated as a "positive deviant" case in the sense of Timcke, Gaffley and Rens (2023): a case that achieves an outcome that theory and standard practice would not predict for a state of its size and geopolitical exposure.

3.2 Analytical framework: three-stage forensic audit protocol

The analytical framework applies a three-stage forensic audit protocol designed to derive findings that are both empirically grounded and institutionally actionable. Stage 1 is **dependency mapping**: systematic identification of all points at which Pakistan's CII systems are operationally controlled by foreign-domiciled entities, drawing on primary sources from Barrick Mining Corporation (2026) and Barrick Mining Corporation (2025), and the CPEC digital infrastructure documentation reviewed in Hassan (2025) and Menhas et al. (2019). Stage 2 is **legislative gap analysis**: comparison of Pakistan's PECA against the Swiss Federal Act on Data Protection (FADP) across the five regulatory dimensions identified by Dinh and Nguyen (2024) as necessary and sufficient for CII sovereignty, with the gap level assessed on a three-point scale (None / Partial / Full). Stage 3 is **framework construction**: specification of the minimum necessary technical and legislative interventions to achieve the Swiss sovereignty threshold within Pakistan's institutional constraints, evaluated against the criterion of operational actionability — each element must be implementable without constitutional amendment, without foreign capital injection, and without requiring Pakistan to develop a domestic technology industry.

3.3 Data sources and limitations

Three categories of source material are employed: (1) primary policy documents, comprising the Swiss NCS (Swiss Federal Council, 2023), the NCSC's sector-specific Information and Communications

Technology (ICT) Minimum Standards (NCSC Switzerland, 2026; Federal Office for National Economic Supply, 2023), Barrick Mining Corporation's 2026 Reko Diq project update and 2025 annual report; (2) secondary peer-reviewed literature retrieved through systematic searches of the scite and Scholar Gateway databases; and (3) ICS security technical documentation from IEEE and ECCWS conference proceedings. Three limitations constrain the analysis. First, the study establishes feasibility and necessity but cannot quantify the welfare gains from PSS adoption. Second, it relies on publicly available documentation; proprietary contracts may contain sovereignty provisions not visible in public sources. Third, the Swiss governance model's replicability in Pakistan depends on institutional capacity-building timelines that this article cannot estimate. Future quantitative research should measure dependency concentrations through network-level audits and model transition economics using the framework of Qu, Yuan and Xu (2025).

4 Results

4.1 The Swiss benchmark: armed digital neutrality in practice

The Swiss National Cyber Strategy (NCS), together with its 2025 implementation programme and the mandatory critical-infrastructure incident-reporting regime in force since April 2025, operationalises what Ristolainen (2023) terms a "techno-economic coalition" governance posture: a comprehensive, standards-based architecture that insulates CII from external coercion not through military deterrence but through architectural autonomy. Its three interlocking pillars distinguish it from less operationally specific governance frameworks. The first is binding, sector-specific ICT Minimum Standards for critical infrastructure operators, developed by the Federal Office for National Economic Supply (FONES) and, since March 2024, administered by the NCSC (NCSC Switzerland, 2026; Federal Office for National Economic Supply, 2023): mandatory for the electricity sector under the Electricity Supply Ordinance since July 2024 and for the gas sector since July 2025, with additional sector standards in progress. The second is a statutory mandatory-reporting regime: since 1 April 2025, operators of designated critical infrastructure sectors (energy, water, finance, healthcare, telecommunications, transport, and others) are legally required under Articles 74a–74f of the Information Security Act to report significant cyberattacks to the NCSC within twenty-four hours of detection, with fines of up to CHF 100,000 for non-compliance (NCSC Switzerland, 2026). The third is centralised institutional authority: since becoming a full federal office on 1 January 2024, the NCSC has consolidated technical analysis, incident response, and standards enforcement under a single accountable body, backed by a CHF 10 million budget increase for 2026 and a further CHF 5 million from 2027 (NCSC Switzerland, 2026) — a provision that directly addresses the attack vector documented by Olijnyk, Bond and Rrushi (2022) in their physics-centric malware analysis.

Calcara and Marchetti (2021) classify this architecture as a public governance ecosystem: a model in which the state maintains formal institutional relationships with technology vendors, sets mandatory standards, and exercises centralised audit authority. Their comparative analysis of France and the United Kingdom establishes empirically that this model outperforms private governance ecosystems on CII protection metrics. The Swiss model does not merely aspire to sovereignty; it enforces it through audited compliance.

4.2 Finding 1: the legislative vacuum

The first finding was derived through the Stage 2 legislative gap analysis described in Section 3.2. The analytical process proceeded in four steps. First, the three-element sovereignty framework established by Dinh and Nguyen (2024) was adopted as the minimum threshold: (a) data residency mandates preventing state data from being stored in foreign-governed environments; (b) sovereign key management preventing foreign vendors from possessing decryption authority; and (c) vendor liability frameworks imposing criminal or civil consequences for sovereignty breaches. Second, the full text of Pakistan's Prevention of Electronic Crimes Act 2016, including its 2021 amendment, was examined systematically for provisions responsive to each element. Consistent with Bokhari's (2023) empirical

finding that ambiguity in Pakistan's cybersecurity legislation is a primary predictor of implementation failure, the search yielded no relevant provisions on any element. Third, the comparison was extended across the five operational dimensions identified in the Swiss NCS framework: data residency, encryption key management, vendor accountability, audit rights, and firmware security controls. Fourth, a gap level was assigned on a three-point scale (None, Partial, Full) by matching each PECA provision against the corresponding Swiss FADP standard.

Table 1 presents the results of this five-dimension legislative gap analysis. The divergence is categorical: PECA scores at the None level across all five dimensions, while the Swiss FADP achieves Full compliance on all five. This is not a gap that can be closed through incremental amendment; it requires purpose-built legislation.

Regulatory Dimension	Swiss FADP Standard	Pakistan PECA Status	Gap Level	Proposed PSS Sovereign Infrastructure Act Clause	Impl. Phase
Data Residency	Mandatory for all CII. Data must remain in Swiss-controlled servers. Extraterritorial storage prohibited for state-designated assets.	Absent. PECA contains no provision specifying where CII data must be stored or processed.	None	Mandatory domestic data residency for all PSS-designated CII assets; criminal penalties for non-compliance.	Phase 1
Encryption Key Management	Sovereign key custody mandatory. No foreign-domiciled service provider. State holds all master keys.	Absent. PECA's encryption provisions address cybercrime evidence handling, not sovereign key management for CII.	None	National Master Key Mandate establishing state-exclusive decryption authority over all CII operational data.	Phase 1
Vendor Accountability	Mandatory security guarantees. Criminal liability for CII vendors whose systems create exploitable sovereignty gaps.	Absent. Vendor contracts are governed by private commercial law with broad indemnification clauses; no sovereignty liability standard exists.	None	Strict Sovereignty Liability Clause: vendors face criminal exposure for any data exfiltration or access facilitated to foreign governments.	Phase 1
Independent Audit Rights	Annual independent state audit of all CII vendors. Audit findings are legally binding and trigger mandatory remediation.	Absent. PECA contains no provision for state-initiated technical audits of CII service providers or their systems.	None	Mandatory bi-annual independent technical audit of all PSS-designated systems; non-compliance triggers licence revocation.	Phase 2
Firmware Security Controls	State pre-approval and independent verification required for all CII firmware updates. Source code escrow mandatory.	Absent. No provision in PECA or subordinate regulations requires pre-approval, escrow, or independent verification of firmware.	None	Mandatory state pre-approval and source code escrow for all firmware updates to CII-designated industrial control systems.	Phase 2

Table 1. Finding 1 — Five-Dimension Legislative Gap Analysis: Swiss FADP vs. Pakistan PECA vs. Proposed PSS Sovereign Infrastructure Act. Sources: Swiss Federal Council (2023); NCSC Switzerland (2026); Prevention of Electronic Crimes Act Pakistan (2016, amended 2021); Dinh and Nguyen (2024).

Table 1 reveals a categorical legislative vacuum, not a marginal gap. Pakistan's PECA scores at the None level across all five dimensions. The Swiss FADP achieves Full compliance on all five. This pattern confirms Bokhari's (2023) empirical finding at the structural level: Pakistan's cybersecurity legislation was designed for an entirely different threat model — domestic cybercrime and online speech regulation — and is not merely inadequate for CII sovereignty protection; it is architecturally irrelevant to it. The gap cannot be closed through amendment of PECA; it requires a dedicated Sovereign Infrastructure Act that addresses each of the five dimensions as a legally separate and independently enforceable obligation.

4.3 Finding 2: operational freeze risk — mapping Pakistan's exposure

The second finding was derived through the Stage 1 dependency mapping protocol described in Section 3.2. The analytical process proceeded in three steps. First, the current digital management architecture of Reko Diq and the CPEC energy grid was mapped from primary sources. For Reko Diq, the Barrick Mining Corporation (2026, 2025) disclosures identify EPCM contract structures under which geological mapping data — the informational DNA of Pakistan's mineral wealth — is processed in cloud environments controlled by international engineering contractors, with Fluor Corporation (United States) engaged as lead EPCM contractor for the project. Barrick Mining Corporation (2026) subsequently announced that development activity at Reko Diq would be slowed and the project review extended to mid-2027 in response to escalating security risks in Pakistan and the region, with possible significant increases to the previously disclosed Phase 1 capital cost of USD 5.6–6.0 billion and Phase 2 cost of USD 3.3–3.6 billion. That slowdown alters the project timeline but not the governance architecture analysed here: the EPCM contract structures, the cloud processing of geological data and the absence of Pakistani-held encryption keys persist under reduced capital spend, and a project held under extended review by a foreign operator is if anything more exposed to the dependency configurations set out below, not less. For the CPEC energy grid, Hassan (2025) and Menhas et al. (2019) document the digital integration architecture, confirming that SCADA control systems for CPEC-financed power generation capacity are managed by Chinese-domiciled vendors under contractual arrangements that do not include independent Pakistani audit rights.

Second, both architectures were cross-referenced against the ICS attack vector typology established by Ribas Monteiro, Rodrigues and Zambroni de Souza (2023), Sekonya and Sithungu (2023), and Olijnyk, Bond and Rrushi (2022). Four specific attack vectors were identified as immediately applicable: (V1) SCADA access freeze through foreign vendor compulsion; (V2) geological database lockout through cloud access revocation; (V3) firmware injection via remote update channel; and (V4) CLOUD Act-compelled data disclosure. Third, each vector was matched against documented historical precedents and assessed against the protective measures currently in place in Pakistan's architecture.

Table 2 presents the operational vulnerability matrix derived from this analysis. Across four critical asset configurations and four attack vectors, the assessment finds zero protective measures in place for any vector against any asset.

CII Asset	Current Control Architecture	Foreign Control Layer	Primary Attack Vector	Documented Precedent	Protective Measures in Place	Risk Level
Reko Diq — Geological Data Systems	Geological mapping and resource estimation data processed by international EPCM contractors.	internationally domiciled cloud environments; no Pakistani-held encryption keys.	V2: Cloud access revocation / database lockout under diplomatic pressure or sanctions regime.	SAP licence revocation from Russian state enterprises (2022); SWIFT exclusion (2022).	None	Critical
Reko Diq — SCADA Operational	Real-time equipment telemetry and	Foreign-managed SCADA	V1: SCADA access freeze triggered by	Transnet ransomware attack, South	None	Critical

CII Asset	Current Control Architecture	Foreign Control Layer	Primary Attack Vector	Documented Precedent	Protective Measures in Place	Risk Level
Control	operational control outsourced to EPCM contractor digital infrastructure.	workstations; no independent Pakistani audit layer or parallel control capability.	contractor system suspension or foreign government compulsion.	Africa (2021): operations halted for seven days. (Timcke et al., 2023)		
CPEC Energy Grid — SCADA Control Layer	Load balancing, demand forecasting, and fault detection managed through CPEC vendor SCADA deployments.	Chinese-domiciled SCADA vendor; no mandatory Pakistani pre-approval for system changes or access.	V1: SCADA access freeze or manipulation during diplomatic deterioration. V4: CLOUD Act data disclosure.	BlackEnergy Advanced Persistent Threat (APT) attack, Ukraine (Dec. 2015): 6-hour grid outage, 230,000 affected. (Sekonya & Sithungu, 2023)	None	Critical
CPEC Energy Grid — Firmware Update Channel	Routine firmware updates to grid ICS equipment received remotely from Chinese-domiciled SCADA vendor without state pre-approval.	Vendor retains remote firmware update authority; no source code escrow or state verification requirement.	V3: Firmware injection delivering physics-centric malware capable of irreversible physical damage.	Aurora generator test, Idaho National Laboratory, 2007: malicious remote commands physically destroyed a generator. (Olijnyk et al., 2022)	None	Critical

Table 2. Finding 2 — Operational Vulnerability Matrix: Pakistan's Critical Infrastructure Exposure to Corporate-Mediated Freeze Attacks. Sources: Barrick Mining Corporation (2026, 2025); Hassan (2025); Menhas et al. (2019); Olijnyk, Bond and Rrushi (2022); Sekonya and Sithungu (2023); Timcke, Gaffley and Rens (2023).

Table 2 reveals a consistent pattern across all four asset configurations: zero protective measures are in place against any of the four identified attack vectors. The risk level is assessed as Critical for all assets, reflecting the combination of high asset value (Reko Diq reserves estimated at United States Dollars (USD) 500 billion; CPEC energy capacity representing a substantial fraction of Pakistan's national grid), demonstrated precedent for the attack vectors in analogous contexts, and complete absence of technical or legislative countermeasures. The forensic conclusion is unambiguous: Pakistan's most strategically consequential assets can be immobilised through corporate-mediated instruments without military action, without warning, and without any legal recourse under the current PECA framework.

4.4 Finding 3: the Pakistan Sovereign Stack as an actionable framework

The third finding was derived through the Stage 3 framework construction protocol described in Section 3.2. The analytical process proceeded in four steps. First, the Swiss NCS was reverse-engineered into its minimum viable components — the smallest set of legislative and technical elements that, taken together, achieve the Armed Digital Neutrality threshold against each of the four attack vectors identified in Finding 2. Second, each component was evaluated against Pakistan's institutional constraints: Does it require constitutional amendment? Does it require foreign capital? Does it require a domestic technology industry that does not exist? Components failing any of these tests were redesigned. Third, the resulting framework was validated against the World Trade Organization (WTO) trade compatibility criterion — Qu, Yuan and Xu (2025) identify this as a persistent barrier to data localisation policies in emerging nations — confirming that phased data residency requirements, as implemented in Switzerland, are consistent with existing trade agreements when applied to state-designated CII assets

rather than general commercial data. Fourth, the components were sequenced into three implementation phases based on urgency, technical complexity, and institutional capacity requirements.

Table 3 presents the resulting PSS framework, comprising five legislative and two technical components across three implementation phases. Figure 1, which follows, presents the architecture of the complete PSS system as a layered governance model.

PSS Component	Type	Description	Swiss Precedent	Vulnerability Addressed	Impl. Phase	Institutional Actionability
Sovereign Infrastructure Act	Legislative	Primary CII sovereignty legislation establishing data residency, key management, vendor liability, audit rights, and firmware controls as legally enforceable obligations.	Swiss FADP 2023; NCS mandatory standards framework.	V1, V2, V3, V4 (systemic)	Phase 1	Requires Parliamentary passage only; no constitutional amendment needed. Precedent: PECA itself.
National Master Key Mandate	Legislative + Technical	Establishes state-exclusive decryption authority over all CII operational data. No foreign-domiciled provider may hold or access Pakistan-held encryption keys.	Modelled on Swiss sector ICT Minimum Standards and NCSC incident-reporting practice (this is a proposed PSS design element, not an existing Swiss legal mandate).	V4: CLOUD Act data disclosure compulsion	Phase 1	Implementable through NITB (National IT Board); requires hardware security module procurement. No constitutional barrier.
Firmware Pre-Approval and Source Code Escrow	Legislative + Technical	All firmware updates to CII-designated ICS systems require state pre-approval and independent verification. Vendors must deposit source code in a sovereign escrow facility.	ICT Minimum Standard: ICS change and patch management (Federal Office for National Economic Supply, 2023).	V3: Firmware injection / physics-centric malware delivery	Phase 1	Requires PTA (Pakistan Telecom Authority) regulatory expansion; no new agency needed.
Mandatory Bi-Annual CII Technical Audit	Legislative	Independent technical audits of all PSS-designated systems every 24 months. Non-compliance triggers mandatory licence revocation and operational handover to domestic operators.	NCSC Switzerland annual CII vendor audit programme, operational since 2017.	V1, V2: Detection of embedded access pathways	Phase 2	Requires training of 50–100 state-certified ICS auditors; achievable through Swiss-Pakistan Partnership.
Blockchain Mineral Data Ledger	Technical	Immutable, cryptographically secured blockchain ledger for all Reko Diq geological data, extraction volumes, and revenue flows.	Swiss cantonal land registry blockchain pilots (2023–2025); Swiss Federal Financial Market Infrastructure Act.	V2: Geological database lockout / data manipulation	Phase 1	Deployable on existing NITB cloud infrastructure; no new hardware required beyond validator nodes.

PSS Component	Type	Description	Swiss Precedent	Vulnerability Addressed	Impl. Phase	Institutional Actionability
		Operates on sovereign Pakistani infrastructure with state-controlled validator nodes.				
Vendor Sovereignty Liability Clause	Legislative	Any vendor facilitating foreign government access to CII operational data or systems faces criminal prosecution under Pakistani law, with minimum seven-year imprisonment and mandatory asset seizure.	Swiss criminal liability for CII data breaches under revised FADP 2023, Article 61.	V1, V2, V4: Deterrence of corporate intermediary cooperation with hostile foreign actors	Phase 1	Included in Sovereign Infrastructure Act; no separate legislative vehicle required.
Policy Contagion Detection System	Technical	Real-time anomaly detection across all PSS-designated systems, using network telemetry and software update pattern analysis to identify early signatures of coordinated external digital action before operational impact.	ICT Minimum Standard 'Detect' function for CII operational systems (Federal Office for National Economic Supply, 2023), aligned with International Electrotechnical Commission (IEC) 62443 standard.	V1, V3: Early warning of SCADA manipulation and firmware attack preparation	Phase 2	Deployable on NITB infrastructure; requires integration with SCADA monitoring systems in Phase 1.

Table 3. Finding 3 — Pakistan Sovereign Stack: Legislative and Technical Framework Components. Sources: NCSC Switzerland (2026); Swiss Federal Council (2023); Dinh and Nguyen (2024); Azevedo et al. (2024); Qu, Yuan and Xu (2025); author's framework synthesis.

Table 3 demonstrates that the PSS is institutionally actionable: five of the seven components are deployable in Phase 1 without constitutional amendment, new agency creation, or foreign capital. The two Phase 2 components — the mandatory audit programme and the Policy Contagion Detection System — require institutional capacity-building that can be achieved through the Swiss–Pakistan Security Partnership proposed in Section 6. All seven components address specific attack vectors identified in Table 2, ensuring that the framework is forensically grounded rather than aspirationally generic.

Figure 1 presents the complete PSS architecture as a layered governance model, illustrating the vertical integration from current vulnerability exposure through legislative and technical remediation layers to the institutional arrangements that sustain the framework over time.

FIGURE 1 — PAKISTAN SOVEREIGN STACK: LAYERED GOVERNANCE ARCHITECTURE

CURRENT STATE — DIGITAL SUZERAINTY
Reko Diq: Foreign EPCM Cloud • Energy Grid: Chinese SCADA • Zero domestic encryption keys • No audit rights • No firmware controls

▼ PSS Intervention Architecture ▼

LAYER 1 — LEGISLATIVE FRAMEWORK (Phase 1)
Sovereign Infrastructure Act • National Master Key Mandate • Vendor Sovereignty Liability Clause • Data Residency Mandate

LAYER 2 — KEY MANAGEMENT & DATA SOVEREIGNTY (Phase 1)

Figure 1. Pakistan Sovereign Stack (PSS): Layered Governance Architecture from Current Vulnerability State to Armed Digital Neutrality. Source: Author's framework synthesis, derived from Swiss Federal Council (2023) and NCSC Switzerland (2026).

5 Discussion

The three findings presented in Section 4 converge on a single strategic diagnosis: Pakistan's critical infrastructure operates in a condition of structural digital dependency that is simultaneously a legislative vacuum, an operational security crisis, and a solvable policy problem. The legislative vacuum finding (Finding 1) and the operational vulnerability finding (Finding 2) are jointly necessary to establish the problem's severity; the PSS framework (Finding 3) is the response that they jointly necessitate.

The findings have three implications that extend beyond Pakistan. First, they confirm the cross-national validity of Qu, Yuan and Xu's (2025) central finding that international cooperation alone, without domestic legal framework and technical capability, produces the "externally dependent pathway" to digital vulnerability rather than digital sovereignty. Pakistan's CPEC participation exemplifies this trajectory precisely: a state that has accepted digital infrastructure investment without insisting on domestic sovereignty conditions has not acquired a resource but incurred a structured dependency. The PSS framework addresses this by requiring that the legal and technical sovereignty conditions be established before, not after, infrastructure integration.

Second, the findings support Timcke, Gaffley and Rens's (2023) argument that cybersecurity must be a core dimension of socioeconomic development policy, not a technical afterthought. Reko Diq's USD 500 billion reserve valuation and the CPEC energy grid's centrality to Pakistan's industrial development programme mean that the economic stakes of digital vulnerability are not marginal but existential at the national scale. Clayton, Maggiori and Schreger's (2025) formal model establishes that the welfare costs of hegemonic coercion through technology dependencies are bounded only by the economic significance of the targeted asset. Reko Diq and the national grid set that bound very high indeed.

Third, the PSS framework's design as a reproducible methodology for Global South economies addresses the gap identified by Qu, Yuan and Xu (2025): that existing digital sovereignty frameworks have been developed in and for OECD institutional contexts and do not transfer readily to emerging economies with different institutional capacities, different legal traditions, and different technology dependency profiles. The PSS's phased implementation structure, its reliance on existing Pakistani institutions rather than new agency creation, and its explicit WTO-compatibility validation constitute a transfer engineering effort that the existing literature has not previously attempted at this level of operational specificity.

The study's limitations, acknowledged in Section 3.3, suggest directions for future quantitative research. Specifically, the dependency concentration ratios for Pakistan's Reko Diq and energy grid architectures, analogous to the DNS concentration metrics of Azevedo et al. (2024), would provide empirical grounding for the risk levels assessed in Table 2. Bokhari's (2023) survey methodology, adapted to the CII sector specifically, could produce implementation gap data that would allow the Phase 1–3 timeline in Table 3 to be calibrated against actual institutional capacity.

Figure 2 synthesises the maturity gap across all five regulatory dimensions by placing Pakistan's current and projected PSS-enabled sovereignty posture alongside Switzerland and the European Union. The comparison makes visually explicit what Table 1 established analytically: Pakistan's current architecture scores zero across all five dimensions, while Switzerland achieves full compliance on all five and the EU achieves substantive but partial coverage in three to four. The figure also illustrates the PSS's intended endpoint: full alignment with the Swiss benchmark on all five dimensions, closing the maturity gap through the phased legislative and technical interventions detailed in Table 3. Jiang (2024), in a cross-national analysis of digital sovereignty models across China and South Africa, argues that emerging economies must reconceptualise digital sovereignty not merely as territorial legal doctrine but as a function of "digital capacity, self-sufficiency and autonomy." Figure 2 operationalises that reconceptualisation, translating it into a measurable five-dimension maturity model that Pakistan can use to benchmark its PSS implementation progress against established international comparators. Arnold (2022), studying digital market integration in East Africa, similarly finds that emerging nations that rely on foreign technology providers without building domestic sovereignty architecture remain in "a subordinate political position in global power relations" — a condition Figure 2's current Pakistan column captures with uncomfortable precision.

Figure 2 — Digital Sovereignty Maturity Comparison

Sovereignty Dimension	Switzerland (NCS)	European Union (GDPR / ENISA)	Pakistan Current (PECA)	Pakistan with PSS
● Full ◗ Partial ○ None — Legend				
Data Residency	● **Mandatory All CII**	◗ Partial Some sectors	○ Absent Not specified	● **Full All CII assets**
Encryption Key Management	● **Sovereign key custody – zero vendor access**	◗ Partial Varied standards	○ Absent Vendor-controlled	● **Full National Master Key**
Vendor Accountability	● **Criminal Liability**	◗ Partial AI Act coverage	○ Absent Indemnified	● **Full Sovereignty clause**
Independent Audit Rights	● **Annual Mandatory**	◗ Partial Sector-specific	○ Absent No CII audit	● **Bi-annual All PSS systems**
Firmware Security Controls	● **Pre-approval Source escrow**	◗ Partial Sector-led	○ Absent No provisions	● **Full State pre-approval**
Overall Sovereignty Score	**5 / 5 Full Protection**	3–4 / 5 Substantial	**0 / 5 No Protection**	**5 / 5 Full Protection**

Figure 2. Digital Sovereignty Maturity Comparison: Switzerland, European Union, Pakistan (Current) and Pakistan with PSS across Five Regulatory Dimensions. Sources: Swiss Federal Council (2023); NCSC Switzerland (2026); Dinh and Nguyen (2024); Jiang (2024); author's comparative assessment based on Swiss Federal Council (2023) and NCSC Switzerland (2026) standards.

6 Conclusions

This article set out to answer three research questions concerning Pakistan's critical infrastructure exposure to corporate-mediated digital coercion and the viability of the Swiss NCS as a governance benchmark for remediation. The forensic audit conducted across three analytical stages established the following answers.

RQ1 — Legislative Adequacy: No. Pakistan's Prevention of Electronic Crimes Act (PECA) scores at the None level across all five dimensions of the legislative gap analysis (data residency, key management, vendor accountability, audit rights, firmware controls). This finding, derived through systematic comparison against the Swiss FADP, confirms Bokhari's (2023) empirical observation that ambiguity and absence in Pakistan's cybersecurity legislation are structural rather than incidental features. A purpose-built Sovereign Infrastructure Act is required; incremental PECA amendment is insufficient.

RQ2 — Operational Vulnerabilities: Both Reko Diq and the CPEC energy grid are fully exposed to all four identified attack vectors (SCADA access freeze, geological database lockout, firmware injection, CLOUD Act data disclosure) with zero protective measures in place. The attack precedents are documented: the 2015 BlackEnergy attack on Ukraine's grid, the 2021 Transnet ransomware attack in South Africa, and the 2022 SAP licence revocations from Russian enterprises collectively constitute an operational playbook for the vulnerabilities identified in Table 2.

RQ3 — Framework Viability: Yes. The Pakistan Sovereign Stack's seven components — five legislative and two technical — are all institutionally actionable within Pakistan's existing political economy without constitutional amendment, without foreign capital injection, and without requiring domestic technology industry development. Five of the seven components are deployable in Phase 1 through existing institutions (National Information Technology Board (NITB), Pakistan Telecommunication Authority (PTA), Parliament). The framework is WTO-compatible and is designed as a reproducible template for other Global South economies facing analogous structural dependencies.

Two international initiatives follow directly from these conclusions. A formal *Swiss–Pakistan Security Partnership*, structured as a bilateral technical cooperation agreement between Pakistan's NITB and Switzerland's Federal Office for National Economic Supply (FONES) and NCSC, would provide the institutional knowledge transfer, audit methodology training, and technical standards alignment required to implement the Phase 2 components. A *Global South Digital Sovereignty Consortium*, modelled on the PSS architecture and open to resource-dependent non-aligned economies, would allow member states to federate Policy Contagion detection intelligence and negotiate collectively with technology vendors, creating the collective sovereignty that Ristolainen (2023) identifies as the only structurally adequate response to hegemonic digital coercion.

Digital neutrality is not a retreat from the global economy. For Pakistan, it is the technical and legislative precondition for participating in that economy as a sovereign peer rather than as a structured dependent — and the evidence assembled in this article establishes, unambiguously, that the gap between those two conditions is the difference between a policy choice and a national security emergency.

Declarations

Conflict of Interest: The author declares no conflict of interest.

Funding: This research received no external funding.

Data Availability: This is a conceptual and comparative analysis. All primary policy sources are publicly available from www.admin.ch and www.ncsc.admin.ch. All secondary sources are cited with full DOIs.

References

Adler-Nissen, R. and Eggeling, K. A. (2024) 'The Discursive Struggle for Digital Sovereignty: Security, Economy, Rights and the Cloud Project Gaia-X', *JCMS: Journal of Common Market Studies*, 62(4), pp. 993–1011. Available at: https://doi.org/10.1111/jcms.13594

Arnold, S. (2022) 'Drivers and Barriers of Digital Market Integration in East Africa: A Case Study of Rwanda and Tanzania', *Politics and Governance*, 10(2). Available at: https://doi.org/10.17645/pag.v10i2.4922

Azevedo, A. C., Scheid, E. J., Franco, M. F., Boeira, D. F. F., Zembruzki, L. and Granville, L. Z. (2024) 'The Role of Network Centralization in Shaping Digital Sovereignty: An Analysis Under the DNS Lens', *International Journal of Network Management*, 35(1). Available at: https://doi.org/10.1002/nem.2309

Barrick Mining Corporation (2025) *Annual Report 2025*. Toronto: Barrick Mining Corporation.

Barrick Mining Corporation (2026) *Barrick Provides an Update on Reko Diq*. Toronto: Barrick Mining Corporation, 2 April [Online]. Available at: https://www.barrick.com/English/news/news-details/2026/barrick-provides-an-update-on-reko-diq/default.aspx (Accessed: 18 September 2026).

Blancato, F. G. (2023) 'The Cloud Sovereignty Nexus: How the European Union Seeks to Reverse Strategic Dependencies in its Digital Ecosystem', *Policy & Internet*, 16(1), pp. 12–32. Available at: https://doi.org/10.1002/poi3.358

Bokhari, S. A. A. (2023) 'A Quantitative Study on the Factors Influencing Implementation of Cybersecurity Laws and Regulations in Pakistan', *Social Sciences*, 12(11), 629. Available at: https://doi.org/10.3390/socsci12110629

Calcara, A. and Marchetti, R. (2021) 'State-Industry Relations and Cybersecurity Governance in Europe', *Review of International Political Economy*, 29(4), pp. 1237–1262. Available at: https://doi.org/10.1080/09692290.2021.1913438

Clayton, C., Maggiori, M. and Schreger, J. (2025) 'A Theory of Economic Coercion and Fragmentation', *SSRN Electronic Journal*. Available at: https://doi.org/10.2139/ssrn.5076012

Dinh, T. H. and Nguyen, P. (2024) 'Protecting National Sovereignty in Cyberspace within the Context of Digital Globalization', *Eudaimonia*, 8(1), pp. 5–29. Available at: https://doi.org/10.51204/ivrs_24101a

Federal Office for National Economic Supply (2023) *Minimum Standard for Improving ICT Resilience*. Bern: Federal Office for National Economic Supply (FONES), revision May 2023.

Hassan, K. (2025) 'CPEC in the Digital Age: China's Success in Hard and Soft Power in Pakistan', *Global Media and Communication*, 21(1), pp. 91–106. Available at: https://doi.org/10.1177/17427665251336633

Jiang, M. (2024) 'Models of State Digital Sovereignty From the Global South: Diverging Experiences From China, India and South Africa', *Policy & Internet*, 16(4), pp. 727–738. Available at: https://doi.org/10.1002/poi3.427

Maksan, A. and Leško, L. (2025) 'Cyber Security of Critical Infrastructure', *Global Journal of Business and Integral Security*, 8(1). Available at: https://gbis.ch/index.php/gbis/article/view/921 (Accessed: 22 September 2026).

Malatji, M., Marnewick, A. L. and von Solms, S. (2021) 'Cybersecurity Policy and the Legislative Context of the Water and Wastewater Sector in South Africa', *Sustainability*, 13(1), 291. Available at: https://doi.org/10.3390/su13010291

Mann, M. and Daly, A. (2020) 'Geopolitics, Jurisdiction and Surveillance', *Internet Policy Review*, 9(3). Available at: https://doi.org/10.14763/2020.3.1501

Maxigas and ten Oever, N. (2023) 'Geopolitics in the Infrastructural Ideology of 5G', *Global Media and China*, 8(3), pp. 271–288. Available at: https://doi.org/10.1177/20594364231193950

Menhas, R., Mahmood, S., Tanchangya, P., Safdar, M. N. and Hussain, S. (2019) 'Sustainable Development under Belt and Road Initiative: A Case Study of China–Pakistan Economic Corridor's Socio-Economic Impact on Pakistan', *Sustainability*, 11(21), 6143. Available at: https://doi.org/10.3390/su11216143

Musiani, F. (2022) ‘Infrastructuring Digital Sovereignty: A Research Agenda for an Infrastructure-Based Sociology of Digital Self-Determination Practices’, *Information, Communication & Society*, 25(6), pp. 785–800. Available at: https://doi.org/10.1080/1369118x.2022.2049850

NCSC Switzerland (2026) *ICT Minimum Standards for Critical Infrastructure*. Bern: National Cyber Security Centre. Available at: https://www.ncsc.admin.ch/ncsc/en/home/infos-fuer/infos-it-spezialisten/themen/ikt-minimalstandards.html (Accessed: 18 September 2026).

Olijnyk, J., Bond, B. and Rrushi, J. (2022) ‘Design and Emulation of Physics-Centric Cyberattacks on an Electrical Power Transformer’, *IEEE Access*, 10, pp. 15227–15246. Available at: https://doi.org/10.1109/access.2022.3148046

Pohle, J., Nanni, R. and Santaniello, M. (2024) ‘Unthinking Digital Sovereignty: A Critical Reflection on Origins, Objectives, and Practices’, *Policy & Internet*, 16(4), pp. 666–671. Available at: https://doi.org/10.1002/poi3.437

Przeworski, A. and Teune, H. (1970) *The Logic of Comparative Social Inquiry*. New York: Wiley-Interscience.

Qu, R., Yuan, Y. and Xu, J. (2025) ‘Pathways to Safeguarding Digital Sovereignty Within a Multi-Level Governance Framework: A Cross-National Comparative Study Based on the fsQCA Method’, *Policy & Internet*, 17(3). Available at: https://doi.org/10.1002/poi3.70009

Ribas Monteiro, L. F., Rodrigues, Y. R. and Zambroni de Souza, A. C. (2023) ‘Cybersecurity in Cyber–Physical Power Systems’, *Energies*, 16(12), 4556. Available at: https://doi.org/10.3390/en16124556

Ristolainen, M. (2023) ‘Role of Techno-Economic Coalitions in Future Cyberspace Governance: Backcasting as a Method for Strategic Foresight’, in *Proceedings of the European Conference on Cyber Warfare and Security*, 22(1). Reading: Academic Conferences International, pp. 395–402. Available at: https://doi.org/10.34190/eccws.22.1.1078

Sekonya, N. and Sithungu, S. (2023) ‘An Analysis of Critical Cybersecurity Controls for Industrial Control Systems’, in *Proceedings of the European Conference on Cyber Warfare and Security*, 22(1). Reading: Academic Conferences International, pp. 410–419. Available at: https://doi.org/10.34190/eccws.22.1.1157

Swiss Federal Council (2023) *National Cyberstrategy (NCS)*. Bern: National Cyber Security Centre. Available at: https://www.bacs.admin.ch/en/national-cyberstrategy-ncs (Accessed: 18 September 2026).

Timcke, S., Gaffley, M. and Rens, A. (2023) ‘The Centrality of Cybersecurity to Socioeconomic Development Policy: A Case Study of Cyber-Vulnerability at South Africa’s Transnet’, *The African Journal of Information and Communication*, 32, pp. 1–28. Available at: https://doi.org/10.23962/ajic.i32.16949