STRATEGIC SYSTEMS

EXPOSED BY DESIGN

SCADA, ICS, AND THE CYBER VULNERABILITY OF PAKISTAN'S POWER GRID

Murtaza Asim Shehzad

2026

Executive Summary

On 1 March 2026, Pakistan's national communication satellite PakSat-1R was hijacked. For several minutes, its broadcast feed displayed scrolling anti-state messages before engineers regained control. No group claimed responsibility. No official attribution has been made. The incident lasted minutes. The question it raises will last much longer: if Pakistan's satellite infrastructure can be penetrated and weaponised for strategic messaging with apparent ease, what does that imply for infrastructure that is simultaneously more critical and less visible, the power grid?

This paper argues that Pakistan's electricity infrastructure, built on Supervisory Control and Data Acquisition (SCADA) and Industrial Control Systems (ICS), presents a Tier-1 national security exposure. The vulnerabilities are not hypothetical. They are the same classes of weakness that state-sponsored adversaries have already exploited to collapse power grids in Ukraine, probe infrastructure across Europe and North America, and attempt to trigger industrial explosions in the Middle East. Pakistan's grid is not meaningfully more secure than any of those targets. In several respects, it is less so.

Three findings anchor this assessment. First, Pakistan's grid architecture, aging legacy systems, inadequate IT/OT network separation, foreign vendor dependencies, and near-zero operational technology monitoring, creates an attack surface that Advanced Persistent Threats are designed to exploit. Second, Pakistan operates in a regional threat environment that includes state actors with both the capability and the strategic motivation to conduct sub-threshold infrastructure operations. Third, the institutional response, fragmented across NCCS, NEPRA, NTDC, and multiple DISCOs with no dedicated OT security mandate, is not commensurate with the threat.

The paper closes with a prioritised set of recommendations structured across three time horizons. It is submitted as a working paper, not a finished assessment, and the author explicitly invites challenge, correction, and expert input.

1. The Threat Is No Longer Hypothetical

On 1 March 2026, an unknown actor hijacked the uplink of PakSat-1R, Pakistan's national communication satellite operated by SUPARCO. For several minutes, the broadcast feed was replaced with scrolling text carrying anti-state messaging before ground engineers regained control. The technical execution, intercepting and overriding a satellite uplink, is not trivial. It requires either direct compromise of ground station infrastructure, exploitation of transponder access controls, or sophisticated signal injection. This was not a defacement of a government website. It was a demonstrated capacity to seize control of sovereign communications infrastructure and use it as a platform for strategic messaging.

No group has claimed responsibility. PEMRA and NCERT initiated audits. The news cycle has moved on.

That is precisely the problem.

The PakSat incident is significant not because of what was displayed on screen, but because of what it reveals about the broader posture of Pakistan's critical infrastructure security. If a national satellite's broadcast integrity can be compromised, even briefly, the question that follows is not whether other critical systems are vulnerable. It is which ones, how severely, and who already knows.

The answer, for Pakistan's power grid, is not reassuring.

The International Precedent

The strategic weaponisation of infrastructure cyber vulnerabilities is not a theoretical concern. It is a documented, repeating pattern with a clear trajectory toward greater sophistication and lethality.

Ukraine, 2015. The Sandworm APT group, executed the first confirmed cyber attack to cause a civilian power outage. Using BlackEnergy malware delivered via spear-phishing, they compromised three Ukrainian distribution companies, seized control of SCADA systems, remotely opened circuit breakers, and cut electricity to approximately 230,000 customers. Operators watched helplessly as their HMI screens went dark. Restoration required manual intervention at every affected substation.

Ukraine, 2016. Sandworm returned with Industroyer, the first malware built specifically to speak the native protocols of power grid control systems, including IEC 60870-5-101, IEC 60870-5-104, and IEC 61850. Industroyer did not exploit software bugs. It exploited the fundamental design of the protocols themselves, protocols built for reliability, not security, that authenticate nothing. The attack caused a one-hour blackout in Kyiv. More significantly, it demonstrated a reusable, modular framework for attacking any grid running these protocols, anywhere in the world.

Saudi Arabia, 2017. The Triton malware, developed with a level of ICS-specific expertise that analysts assess required state resources, targeted Triconex safety instrumented systems at a petrochemical facility. Safety systems are the last line of defence against catastrophic industrial accidents. Triton's objective was to disable them, not to cause an outage, but to cause a disaster while removing the mechanisms that would have contained it. The attack was only discovered because a software bug caused an unintended shutdown. The intent was mass casualties.

Mumbai, 2021. A prolonged power outage affecting the city's financial district coincided with reporting by Recorded Future identifying coordinated activity by an APT group, RedEcho, targeting ten Indian power sector organisations. Indian authorities later expressed uncertainty about a direct causal link between the APT activity and the outage. The uncertainty itself is instructive: the attack surface had been so thoroughly penetrated that attribution of a major blackout became genuinely unclear.

These incidents share four characteristics that define the threat Pakistan faces. The attackers are patient, dwell times measured in months before any disruptive action. They are knowledgeable, grid-specific operational understanding goes well beyond generic hacking capability. They are strategic, each incident achieved objectives beyond disruption, including

signalling, capability demonstration, and coercive leverage. And they are persistent, the same groups return, improve, and redeploy.

Why Pakistan Is Not a Bystander

Pakistan does not sit outside this threat landscape. It sits inside it, with several compounding factors that make its exposure acute.

The regional security environment is defined by persistent sub-conventional competition. India has significantly expanded its cyber capabilities over the past decade, including through the establishment of the Defence Cyber Agency in 2019. Both nations have demonstrated willingness to operate in the grey zone, below the threshold of conventional conflict, through proxy actors, information operations, and covert action. The cyber domain is a natural extension of this competition. Sub-threshold infrastructure operations offer exactly what grey zone actors seek: strategic impact, plausible deniability, and the ability to impose costs without triggering escalation.

Pakistan's infrastructure digitalization has accelerated, which has introduced large volumes of Chinese-supplied equipment and operational involvement into generation assets including Sahiwal Coal, Port Qasim, and multiple hydro projects. This creates a vendor dependency dimension that is analytically distinct from conventional APT threats and requires separate consideration.

Finally, Pakistan's grid is structurally fragile in ways that amplify the consequences of any disruption. Nationwide blackouts in January 2021 and January 2023, both caused by technical failures rather than attacks, demonstrated that the system can collapse without adversarial action. A deliberate, well-targeted cyber operation against the same system would not need to be particularly sophisticated to achieve cascading, nationwide effects.

The PakSat incident was a signal. The question is whether Pakistan's institutions are positioned to read it correctly.

2. What Pakistan's Grid Actually Looks Like

Understanding the cyber vulnerability of Pakistan's power grid requires understanding the grid itself, not in exhaustive technical detail, but well enough to see where the attack surface lives and why it is as exposed as it is.

The Architecture

Pakistan's electricity system operates across three functional layers: generation, transmission, and distribution.

Generation is the most fragmented layer. It includes public sector assets under WAPDA, primarily the major hydroelectric stations at Tarbela, Mangla, and Ghazi Barotha, alongside a large and growing portfolio of Independent Power Producers spanning thermal, coal, gas, and renewable sources. CPEC has added significant generation capacity through Chinese-financed and often Chinese-operated plants. Each generation facility runs its own ICS environment, managing turbine controls, switchgear, protection relays, and safety systems. The security posture of each facility is largely a function of whoever built and maintains it, there is no uniform standard.

Transmission is more centralised. The National Transmission and Despatch Company manages Pakistan's high-voltage network, operating at 220kV and 500kV, and is responsible for grid stability across the entire system. At its core is the National Power Control Centre in Islamabad, which serves as the real-time operational nerve centre of the grid. NPCC runs an Energy Management System and SCADA infrastructure that monitors grid frequency, manages load dispatch, and coordinates with generation and distribution entities. This is the highest-value target in Pakistan's electricity infrastructure. Compromise of NPCC's SCADA environment would not affect one region, it would affect the entire national grid simultaneously.

Distribution is the most dispersed and least secured layer. Ten Distribution Companies, LESCO, FESCO, IESCO, PESCO, HESCO, SEPCO, QESCO, MEPCO, GEPCO, and TESCO, serve distinct geographic territories. DISCOs vary enormously in operational capacity, financial health, and

technological investment. Most operate with significant legacy infrastructure and minimal cybersecurity capability.

Where the Vulnerabilities Live

This three-layer architecture creates an attack surface at every level, but the vulnerability profile concentrates around five structural weaknesses.

Legacy Systems Running Without Security Support

Much of Pakistan's grid control infrastructure was installed at a time when cybersecurity was not a design consideration. SCADA systems in older substations and generation facilities run on hardware and software that is no longer manufactured or supported. In many cases this means operating systems, Windows XP, Windows 7, for which Microsoft stopped issuing security patches years ago. Known exploits for these systems are publicly documented and freely available. Upgrading them is not straightforward: SCADA software is often certified to run on specific hardware and OS configurations, meaning a security patch can break operational functionality. The result is a rational but dangerous choice to keep running vulnerable systems rather than risk operational disruption during an upgrade.

Inadequate Separation Between IT and OT Networks

The Purdue Model, the standard architecture for industrial control system security, prescribes strict separation between enterprise IT networks and operational technology networks, with controlled, audited data flows between them. In practice, Pakistan's energy entities have progressively connected these environments for legitimate operational reasons: remote monitoring, data feeds to management systems, vendor access for maintenance. Each connection that bridges the IT-OT boundary is a potential pathway for an adversary who has compromised the enterprise network to reach operational systems. The 2015 Ukraine attack followed exactly this pathway. There is no technical reason to believe Pakistan's implementations are more rigorously segmented than Ukraine's were.

Foreign Vendor Dependencies and the CPEC Dimension

Pakistan's grid incorporates equipment from a wide range of international vendors, Siemens, ABB, GE, and increasingly Chinese manufacturers including Huawei and state-owned enterprises involved in CPEC projects. Vendor relationships create two distinct vulnerability vectors. The first is supply chain integrity: hardware and software supplied by vendors could contain vulnerabilities, backdoors, or malicious functionality. The second is maintenance access: vendors routinely retain remote access to equipment they have supplied for diagnostic and maintenance purposes. These remote access channels, if inadequately secured or monitored, represent persistent entry points into operational environments.

The CPEC dimension adds a geopolitical layer to what is already a technical concern. Chinese state-owned enterprises involved in operating CPEC generation assets occupy a position of deep technical access to Pakistani infrastructure. This is not a conspiratorial observation, it is a structural feature of the contractual and operational arrangements governing these assets, and it warrants analytical attention regardless of current bilateral relations.

Near-Zero Operational Technology Monitoring

Enterprise IT networks in most large organisations now run some form of continuous security monitoring. OT environments in Pakistan's energy sector have almost none of this. The reasons are partly technical, OT monitoring tools must be non-intrusive, because active scanning of industrial networks can disrupt the processes being protected. They are partly cultural, energy sector operations prioritise uptime, and security tooling is perceived as a risk to operational stability. And they are partly financial, dedicated OT security monitoring platforms are expensive and require specialised expertise to operate.

The consequence of this monitoring gap is that an adversary who achieves access to an OT network in Pakistan's grid could conduct reconnaissance, establish persistence, and pre-position for a disruptive operation over a period of months, potentially years, without detection. This is precisely what Dragonfly

and Sandworm did in their respective campaigns before executing disruptive operations.

The Protocols Themselves Are Unauthenticated

The communication protocols that carry control commands across Pakistan's grid, Modbus, DNP3, IEC 60870-5-104, IEC 61850, were designed for reliability in isolated environments. They were not designed for security in networked ones. Most carry no authentication: a command issued on the network is executed because it arrives in the right format, not because the system can verify it came from a legitimate source. An adversary with network access can issue control commands, open circuit breakers, manipulate protection relay settings, alter generator output, that are indistinguishable from legitimate operator commands. Industroyer exploited exactly this. It did not crack encryption or defeat authentication. There was nothing to crack or defeat.

The NPCC as the Critical Node

It is worth being explicit about what NPCC compromise would mean. The National Power Control Centre does not just monitor the grid, it actively manages it in real time, balancing generation and load, issuing dispatch instructions, and responding to faults. A successful attack on NPCC's EMS/SCADA environment that achieved the ability to issue false control commands, or simply to deny operators visibility of the grid state, would not produce a localised outage. It would produce the conditions for a nationwide cascade failure. Pakistan has demonstrated, twice in recent years through purely technical failures, that the grid can collapse nationally from a single point of failure propagating through an under-redundant system. A deliberate attack targeting NPCC would be engineering that collapse intentionally.

3. Who Would Do This and Why

Vulnerability without a credible threat actor is an engineering problem. Vulnerability with one is a national security problem. Pakistan's grid architecture presents an exploitable attack surface. This section addresses who has both the capability to exploit it and a strategic rationale for doing so.

Three threat categories are relevant: state-sponsored Advanced Persistent Threats operating with strategic objectives, the structural risk embedded in vendor and contractor relationships, and non-state actors operating with or without state facilitation. They are not mutually exclusive, the most dangerous scenarios involve combinations.

State-Sponsored APTs: Capability and Motivation

The India Vector

India has invested systematically in offensive cyber capability over the past decade. The establishment of the Defence Cyber Agency in 2019 formalised what had previously been distributed across military intelligence and signals organisations. Indian cyber operations have been documented against Pakistani targets across multiple domains by threat intelligence firms including Kaspersky and TrendMicro, which have tracked APT groups with India nexus including SideWinder and Transparent Tribe.

The strategic logic for targeting Pakistani energy infrastructure is straightforward: sub-threshold operations that impose economic cost, demonstrate capability, and create coercive leverage without triggering the escalatory dynamics of kinetic conflict. Energy infrastructure is a particularly attractive target because disruption is immediately visible to the population, economically damaging, and politically costly, all without a single soldier crossing a border.

This paper does not assert that India has conducted or is currently conducting operations against Pakistan's grid. It asserts that India possesses the capability, that documented India-nexus APT groups have demonstrated sustained interest in Pakistani targets, and that energy infrastructure aligns with the strategic logic of sub-threshold coercive operations. Whether the threat is active is an intelligence question, not an open-source one. Attribution assessments in cyber are probabilistic, not definitive.

The Vendor-State Nexus

The second state-level threat vector is structurally different and more complex. It does not require an adversary to penetrate Pakistan's grid from the outside. It is already inside.

Chinese state-owned enterprises and their subcontractors occupy positions of deep technical access across CPEC energy assets. Operational involvement in plants like Sahiwal Coal and Port Qasim means that Chinese personnel and systems are embedded in the ICS environments of facilities that collectively represent a significant share of Pakistan's installed generation capacity.

The analytical concern here is not about current intent. China and Pakistan maintain a strategic partnership that neither side has an obvious interest in destabilising. The concern is about structural access: the technical ability to affect Pakistani infrastructure exists within contractual and operational arrangements designed for commercial purposes, not security ones. That access is persistent, legitimised, and largely ungoverned by any Pakistani security framework specifically designed to monitor or constrain it. In a future scenario where bilateral interests diverge, a scenario no long-range strategic assessment can rule out, that structural access constitutes a pre-positioned capability.

This is the most politically sensitive claim in this paper. It is made not to impute hostile intent to a current partner, but because any honest threat assessment must account for structural vulnerabilities regardless of present-day relationships.

The Non-State Dimension

Non-state actors generally lack the ICS-specific expertise required to conduct the kind of sophisticated grid attack described in Section 1. Developing Industroyer-class malware requires deep knowledge of industrial protocols and grid operations that is not widely distributed. Criminal ransomware operators, while increasingly bold, typically seek financial return, and Pakistan's energy utilities are not attractive ransomware targets given their financial constraints.

The more credible non-state scenario involves state facilitation. A state actor seeking plausible deniability might provide technical capability, target intelligence, or operational support to a non-state proxy. Pakistan has direct experience of this model in the kinetic domain. The same logic applies in cyber.

The PakSat incident itself may fall into the hacktivist category, anti-state messaging, no claim of responsibility, ambiguous sophistication level. That ambiguity is itself strategically useful to whoever conducted it.

The Strategic Logic of Infrastructure Targeting

Across all these threat actors, the strategic logic of targeting Pakistan's power grid is consistent. Energy infrastructure sits at the intersection of economic activity, governance legitimacy, and civilian welfare. Disrupting it imposes costs across all three simultaneously. A significant grid disruption, measured in days rather than hours, would halt industrial production, freeze financial transactions, disrupt water supply, degrade telecommunications, and generate immediate public pressure on the government. In Pakistan's political environment, where governance legitimacy is already contested and public tolerance for infrastructure failure is low after years of load shedding, a cyber-induced blackout would carry political consequences disproportionate to its technical duration.

From an adversary's perspective, this leverage is available at a fraction of the cost and risk of conventional military operations. There are no soldiers to lose, no aircraft to shoot down, no international legal threshold that is unambiguously crossed. Attribution takes time and may never be conclusive.

A Note on Escalation

One dimension of this threat that Pakistani strategic planners must internalise is the escalation risk running in both directions.

A major cyber attack on Pakistan's grid, particularly during a period of heightened bilateral tension with India, would create immediate pressure for a response. The ambiguity of attribution would complicate that calculus, but public and political pressure would not wait for forensic certainty. Pakistan's nuclear doctrine, premised on full-spectrum deterrence including against sub-conventional threats, creates a theoretical pathway from infrastructure disruption to

nuclear signalling that no responsible analyst should dismiss as remote.

The absence of agreed red lines, hotlines specifically configured for cyber incident communication, or bilateral confidence-building measures in the cyber domain means that both sides are navigating this space without the crisis management architecture that exists, however imperfectly, for the conventional and nuclear domains. Capability development in cyber must be accompanied by strategic doctrine and crisis management architecture, otherwise capability alone increases instability rather than reducing it.

4. The Preparedness Gap

The preceding sections establish that Pakistan's grid presents a compounded attack surface and that credible threat actors exist with both the capability and strategic motivation to exploit it. This section addresses whether Pakistan's institutional and policy response is commensurate with that threat. It is not.

Policy: Articulation Without Implementation

Pakistan's National Cybersecurity Policy 2021 is the primary government document addressing cyber threats. As a statement of intent, it is not inadequate. As an operational framework for protecting critical infrastructure from state-sponsored APTs, it falls significantly short.

The policy's treatment of critical infrastructure is general where it needs to be specific. It does not establish sector-specific security frameworks. It does not address the distinct requirements of operational technology environments as opposed to enterprise IT. It does not set mandatory security baselines for infrastructure operators. It does not create accountability mechanisms for entities that fail to meet security requirements. It articulates that critical infrastructure should be protected without creating the instruments through which that protection is actually enforced.

The legal framework presents similar limitations. The Prevention of Electronic Crimes Act 2016 was designed for the cybercrime context, individual and corporate malfeasance, not for state-sponsored attacks on national infrastructure. PECA provides no meaningful framework for responding to an APT campaign against NTDC's SCADA environment. It is a law enforcement instrument being asked to carry a national security burden it was never designed for.

Regulation: The NEPRA Gap

The National Electric Power Regulatory Authority regulates Pakistan's power sector on safety, tariff, and service quality grounds. It does not regulate cybersecurity. There are no NEPRA-mandated security standards for SCADA and ICS systems operated by NTDC or the DISCOs. There are no requirements for regular security audits of operational technology environments. There are no incident reporting obligations. There are no compliance enforcement mechanisms.

Regulatory mandates are the primary mechanism through which governments establish security baselines across diverse, decentralised infrastructure ecosystems. The United States NERC CIP standards establish mandatory, audited security requirements for bulk power system operators. The EU's NIS Directive mandates security obligations for operators of essential services. Both are imperfect. Both are nonetheless categorically more effective than the voluntary, unmonitored approach that currently governs Pakistan's energy sector cybersecurity.

Without a regulatory mandate, security investment competes with every other operational priority in resource-constrained environments. In Pakistan's energy sector, where circular debt, capacity expansion, and basic operational maintenance already consume available resources, cybersecurity investment without a regulatory requirement to make it will consistently lose that competition.

Institutional Capacity: Fragmented and Under-Resourced

The National Centre for Cyber Security, operating under PTA, serves as Pakistan's primary civilian cybersecurity organisation. Its capacity to address sophisticated OT-specific threats to energy infrastructure is limited by three factors. First, its technical focus has historically been on IT rather than

operational technology. Second, its positioning within PTA's regulatory structure gives it limited authority over entities outside the telecommunications sector, NTDC, NEPRA, and the DISCOs do not fall under PTA's jurisdiction. Third, there is no evidence of a dedicated OT security capability within the organisation at scale.

Within the energy sector itself, institutional responsibility for cybersecurity is fragmented across NTDC, ten DISCOs, WAPDA, and numerous IPPs, each managing their own OT environments with no common security standard, no shared threat intelligence, no coordinated incident response capability, and no cross-entity visibility into the threat landscape. A compromise of FESCO's SCADA environment would not automatically be known to NTDC or LESCO. There is no energy sector equivalent of an Information Sharing and Analysis Centre.

The human capital dimension compounds these weaknesses. ICS security sits at the intersection of engineering, computer science, and industrial process knowledge. No Pakistani educational institution offers a dedicated ICS security curriculum. The professionals with relevant expertise are concentrated in a small number of individuals, primarily within vendor organisations rather than government or infrastructure operators.

The OT Security Governance Vacuum

Underlying all of the above is a more fundamental problem: Pakistan has no governance framework specifically designed for operational technology security in critical infrastructure. The policies that exist were written for IT environments. The regulator with jurisdiction over energy infrastructure has no cybersecurity mandate. The cybersecurity agency with a national remit has limited authority over the energy sector. The military cyber capabilities that could theoretically contribute to infrastructure defence have no publicly defined role in doing so.

The PakSat incident makes this vacuum concrete. Weeks after a demonstrated compromise of sovereign communications infrastructure, there is no publicly visible policy response that addresses the systemic implications, no announced security review of other critical infrastructure, no emergency regulatory action. The incident is being treated as an isolated event to be technically remediated rather than as a signal about a systemic vulnerability requiring a systemic response.

Benchmarking: Where Pakistan Stands

India established the National Critical Information Infrastructure Protection Centre in 2014 with a specific mandate for protecting critical infrastructure from cyber threats. The Defence Cyber Agency, established in 2019, provides military cyber capability with defined roles in national infrastructure defence. India's power sector regulator has initiated sector-specific cybersecurity frameworks following the 2021 Mumbai incident. India's posture is imperfect, but it has the institutional architecture that Pakistan lacks, and it is actively investing in closing its own gaps.

Israel operating in a comparably high-threat environment, provides the more instructive model. The Israel National Cyber Directorate operates dedicated security operations centres serving critical infrastructure sectors. Security standards for infrastructure operators are mandatory and audited. Civilian and military cyber capabilities are coordinated through defined protocols. Israel demonstrates that a resource-constrained nation in a high-threat environment can achieve a high level of infrastructure protection, but only by treating it as a genuine national security priority.

Pakistan's current posture sits well below both reference points on every dimension: policy specificity, regulatory mandate, institutional capacity, OT security expertise, and civil-military coordination. This is not a minor lag. It is a structural deficit.

5. What Needs to Happen

The findings of this paper point to a deficit that is structural, not incidental. Closing it requires action across three time horizons. These recommendations are directed at three audiences simultaneously: policymakers with the authority to mandate action, regulators with the power to enforce it, and infrastructure operators who will ultimately have to implement it. No single actor can close this gap alone.

Horizon 1: Immediate (0 to 6 Months)

Recognise Critical Infrastructure Cybersecurity as a National Security Issue

This is the prerequisite for everything else. The National Security Committee should formally table critical infrastructure cyber threats as a standing agenda item. The National Security Policy should be updated to explicitly name cyber-attacks on energy infrastructure as a Tier-1 threat. This costs nothing and unlocks everything: resource allocation decisions, institutional mandates, and inter-agency coordination all follow from formal threat recognition at the highest level.

Conduct an Emergency Security Audit of NPCC

NPCC is the single highest-consequence target in Pakistan's electricity infrastructure. An emergency security audit of NPCC's EMS and SCADA environment, conducted by technically qualified personnel with OT security expertise, sourced internationally if necessary, should be treated as an immediate priority. The audit should assess network segmentation, access controls, monitoring capability, authentication mechanisms, and vendor access arrangements. Findings should be classified but acted upon within a defined remediation timeline.

Establish a Cross-Agency Critical Infrastructure Cyber Coordination Cell

Pakistan currently has no mechanism for real-time coordination between NCCS, military cyber capabilities, NTDC, and relevant intelligence agencies during a critical infrastructure cyber incident. A dedicated coordination cell should be established with defined membership, authority, communication protocols, and decision-making procedures. It should conduct a tabletop exercise simulating a grid cyber incident within its first ninety days of operation.

Issue a Formal Policy Response to the PakSat Incident

A public statement from the Ministry of IT or the NSC acknowledging that the incident has prompted a review of critical infrastructure security posture across sectors would cost nothing and signal institutional seriousness to both domestic audiences and potential adversaries. The incident should be treated as a systemic indicator, not an isolated technical event.

Horizon 2: Structural (6 to 18 Months)

Mandate NEPRA to Develop and Enforce ICS Cybersecurity Regulations

NEPRA must be given an explicit cybersecurity mandate covering operational technology environments. The resulting framework should establish mandatory security baselines for SCADA and ICS systems operated by NTDC and all DISCOs, require regular third-party security audits, create incident reporting obligations, and establish enforcement mechanisms including financial penalties for non-compliance. The framework should be benchmarked against IEC 62443 and NERC CIP, adapted to Pakistan's operational context.

Establish a Dedicated OT Security Operations Centre for the Energy Sector

Pakistan needs a Security Operations Centre specifically configured for operational technology environments, capable of monitoring industrial protocols, detecting anomalous control system behaviour, and providing real-time situational awareness across the grid. It could be structured as a government-operated facility within an expanded NCCS mandate, as a public-private partnership, or as a joint capability hosted within NTDC. Without this capability, Pakistan will continue to be unable to detect APT activity in its grid until after disruption has occurred.

Develop a Security Governance Framework for CPEC Energy Assets

The structural access that Chinese operators and contractors have to CPEC generation assets requires a dedicated governance framework. This should define what remote access is permissible, under what conditions, with what monitoring and logging requirements. It should require Pakistani technical personnel as mandatory co-participants in any maintenance activity affecting ICS environments. Software updates and firmware changes to control systems at CPEC facilities should be reviewed and approved by Pakistani technical authorities before deployment. These requirements should be pursued through appropriate bilateral channels, framed as a mutual interest in infrastructure security.

Create a National ICS Security Training Pipeline

Pakistan needs a domestic pipeline of professionals with OT security skills. This requires curriculum development at NUST, UET, and GIKI integrating ICS security into engineering programs, a professional certification pathway adapted from international frameworks like GICSP, and structured secondment programs placing trained personnel within NTDC, DISCOs, and major generation facilities. Retention is as important as training, public sector compensation structures for cybersecurity specialists must be reviewed against market rates.

Establish an Energy Sector Information Sharing and Analysis Centre

Energy infrastructure operators in Pakistan currently have no formal mechanism for sharing threat intelligence or incident information with each other. An ES-ISAC, modelled on the E-ISAC serving the North American power sector, would enable collective defence across a fragmented operator landscape. When one DISCO detects a novel phishing campaign, every other DISCO and NTDC should know within hours. This kind of collective intelligence is cheap relative to its security value.

Horizon 3: Strategic (18 to 36 Months)

Develop a National Cyber Deterrence Doctrine

Pakistan needs to articulate, at least in general terms, what constitutes an unacceptable cyber attack on critical infrastructure and what responses it reserves the right to employ. An adversary that believes Pakistan cannot attribute attacks, cannot respond proportionally, and has no doctrine governing cyber operations faces no meaningful deterrence. Deterrence in the cyber domain is imperfect, but the complete absence of any articulated doctrine leaves Pakistan strategically passive in a domain where it faces active threats.

Integrate Cyber Scenarios into National Security Planning

Pakistan's strategic planning and military exercise cycles should systematically incorporate scenarios involving major infrastructure cyber-attacks, including scenarios where attacks occur during periods of elevated bilateral tension. These exercises should stress-test command decision-making under ambiguous attribution, test civil-military coordination mechanisms, and validate the crisis management architecture being built in Horizons 1 and 2.

Phase Out Critical Legacy Systems Through a Funded Modernisation Programme

The long-term solution to legacy system vulnerability is replacement. This requires a nationally funded programme, potentially incorporating international development financing, to systematically upgrade SCADA and ICS infrastructure across the transmission system and major generation assets. New systems should be procured against security specifications that include IEC 62443 compliance, multi-factor authentication, encrypted communications, and vendor security support commitments extending the operational lifetime of the equipment.

A Note on Sequencing and Resources

These recommendations are not a wishlist. They are a prioritised roadmap. Horizons 1 and 2 contain actions achievable within existing or modestly expanded institutional frameworks. Horizon 3 requires sustained

political commitment and significant resource allocation over multiple years.

The objection that Pakistan cannot afford this programme is understandable but ultimately inverts the cost calculation. The economic cost of a major cyber-induced grid disruption, measured in industrial output lost, financial system disruption, emergency response expenditure, and long-term investor confidence damage, would dwarf the cost of the prevention programme described here.

The question is not whether Pakistan can afford to close this gap. It is whether Pakistan can afford not to.

Author's Note

This paper was written by a final-year Strategic Studies student. It was not commissioned. The author has no privileged access to the systems assessed herein, no institutional affiliation with any government agency, and no classified sources. Every claim made in this paper rests on open-source material, academic literature, publicly available technical documentation, threat intelligence reports, and policy documents. Where the analysis reaches beyond what open-source evidence strictly supports, that is a matter of analytical judgement, and the author welcomes challenge on those points specifically.

The paper is published under the banner of SSS, a platform the author is building for rigorous, independent strategic analysis on security, technology, and policy questions. SSS is in its earliest stage. This is its first published output.

The PakSat incident prompted this paper. Not because satellite security and grid security are the same problem, they are not, but because it made visible something that open-source analysis had already established: Pakistan's critical infrastructure has a security posture that does not match its threat environment. That gap deserves serious analytical attention. This paper is an attempt to provide some. It is explicitly a first word, not a last one.

The author is actively seeking expert engagement. If you work in energy sector operations, operational technology security, national cybersecurity policy, or South Asian strategic affairs, and you think something in this paper is wrong, incomplete, or requires sharper treatment feel free to reach out.

Responses, critiques, and offers of collaboration can be directed to: murtazaasim@outlook.com

References and Further Reading

Policy and Regulatory Documents

Government of Pakistan. National Cybersecurity Policy 2021. Ministry of Information Technology and Telecommunication.

Government of Pakistan. Prevention of Electronic Crimes Act 2016. National Assembly of Pakistan.

NEPRA. State of Industry Report 2023. National Electric Power Regulatory Authority.

North American Electric Reliability Corporation. NERC CIP Standards: Critical Infrastructure Protection. Current version.

European Union. Directive on Security of Network and Information Systems (NIS Directive). European Parliament, 2016.

International Electrotechnical Commission. IEC 62443: Industrial Automation and Control Systems Security. Current version.

Technical and Threat Intelligence

Cherepanov, A. WIN32/Industroyer: A New Threat for Industrial Control Systems. ESET Research, 2017.

Dragos Inc. CRASHOVERRIDE: Analysis of the Threat to Electric Grid Operations. Dragos, 2017.

Johnson, B. et al. Attackers Deploy New ICS Attack Framework "TRITON" and Cause Operational Disruption to Critical Infrastructure. FireEye, 2017.

Lee, R.M., Assante, M.J., and Conway, T. Analysis of the Cyber Attack on the Ukrainian Power Grid. E-ISAC, 2016.

Recorded Future. RedEcho: Chinese State-Sponsored Actors Target Indian Power Sector. Insikt Group, 2021.

Symantec Security Response. Dragonfly: Western Energy Sector Targeted by Sophisticated Attack Group. Symantec, 2018.

Stouffer, K., Falco, J., and Scarfone, K. Guide to Industrial Control Systems Security. NIST Special Publication 800-82, current revision.

Academic and Strategic Literature

Arquilla, J. and Ronfeldt, D. "Cyberwar is Coming." Comparative Strategy, 1993.

Clarke, R. and Knake, R. Cyber War: The Next Threat to National Security and What to Do About It. HarperCollins, 2010.

Libicki, M. Cyberdeterrence and Cyberwar. RAND Corporation, 2009.

Lindsay, J.R. "Stuxnet and the Limits of Cyber Warfare." Security Studies, 2013.

Rid, T. Cyber War Will Not Take Place. Oxford University Press, 2013.

Valeriano, B. and Maness, R. Cyber War Versus Cyber Realities. Oxford University Press, 2015.

Zetter, K. Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon. Crown Publishers, 2014.

On Pakistan's Security Context

Fair, C.C. Fighting to the End: The Pakistan Army's Way of War. Oxford University Press, 2014.

Hoyt, T. "Pakistani Nuclear Doctrine and the Dangers of Strategic Myopia." Asian Security, 2009.

Siddiqa, A. Military Inc.: Inside Pakistan's Military Economy. Pluto Press, 2007.

Rizvi, H.A. The Military and Politics in Pakistan. Progressive Publishers, 1986.