Cybercriminality in the Asia-Pacific: Trends, State Responses, and Pakistan's Role

Waleed Ahmad

Executive Summary

- The Asia-Pacific region is witnessing a surge in cybercrime and cyber-enabled attacks, ranging from massive ransomware campaigns to state-linked espionage and organized fraud. In 2024 alone, APAC saw 57,000 ransomware incidents notably in Indonesia, Philippines, Thailand. High-profile breaches (e.g. Indonesia's national data center, Malaysian public transit, Philippine health insurer) underscore critical vulnerabilities.[1] In 2025-2026, APAC has emerged as a key hotspot for state-linked cyber operations, with more than a quarter of global cyber espionage campaigns now targeting or originating from the region. Criminal syndicates in Southeast Asia operate billion-dollar scam centers, and advanced persistent threat (APT) groups (Chinese, North Korean, etc.) now routinely target tech, energy and defense sectors across the region.
- Governments are responding with new laws, agencies and cooperation frameworks. Many APAC countries have upgraded cybersecurity laws and regulations, established national cyber agencies/CERTs, and joined international initiatives. For example, Japan enacted an Active Cyber Defence Law (2025) enabling pre-emptive countermeasures[2], Singapore mandates breach reporting under its Cybersecurity Act[3], and India has reorganized its cybercrime coordination via I4C and a CERT Council.[4] At the regional level, ASEAN ministers endorsed a 10-year Action Plan (2026-2035) on transnational crime that includes cybercrime and online fraud.[5]
- Key challenges persist attribution dilemmas (attacks routed across borders) hamper law enforcement, while human factors (large workforces, insider risk) amplify exposure. APAC firms suffer 8 insider-driven data incidents per month on average, higher than in the West[6],

---

1 PhilHealth hack potentially exposes 42 million people | Insurance Business, https://www.insurancebusinessmag.com/asia/news/cyber/philhealth-hack-potentially-exposes-42-million-people-496453.aspx

2 Cyber Espionage and Ransomware: East Asia's 2025 State-backed Attacks – CyberProof, https://www.cyberproof.com/blog/cyber-espionage-and-ransomware-east-asias-2025-state-backed-attacks/

3 The Top Four Cybersecurity Fronts Shaping Asia Pacific in 2025 - Access Partnership, https://accesspartnership.com/opinion/the-top-four-cybersecurity-fronts-shaping-asia-pacific-in-2025/

4 Pakistan moves to establish first National Cybersecurity Authority to strengthen digital defense - SAMENA Daily News, https://www.samenacouncil.org/samena_daily_news?news=108446

5 ASEAN adopts 10-year action plan to combat transnational crime | Vietnam+ (VietnamPlus), https://en.vietnamplus.vn/asean-adopts-10-year-action-plan-to-combat-transnational-crime-post326324.vnp

6 Mimecast study: APAC reports higher frequency of insider-driven cyber incidents than US and Europe - Asia Pacific Security Magazine, https://www.asiapacificsecuritymagazine.com/mimecast-study-apac-reports-higher-frequency-of-insider-driven-cyber-incidents-than-us-and-europe/

meaning social engineering and negligent behavior are major entry points. Fragmented policies and capacity gaps including talent shortage, legacy infrastructure, digital divide also constrain response.

- Pakistan's role is becoming more prominent. Islamabad faces similar threats: an estimated 40 million cyber incidents in 2024, including a mid-2025 ransomware attack on a major gas company, Blue Locker.[7] Hacktivist groups targeted Pakistani government domains (e.g. false claims of gov.pk "digital blackout").[8] The government has moved to strengthen defenses: a proposed draft Cybersecurity Act (2025) will create a national Cybersecurity Authority, a 14-member CERT Council is coordinating incident response, and the telecom regulator issued a 2023-2028 cybersecurity strategy covering law, resilience, monitoring, capacity and public awareness.[9]
- This op-ed examines these trends and countermeasures, and provides **policy recommendations for Pakistan**, including finalizing legal frameworks, enhancing public-private partnerships, and investing in human-centric security. Addressing cybercriminality in Asia-Pacific thus requires not only technical tools but also regional cooperation and a focus on the human and transnational dimensions of cyber conflict.

Asia-Pacific Threat Landscape

Asia-Pacific now sees some of the world's most frequent and sophisticated cyber-attacks. Major trends include:

1. **Ransomware and Malware:**

APAC faces an unprecedented ransomware surge. In H1 2024, there were over *57,000* ransomware attacks regionally[10]. Threat actors now use **double/triple extortion** (data leaks or service disruption) beyond mere encryption. For example, a LockBit 3.0 attack in mid-2024 crippled fuel distribution in Indonesia's Java region.[11] Similar breaches hit critical services including Indonesia's National Data Centre, Malaysia's metro transit systems, and the Philippines' PhilHealth insurer exposing 42 million records in Sept 2023.[12]

2. **State-sponsored Cyber Espionage:**

---

7 MENA > The New Reality of Cyber - Physical Risks in Pakistan | Lockton, https://global.lockton.com/mena/en/news-insights/the-new-reality-of-cyber-physical-risks-in-pakistan

8 cabinet.gov.pk, https://cabinet.gov.pk/SiteImage/Misc/files/NTISB%20Advisories/2024/3.pdf

9 PTA Issues Cyber Security Strategy 2023-2028 for Pakistan's Telecom Sector: A Five Year Plan Towards Digital Resilience, https://www.pta.gov.pk/category/pta-issues-cyber-security-strategy-2023-2028-for-pakistans-telecom-sector-a-five-year-plan-towards-digital-resilience-980103515-2024-07-04

10 The Top Four Cybersecurity Fronts Shaping Asia Pacific in 2025 - Access Partnership, https://accesspartnership.com/opinion/the-top-four-cybersecurity-fronts-shaping-asia-pacific-in-2025/

11 PhilHealth hack potentially exposes 42 million people | Insurance Business, https://www.insurancebusinessmag.com/asia/news/cyber/philhealth-hack-potentially-exposes-42-million-people-496453.aspx

Chinese, North Korean, Iranian and other APT groups are active. These teams target tech R&D, energy and defense networks. Notably, Chinese hackers (e.g. “MirrorFace”) seek semiconductor and telecom secrets, while North Korea’s Lazarus and allied groups have stolen cryptocurrency and carried out phishing campaigns in the region.[13] Taiwan and Japan report daily intrusion attempts, and South Korea suffers frequent attacks often traced to DPRK, aimed at government, military and finance sectors. Such campaigns blend intelligence gathering with criminal profit.

3. **Transnational Organized Crime and Scams:**

Southeast Asia hosts large criminal fraud hubs. Syndicates in Cambodia, Lao PDR, Myanmar and the Philippines run elaborate “scam centers” that exploit global victims through romance scams, bogus investments and fake lotteries. These operations employ forced labor and even trafficked workers, generating US$40 billion annually.[14] The use of social media and now deepfake/AI tools is exploding deepfake-based schemes grew 600% by late 2024. Meanwhile, traditional phishing and fraud continue: APAC populations experience higher rates of data exposure from compromised credentials, partly due to large unregulated messaging platforms in Southeast Asia.

4. **Insider & Human Risk:**

Human factors are key vulnerabilities. Studies show APAC organizations average eight insider-caused data breaches per month, more than in Europe (6) or North America (5). Common culprits include compromised credentials, negligent staff or malicious insiders. In practice, attackers exploit routine behaviors for example “check this urgent invoice!” to bypass technical defenses. High-turnover workforces and rapid digital adoption mean even well-funded organizations struggle with awareness. This “human attack surface” is now recognized as critical. Attackers often penetrate networks not by hacking firewalls, but by hacking trust and curiosity.

State Responses and Regional Cooperation

Governments across Asia-Pacific are elevating cybersecurity as a strategic priority:

- **New Laws and Standards:**

Countries are updating legal frameworks. Singapore’s Cybersecurity Act (2018) now requires critical infrastructure operators to report breaches, and regulates SOCs, data centers and

---

12 PhilHealth hack potentially exposes 42 million people | Insurance Business, https://www.insurancebusinessmag.com/asia/news/cyber/philhealth-hack-potentially-exposes-42-million-people-496453.aspx

13 Cyber Espionage and Ransomware: East Asia's 2025 State-backed Attacks – CyberProof, https://www.cyberproof.com/blog/cyber-espionage-and-ransomware-east-asias-2025-state-backed-attacks/

14 INTERPOL. Cyber Threat Assessment Report 2025-2026_. 2025.
https://www.interpol.int/content/download/24327/file/CYBER_ASP%20Cyber%20Threat%20Assessment%20Report_2025_2026_v4.pdf

telecoms. Japan introduced the Active Cyber Defence Law (2025), legally allowing government entities to preemptively sinkhole or counterattack on imminent threats. South Korea strengthened its Cyber Security Act, mandating multi-factor authentication for financial transactions. India has drafted amendments to its IT Act and PECA to cover new offenses like identity theft and is implementing the Cybersecurity Framework (2023). China continues to tighten its Cybersecurity Law and Data Security Law (latest amendments in 2025) to enforce data localization and heavy penalties for noncompliance.[15]

- **National Cyber Agencies and CERTs:**

Many states now host centralized cyber agencies. Pakistan is creating a new Cybersecurity Authority (2025) under its National Cyber Security Policy. An interim 14-member CERT Council (per the 2023 CERT Rules) coordinates incident response across ministries, ISPs and banks.[16] Australia has the Cyber and Infrastructure Security Centre (ACSC), India has CERT-In and the National Cybercrime Threat Analytics Unit which is the part of I4C.[17] ASEAN has an ASEAN-Japan CERT center for capacity building. These agencies facilitate national risk assessments, threat intel sharing, and law enforcement coordination.

- **National Strategies and Capacity-Building:**

Many states published multi-year cyber strategies. For example, Pakistan's telecom regulator (PTA) released a Cybersecurity Strategy 2023-28 with six pillars: legal framework, resilience, monitoring, capacity, cooperation and awareness. It mandates a multi-stakeholder approach including public-private, academia, civil society. Similarly, the Philippines and Thailand have their National Cybersecurity Strategies. Training programs are being scaled: Singapore's CSA program, Japan's JPCERT trainings, and India's cybersecurity skill initiatives (vulnerability labs, forensics courses).

- **Public-Private Partnerships:**

Public-private cooperation is growing. Industry consortia like the Asia-Pacific CCAPAC (AWS, Cisco, KnowBe4, etc.) promote best practices and joint capacity projects. Tech companies invest regionally. For example, AWS's $5b Thailand cloud build, Cisco's 50,000 cybersecurity talent goal. Governments encourage shared exercises like cyber drills with banks and utilities and encourage reporting by offering legal safe-harbors or "bug bounties" (Malaysian Cyber Security Exchange, India's Bug Bounty for critical infra).[18]

---

15 The PRC's Evolving Cyber Laws and Implications for Southeast Asia's Digital Economy and Integration | New Perspectives on Asia | CSIS

https://www.csis.org/blogs/new-perspectives-asia/prcs-evolving-cyber-laws-and-implications-southeast-asias-digital

16 Pakistan moves to establish first National Cybersecurity Authority to strengthen digital defense - SAMENA Daily News, https://www.samenacouncil.org/samena_daily_news?news=108446

17 India: enhancing Cybercrime Response, Digital Resilience - OpenGov Asia, https://opengovasia.com/india-enhancing-cybercrime-response-digital-resilience/

18 The Top Four Cybersecurity Fronts Shaping Asia Pacific in 2025 - Access Partnership, https://accesspartnership.com/opinion/the-top-four-cybersecurity-fronts-shaping-asia-pacific-in-2025/

Challenges and Policy Gaps

Despite progress, significant gaps remain:

a) **Attribution and Jurisdiction:**

Cyberattacks often cross borders. Uncertainty over an attacker's origin complicates response. APAC states struggle to pursue offenders legally when trials lead offshore. For instance, Pakistan's PECA (2016) lacks extraterritorial reach, so attacks from abroad often go immune. Analysts note that joining the Budapest Convention would facilitate international evidence-sharing and legal assistance, but Pakistan has not yet ratified it due to concerns over data privacy and sovereignty.[19] The Ministry of Foreign Affairs has stated that the convention is "highly intrusive" and would compromise Pakistan's data. Intelligence agencies have also raised reservations, citing Israel's participation in the convention, which Pakistan doesn't recognize as a state.[20]

Some analysts argue that joining the convention would facilitate international cooperation and help combat cybercrime, but Pakistan is cautious about potential risks. The country has enacted its own laws, like the Prevention of Electronic Crimes Act (PECA) 2016, but joining the convention would require harmonizing national laws with global standards. The lack of such treaties means many transnational criminals evade accountability.

b) **Fragmented Policies:**

Regional responses are uneven. While Singapore and Japan lead with mature frameworks, others lag. Some ASEAN states only have draft cyber laws or limited enforcement capability. Divergent national priorities like Vietnam's focus on data localization vs. Indonesia's openness to foreign investment in ICT hinder a cohesive ASEAN approach. The digital divide is stark and nearly one-third of APAC's population is offline, limiting workforce development and creating "blind spots" where unmonitored networks may be exploited.[21]

c) **Human and Infrastructure Gaps:**

Talent shortages plague many governments and businesses. Surveys find more than 80% of APAC firms cite lack of certified security professionals. Critical infrastructure is still migrating from legacy IT/OT systems to smart networks and during this transition, outdated protocols remain vulnerable. Many organizations still treat cybersecurity as an IT issue rather than an

---

19 Should Pakistan sign the Budapest Convention?, https://tribune.com.pk/story/2387309/should-pakistan-sign-the-budapest-convention

20 Budapest Convention: Risk and Benefit Analysis for Pakistan, https://issra.pk/pub/insight/2024/Budapest-Convention-Risk-and-Benefit-Analysis-for-Pakistan/Budapest-Convention-Risk-and-Benefit-Analysis-for-Pakistan.html

21 The Top Four Cybersecurity Fronts Shaping Asia Pacific in 2025 - Access Partnership, https://accesspartnership.com/opinion/the-top-four-cybersecurity-fronts-shaping-asia-pacific-in-2025/

enterprise risk and the Lockton report warns of "false sense of security" in Pakistan's utilities.[22] As the Lockton analysis notes, Pakistan's energy and resources sectors, power plants, pipelines, upcoming mines are **prime targets** due to the potentially massive economic impact.[23]

Key Asia-Pacific Countermeasures (2023-2026)

Country/Region	Major Laws/Policies	CERT/Agency	Notable Initiatives
Japan	Active Cyber Defence Law (2025); Revised Cybersecurity Strategy	JPCERT/CC and NISC	AI-driven defenses, joint drills with US/Japan
China	Cybersecurity Law (2016, amendments 2025); Data Security Law	CAC, China Electronic Info. & Tech. Acad.	Data localization rules and Belt & Road cyber standards
India	NCSP-2021; IT Act & PECA amendments; Digital India policy	CERT-In and NCIIPC	I4C cybercrime center and national forensics labs
Singapore	Cybersecurity Act (2018, updated) and Personal Data Protection Act	SingCERT and CSA	ASEAN Cyber Drill Leader and 5G/Open RAN research
Malaysia	Cybersecurity Act (2020) and Digital Economy Blueprints	MyCERT and NCSC	ASEANAPOL cybercrime ops and national certification programs
ASEAN (regional)	ASEAN Cybersecurity Cooperation Strategy (2021-2025) and ASEAN CERT-to-CERT WG	ASEANAPOL and ASEAN CERTs	ASEAN-Japan CERT capacity building and transnational crime plan (2026-2035)
Pakistan	PECA 2016 and Draft Cybersecurity Act (2025)	NCERT Council and NTISB (Govt)	PTA Cybersecurity Strategy 2023-28 and CERT Council
Australia	Cybersecurity Strategy 2023 and Security Legislation	ACSC (govt CERT)	ANZCERT drills and cyber exercises with allies

Table: Examples of recent cyber policy measures and organizations in Asia-Pacific states. This is illustrative, not exhaustive.

Pakistan's Cybersecurity Landscape (2023-2026)

Pakistan has begun responding to these challenges, though gaps remain:

---

22 The Top Four Cybersecurity Fronts Shaping Asia Pacific in 2025 - Access Partnership, https://accesspartnership.com/opinion/the-top-four-cybersecurity-fronts-shaping-asia-pacific-in-2025/

23 MENA > The New Reality of Cyber - Physical Risks in Pakistan | Lockton, https://global.lockton.com/mena/en/news-insights/the-new-reality-of-cyber-physical-risks-in-pakistan

- **Recent Incidents:** Pakistan saw *millions* of cyberattack attempts. A subsidiary of the Power Ministry reported 40 million attacks in 2024.[24] In August 2025, the National Cyber Emergency Response Team (NCERT) warned of an active *Blue Locker* ransomware campaign that hit one of Pakistan's largest gas producers supplying 20% of national gas. Energy, mining and telecom companies are explicitly cited as attractive targets due to their economic impact. Meanwhile, hacktivist groups claimed high-visibility outages in Dec 2023 an Indian-affiliated group "Vanguard" purported to take down the gov.pk domain, and in Jan 2024 "**UCC Error 404 Team**" claimed defacements of government, defense and banking websites.[25] These were framed as propaganda but did highlight genuine security lapses and the potency of misinformation.
- **Government Responses:** Building on its 2021 Cybersecurity Policy, Pakistan is strengthening its institutional framework. In late 2025 Parliament completed a draft National Cybersecurity Act to create the country's first dedicated Cybersecurity Authority. This Authority will oversee standards, incident response and risk mitigation across all Critical Information Infrastructures (CII). Even before its enactment, an interim CERT Council, 14 members from IT, Defense, Interior, Foreign Affairs, academia and telecoms has been established under the 2023 CERT Rules to coordinate cyber incident response. Several key systems including NADRA, tax, telecom are already designated as CII under PECA-2016.[26]
- **Strategic Policy:** The Pakistan Telecommunication Authority (PTA) in Dec 2023 issued a Cybersecurity Strategy 2023-28 for the telecom sector. It outlines six pillars: legal frameworks, resilience, monitoring/incident response, capacity building, cooperation, and awareness. Emphasis is on a multi-stakeholder approach involving regulators, carriers, security firms and academia. This reflects a shift towards proactive resilience. Meanwhile, Federal agencies have begun pushing digital literacy campaigns and publishing threat advisories like financial scam warnings in 2023. Law enforcement agency FIA's Cyber Crime Wing also tracks cyberfraud. However, Pakistan has yet to fully ratify international frameworks like the Budapest Convention, limiting cross-border evidence gathering.[27]
- **Capacity Building:** Pakistan is increasing investment in cyber skills. The National University of Science and Technology (NUST) and NIPA Peshawar have launched cybersecurity degree programs with research centers. The defense forces are reportedly expanding their Cyber Command units, though details are classified. Private sector initiatives include a national hackathon for critical infrastructure (2024) and industry-led training in

---

24 MENA > The New Reality of Cyber - Physical Risks in Pakistan | Lockton, https://global.lockton.com/mena/en/news-insights/the-new-reality-of-cyber-physical-risks-in-pakistan

25 cabinet.gov.pk, https://cabinet.gov.pk/SiteImage/Misc/files/NTISB%20Advisories/2024/3.pdf

26 Pakistan moves to establish first National Cybersecurity Authority to strengthen digital defense - SAMENA Daily News, https://www.samenacouncil.org/samena_daily_news?news=108446

27 Should Pakistan sign the Budapest Convention?, https://tribune.com.pk/story/2387309/should-pakistan-sign-the-budapest-convention

banking security. However, resource gaps persist, the ratio of skilled professionals to need remains low, and many public networks still use outdated protocols.

Pakistan's evolving cyber landscape reflects a mix of aspiration and risk. Like its neighbors, it must balance the need for strong cybersecurity measures with concerns over surveillance and governance. For example, civil society has questioned how new laws like the Budapest treaty might affect privacy. Achieving the right balance will be critical to both security and public trust.

Policy Recommendations for Pakistan

To strengthen Pakistan's cyber resilience, we recommend:

- **Enact and Empower the Cyber Authority (Legal/Policy):** Finalize the National Cyber Security Act (2026) swiftly and operationalize the Cybersecurity Authority with a clear mandate. Grant, it powers for breach reporting, critical infrastructure protection, and coordination with provinces. Update PECA or related laws to cover emerging crimes like SIM-swap fraud, AI-driven deepfakes. Ratify the Budapest Convention or UN cybercrime treaty to enable international evidence sharing.
- **Enhance Technical Defenses (Capacity & Coordination):** Invest in cybersecurity technology including SIEM platforms, endpoint protection, AI-driven detection. Accelerate modernization of SCADA/ICS in power and utilities. Strengthen the NCERT/CERT-IN infrastructure, ensure well-resourced Security Operations Centers (SOCs) for energy, banking and telecom. Institute mandatory incident reporting and drill exercises like cyber wargames across government and key industries. Encourage adoption of zero-trust and multi-factor authentication nationwide.
- **Build Workforce and Research:** Expand cybersecurity education and fund university programs) and vocational training. Offer scholarships for cyber degrees and incentivize private sector internships. Support research institutes to study social engineering and regional cybercrime patterns on human vulnerabilities and transnational networks. Create a national CERT-academia consortium to develop homegrown tools like malware analysis, threat intelligence suited to Pakistan's context.
- **Public-Private Partnerships (Governance):** Formalize cooperation between government, industry and academia. For example, expand the existing CERT Council to include banks and tech firms as members or observers. Launch a national bug bounty program for government websites. Encourage telecom operators to share threat data leveraging Pakistan's 1LINK and Telecom Infra Companies. Collaborate with energy and finance sectors on joint cyber drills. Leverage industry expertise to upskill civil servants like Singapore's SSA in Smart Nation.
- **Regional and Diplomatic Engagement:** Deepen collaboration with Asian partners. Join regional cyber exercises like those run by ASEAN, ASEAN+3. Seek bilateral MoUs with neighboring CERTs including China, Iran, Central Asia for real-time CSIRT-to-CSIRT

communication. Actively participate in forums like APCERT, Asia-Pacific CERT Council, and South Asian CERT Exchange. Contribute to international cyber norms dialogues, UN Ad Hoc Committee to both influence and learn from global standards.

- **Strengthen Public Awareness and Legal Enforcement:** Launch nationwide cyber hygiene campaigns like school curricula, media PSAs focusing on phishing and social engineering risks. Empower law enforcement with specialized cybercrime units and forensic labs expanding what FIA and NADRA already do. Develop clear SOPs for digital evidence collection in police forces. Engage civil society to audit new cyber laws to balance security and privacy. By raising general awareness, the human attack surface can be reduced, complementing technical defenses.

Conclusion

Asia-Pacific's evolving cyber threat environment underscores that cyber conflicts are as much human and geopolitical as they are technical. As highlighted throughout this analysis, attackers exploit routine behaviors, weak institutions and cross-border loopholes. Strengthening Pakistan's cybersecurity will therefore require integrating technical tools with an understanding of human vulnerabilities and transnational crime networks - themes central to my own research. By aligning national policies with Asia-Pacific best practices and focusing on people-centric resilience, Pakistan can better safeguard its digital future.

About Author:

Waleed Ahmad, an M.Phil. scholar in International Relations specializing in Emerging Technologies, AI, and Cyber Security. With a bachelor's degree in Peace and Conflict Studies, he delves into the intersection of Cyber security and its impact on reshaping the dimensions of Peace and Conflict. Waleed's passion for understanding the evolving landscape of global security is reflected in his research, which explores the intricate dynamics between technological advancements and international relations.