Cyber Law Reform for Human-Centred Governance in Sri Lanka

Niranjan W. Meegammana[1], N. S. Punchihewa[1], Harinda Fernando[2]
[1]University of Colombo, [2]Sri Lanka Institute of Information Technology, Sri Lanka[3]
niranjan.meegammana@gmail.com

Abstract
Cybercrime has become a major governance challenge, threatening public trust, human rights, and national security. Sri Lanka's Computer Crimes Act (2007) and related legislation have not kept pace with emerging risks such as ransomware, AI-driven fraud, and crypto-enabled offences. This study examines the adequacy of Sri Lanka's cybercrime framework in addressing contemporary threats and aligning with global rights-based standards. Using a hybrid qualitative methodology combining doctrinal legal analysis and expert interviews with judges, policymakers, and cybersecurity professionals, the research identifies three core deficiencies: outdated legal definitions, weak rights safeguards, and fragmented institutional coordination. Drawing on international benchmarks such as the Budapest Convention, GDPR, and NIS2 Directive, the paper proposes a four-layered reform framework founded on human rights, institutional capacity-building, international harmonisation, and adaptive governance. The proposed reforms aim to guide policymakers towards a modern, transparent, and citizen-centred cyber law regime that enhances digital resilience and democratic legitimacy in Sri Lanka and offers a transferable model for other developing jurisdictions.

Keywords: Cybercrime, Legal Reforms, Human Rights, Sri Lanka, Policy Innovation, Digital Justice, Governance

Introduction
Cybercrime represents one of the most pressing governance and human-rights challenges of the twenty-first century. As societies undergo digital transformation, states are compelled to adapt legal frameworks that safeguard both national security and individual liberties. The World Economic Forum identifies cyber threats as one of the five greatest global risks, comparable to climate change and geopolitical instability. For Sri Lanka, the challenge lies

not only in technological vulnerability but also in ensuring that its cyber laws reflect democratic values, due-process guarantees, and international cooperation. In the aftermath of the COVID-19 pandemic, rapid digitisation accelerated Sri Lanka's dependence on digital platforms for commerce, education, and governance. More than twelve million citizens now rely on online systems, yet the principal legal instrument the Computer Crimes Act (CCA) No. 24 of 2007 remains largely unchanged since its enactment nearly two decades ago. The Act was drafted before the emergence of artificial intelligence, ransomware-as-a-service, and decentralised blockchain ecosystems. Consequently, Sri Lanka's legal regime does not adequately address AI-driven fraud, data-poisoning attacks, or cross-border crypto-crimes that transcend territorial jurisdiction.

The conceptual foundation of cyber law reform rests on the social-contract principles articulated by John Locke (1689), who emphasised liberty, accountability, and the consent of the governed. Modern cybersecurity governance must therefore integrate technological safeguards with constitutional oversight and participatory decision-making. However, many developing democracies including Sri Lanka continue to adopt executive-driven legal reforms without sufficient stakeholder consultation. This has led to an imbalance between securitisation and civil liberties, undermining both legitimacy and public trust.

Recent comparative developments illustrate a widening policy gap. India's Digital Personal Data Protection Act (2023) introduces consent-based processing and breach-notification obligations; Singapore's Cybersecurity Act (2018) mandates critical-infrastructure audits and incident reporting; and the European Union's NIS2 Directive (2023) sets harmonised resilience standards across essential sectors. In contrast, Sri Lanka lacks integrated mechanisms for rights protection, institutional coordination, and international interoperability. The result is a fragmented system where agencies such as the CERT, ICTA, and law-enforcement divisions operate with overlapping mandates and limited accountability.

This study therefore examines how Sri Lanka's cybercrime framework can be modernised through a rights-based and policy-oriented approach. It aims to:

(1) identify doctrinal and institutional gaps in the existing legislation;

(2) analyse alignment with international legal instruments such as the Budapest Convention and GDPR; and

(3) propose a layered policy framework to strengthen governance, transparency, and digital trust. By framing cybercrime law reform as a governance and human-rights imperative, this paper positions Sri Lanka's experience within a broader discourse on inclusive and future-oriented digital policymaking.

Methodology

This study adopts a hybrid qualitative methodology that integrates doctrinal legal analysis with semi-structured expert interviews to explore how Sri Lanka's cybercrime legislation aligns with global human-rights standards and governance frameworks. The approach is interpretive and exploratory rather than hypothesis-testing, consistent with the traditions of socio-legal and policy research.

Doctrinal Analysis

The doctrinal strand critically examines key statutory instruments namely the Computer Crimes Act (2007), Electronic Transactions Act (2006), Personal Data Protection Act (2022), and Online Safety Act (2024) against international instruments such as the Budapest Convention (2001), General Data Protection Regulation (2018), and the EU NIS2 Directive (2023). The analysis evaluates six domains regarded as pillars of effective cyber law: offence definitions, procedural powers, digital-evidence admissibility, privacy safeguards, institutional coordination, and international cooperation. Each domain is assessed for consistency with principles of proportionality, legality, and rights-based oversight.

Expert Interviews

To complement the textual analysis, five semi-structured interviews were conducted between May and July 2020 with purposely selected experts representing the judiciary, legal profession, academia, industry, and policy sector. Participants included an appellate-court judge, a senior lawyer, a cybersecurity consultant, a university legal scholar, and a government policymaker. Each interview lasted approximately 90 minutes and followed a

flexible guide addressing four themes: definitions and typologies of cybercrime, institutional capacity, cross-border cooperation, and reform priority.

Data Analysis

Interview transcripts were thematically analysed using Braun and Clarke's six-phase framework familiarisation, coding, theme generation, review, definition, and reporting to integrate doctrinal insights with practitioner perspectives. Triangulation between sources ensured analytical rigour, while reflexive memoing preserved interpretive depth. This hybrid design provided an empirically grounded and normatively coherent basis for formulating the layered reform framework presented in subsequent sections

Findings

The analysis identified three interconnected domains of deficiency within Sri Lanka's cybercrime legal framework: (1) legislative and definitional gaps, (2) rights-protection weaknesses, and (3) institutional and procedural shortcomings. These themes emerged consistently across doctrinal review and expert interviews, underscoring the urgency for a coherent, rights-based reform agenda.

Legislative and Definitional Gaps

The Computer Crimes Act (2007) remains the central instrument for prosecuting cyber-related offences; however, its language reflects a pre-AI era. Interviewees highlighted several deficiencies:

Outdated offence categories: The Act employs technology-neutral definitions that fail to capture algorithmic manipulation, data-poisoning, or cloud-based intrusions.

Absence of AI, ransomware, blockchain and cryptocurrency provisions: Neither the CCA nor related statutes recognise AI-driven deception, ransomware-as-a-service, or decentralised-finance frauds.

Ambiguity in digital-evidence rules: Courts lack clear criteria for admissibility, authenticity, and chain-of-custody. Hence evidence is often dismissed or delayed because forensic procedures are undefined.

Limited cross-border enforceability: Mutual Legal Assistance Treaties (MLATs) remain inactive, restricting collaboration with jurisdictions under the Budapest Convention.

These legal gaps weaken deterrence and complicate prosecution of complex cyber-offences that transcend national boundaries.

Rights-Protection Weaknesses

Both doctrinal and interview evidence reveal that the present framework insufficiently safeguards individual rights:

Privacy and data protection: Although the Personal Data Protection Act (2022) was enacted, the oversight authority is yet to be operationalised. Consequently, data subjects lack effective remedies for misuse or breaches.

Freedom of expression: The 2019 temporary social-media ban following the Easter attacks exemplified executive overreach without judicial authorisation. Such measures contradict the ICCPR Articles 17 and 19.

Overbroad investigative powers: The Online Safety Act (2024) grants authorities access to personal data and the ability to remove content without a proportionality test or independent review.

Due-process inconsistencies: Notification of investigation, right to appeal, and mechanisms for data erasure are inadequately defined, limiting procedural fairness.

From a governance perspective, these weaknesses erode public trust and threaten Sri Lanka's compliance with its obligations under international human-rights law.

Institutional and Procedural Shortcomings

Stakeholders repeatedly emphasised that institutional fragmentation and limited capacity hinder effective enforcement:

Overlapping mandates: Sri Lanka CERT, the ICT Agency, and law-enforcement divisions operate with minimal coordination or shared protocols.

Resource constraints: Specialised cybercrime units within the CID and CERT lack digital-forensic expertise and technical infrastructure.

Judicial knowledge gap: Judges and prosecutors are seldom trained in digital evidence handling or international cooperation procedures.

Absence of incident-reporting culture: Private and public institutions are not legally required to disclose breaches, resulting in data under-reporting and limited situational awareness.

These issues collectively point to the absence of a national cybersecurity governance framework capable of unifying institutional efforts.

Comparative Insights

Cross-jurisdictional analysis revealed that Sri Lanka lags behind regional and international peers:

Country/ Region	**Key Instruments**	**Distinctive Features**	**Lessons for Sri Lanka**
India	DPDP Act 2023	Consent-based data use; breach reporting	Link privacy with enforcement
Singapore	Cybersecurity Act 2018; PDPA	CII audits; provider licensing	Ensure sectoral compliance
European Union	NIS2; GDPR	Resilience and rights-based rules	Embed rights and risk duties
ASEAN Region	Cybersecurity Strategy 2025	Regional standards alignment	Strengthen cooperation, MLATs

Table 1. Comparative Cyber Law Frameworks and Key Lessons for Sri Lanka

Comparatively, Sri Lanka lacks institutional coherence and harmonised risk-management obligations. Participants stressed that without a unified authority

similar to Singapore's CSA, the country risks remaining reactive rather than strategic.

Empirical Interview Themes

The interviews revealed four recurring themes that humanise the doctrinal findings:

1. Need for rights-based modernisation: Experts agreed that criminalisation alone cannot build public trust; reforms must embed privacy, dignity, and accountability.

2. Institutional fragmentation: Respondents described overlapping leadership among ICTA, CERT, and the Ministry of Justice as a barrier to timely policy action.

3. Judicial and educational gaps: Continuous professional development in digital-forensic science and cyber-law interpretation was widely requested

4. Public-awareness deficit: Citizens remain largely unaware of their legal remedies, reducing deterrence and engagement with digital-rights discourse.

5. These perspectives reflect the socio-legal dimension of cyber governance emphasising that law reform must be accompanied by education and institutional learning.

Synthesis

Across doctrinal and empirical evidence, three converging insights emerge:

1. Legal modernisation requires updated offence definitions, cross-border enforcement mechanisms, and digital-evidence standards consistent with the Budapest Convention.

2. Institutional capacity-building demands a national digital-forensics laboratory, inter-agency coordination framework, and regular judicial training.

3. Rights integration necessitates embedding privacy, proportionality, and transparency principles into investigative and regulatory practice.

Collectively, these findings confirm that Sri Lanka's cybercrime framework remains reactive, executive-driven, and fragmented. Without legislative renewal and institutional reform, digital governance risks becoming a source of rights violations rather than protection. The next section interprets these findings through a policy lens, demonstrating how layered reforms grounded in human rights, institutional capacity, and international alignment can guide Sri Lanka toward resilient and democratically legitimate cyber governance.

Discussion

The findings reveal a decisive need to reinterpret cybercrime law not merely as a technical instrument but as a pillar of democratic governance. The legislative gaps, rights deficiencies, and institutional fragmentation identified in this study illustrate how the absence of coordinated cyber policy undermines both national security and citizens' trust in the state. Within the humanities and social-science perspective, law operates as a social contract that mediates power, participation, and accountability in the digital sphere. Hence, reform must embed human values and ethical governance alongside legal precision.

From Control to Governance

Sri Lanka's cybercrime framework reflects a command-and-control model inherited from early post-colonial legal drafting. Such an approach prioritises state surveillance and enforcement over participatory governance. As Locke's theory of consent underscores, legitimacy derives from public accountability, not coercion. A rights-based cyber law must therefore replace unilateral executive discretion with transparent, consultative mechanisms that engage civil society, academia, and industry. This shift from control to governance would restore the normative balance between security and liberty.

International Norms and Comparative Lessons

Global instruments such as the Budapest Convention, GDPR, and NIS2 Directive provide a normative compass for reform. They link security obligations to privacy, transparency, and proportionality principles that remain weakly embedded in Sri Lanka's current statutes. The European Union's experience demonstrates that cybersecurity resilience can coexist with rights protection when duties of reporting, accountability, and oversight are legally codified. Similarly, India's DPDPA 2023 integrates consent and grievance redress, while Singapore's Cybersecurity Act 2018 enforces sectoral compliance through independent regulation. These examples illustrate that cyber law reform must combine legal precision with institutional maturity and public participation.

Human Rights and Digital Justice

Interview participants repeatedly highlighted the ethical dimension of cyber governance: security cannot be pursued at the expense of dignity and freedom. The absence of effective data-protection enforcement, overbroad investigative powers, and inadequate judicial review jeopardise Sri Lanka's obligations under the International Covenant on Civil and Political Rights (1966). Embedding human-rights clauses within cyber legislation would strengthen legitimacy and global credibility. Rights such as privacy, expression, and access to remedy must be framed as enforceable entitlements, not discretionary benefits.

Institutional Coordination and Capacity

Sustainable cyber governance requires capable, coordinated institutions. The interviews revealed a governance vacuum caused by overlapping agencies CERT, ICTA, and law-enforcement units each operating without shared protocols. Establishing a National Cybersecurity Commission would centralise oversight, streamline reporting, and align national standards with international frameworks. Investment in a certified digital-forensics laboratory, cross-agency data-sharing agreements, and judicial training programmes would enhance investigative efficiency while maintaining due-process safeguards. Such institutional strengthening represents both a capacity-building and a trust-building exercise.

Societal Awareness and Public Engagement

Policy effectiveness ultimately depends on public understanding. Limited legal literacy and digital-rights awareness among citizens perpetuate under-reporting of cyber incidents. A national awareness campaign integrated into school curricula and professional training could empower citizens to recognise cyber risks, report offences, and exercise data-protection rights. Embedding digital citizenship education within the broader civic-education agenda would transform cyber law from an elite legal domain into a participatory governance tool.

Towards Adaptive Governance

Finally, reform must be conceived as an adaptive process responsive to technological change. Fixed statutory definitions risk obsolescence; hence, a Triennial Cyber Law Review Cycle is proposed to evaluate emerging risks such as quantum computing, artificial intelligence, and deepfake manipulation. Continuous policy review, informed by academic research and public consultation, would ensure flexibility while upholding legal certainty. This adaptive model positions Sri Lanka to anticipate, rather than merely react to, future threats.

Overall, the discussion situates cybercrime law within the continuum of governance, rights, and accountability. Legislative reform without institutional and cultural transformation would merely reproduce existing weaknesses. Conversely, a layered approach linking legal modernisation, institutional development, and civic participation can embed digital resilience within democratic practice. Cyber law thus becomes not only a defence mechanism but a framework for inclusive, transparent, and rights-centred governance suited to the digital age.

Reform Framework

Translating analysis into actionable reform requires a multi-layered approach that strengthens institutions, aligns legislation with international standards, and restores public confidence in digital governance. This study proposes a four-layered rights-based framework designed to guide ms with adaptive governance illustrated in Figure1.

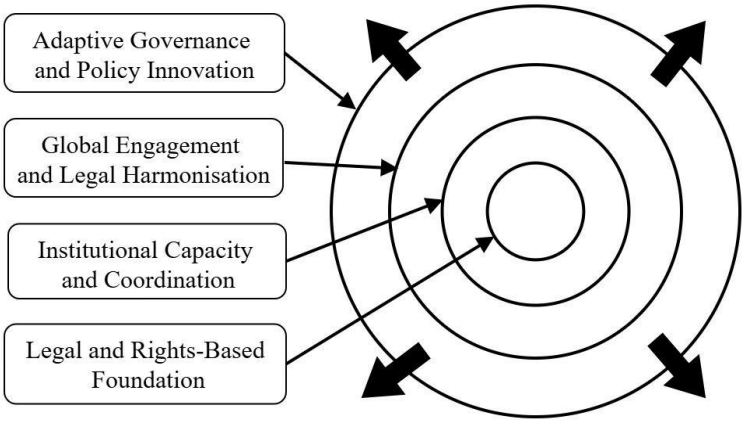

Fig.1. Proposed cybersecurity law reform framework.

Layer 1: Legal and Rights-Based Foundation

Legislative renewal must begin by redefining offences and embedding rights protections. Amendments to the Computer Crimes Act (2007) should include explicit provisions for AI-enabled crime, crypto-currency abuse, and supply-chain attacks. Simultaneously, full implementation of the Personal Data Protection Act (2022) is essential to guarantee privacy, transparency, and accountability. A constitutional clause affirming digital rights covering privacy, due process, and freedom of expression would anchor reforms within democratic legitimacy. All new laws should undergo human-rights impact assessments prior to enactment.

Layer 2: Institutional Capacity and Coordination

Sri Lanka needs a unified structure for cyber governance. Establishing a National Cybersecurity Commission (NCC) under the Ministry of Justice could consolidate existing agencies such as CERT, ICTA, and law-enforcement cyber units. The NCC should oversee a National Digital Forensics Laboratory, responsible for certification, evidence handling, and expert training. Judges, prosecutors, and investigators must undergo continuous professional education on digital-evidence management and cross-border legal processes. Inter-agency coordination protocols using MITRE ATT&CK, ISO 27001, and STRIDE standards will enable coherent policy implementation and accountability.

Layer 3: Global Engagement and Legal Harmonisation

International collaboration remains a cornerstone of modern cyber law. Sri Lanka should operationalise its obligations under the Budapest Convention (2001) by finalising Mutual Legal Assistance Treaties (MLATs) and participating in joint investigations through INTERPOL. Adopting core elements of the EU NIS2 Directive (2023) such as breach notification, supply-chain security, and minimum resilience standards will facilitate alignment with global partners. Active involvement in the ASEAN Cybersecurity Cooperation Strategy (2025) and other regional frameworks will enhance interoperability and trust in cross-border data flows.

Layer 4: Adaptive Governance and Policy Innovation

Cyber law must evolve with technological progress. A Triennial Cyber Law Review Cycle should be institutionalised to evaluate new risks arising from quantum computing, deepfakes, and emerging AI models. Public consultations involving academia, industry, and civil-society organisations should precede every major amendment. Establishing a Cyber Law Research and Training Centre at university level can support continuous policy learning and evidence-based law-making. Periodic publication of a national Cybersecurity White Paper would ensure transparency and stimulate informed public debate.

Implementation Timeline

Timeframe	Key Actions
Short-term (0 – 12 months)	Amend Computer Crimes Act (2007) to include AI and cryptocurrency offences; activate the Data Protection Authority; establish a National Digital Forensics Laboratory.
Medium-term (1 – 3 years)	Form a National Cybersecurity Commission; launch mandatory breach-notification rules; train judiciary and law enforcement; develop a Critical Infrastructure Protection Framework.

Long-term (3 – 5 years)	Ratify Mutual Legal Assistance Treaties (MLATs); embed surveillance oversight mechanisms in primary legislation; operate a Cyber Law Research Centre; publish an annual National Cyber Governance Review.

Policy Rationale

This four-layered model balances security, rights, and innovation. It positions Sri Lanka within global cybersecurity discourse while preserving constitutional guarantees of liberty and privacy. The framework encourages evidence-based policymaking and participatory reform, positioning the nation as a regional exemplar of rights-centred digital governance.

Conclusion

Sri Lanka's existing cybercrime framework, centred on the Computer Crimes Act (2007), no longer reflects the realities of a digitised society. The research demonstrates that outdated definitions, weak procedural safeguards, and fragmented institutions have limited the country's ability to prevent, investigate, and prosecute cyber-offences while upholding citizens' rights. Without coordinated reform, digital governance risks eroding public trust and hindering participation in the global digital economy.

This study advances a four-layered reform model that integrates human-rights protection, institutional coordination, international harmonisation, and adaptive governance. Modernising legislation, enforcing the Personal Data Protection Act (2022), and establishing a National Cybersecurity Commission would enhance accountability and capacity. Incorporating international standards such as the Budapest Convention and NIS2 Directive ensures interoperability and cross-border cooperation. Equally important is embedding ethical oversight, judicial training, and digital-rights literacy to create a culture of informed participation. The findings underscore that cybercrime law reform is not solely a technical or legal necessity; it is a constitutional and moral responsibility to safeguard liberty, dignity, and the rule of law. By aligning national legislation with democratic principles and global norms, Sri Lanka can position itself as a regional leader in rights-based digital governance. Implementing this framework will enable a secure, transparent, and inclusive digital future that strengthens both state resilience and citizen empowerment.

References

Aggarwal, D., Brennen, G.K., Lee, T., Santha, M. and Tomamichel, M. (2018) 'Quantum attacks on Bitcoin, and how to protect against them', Ledger, 3, pp. 68–90.

Baharlouei, R., Kouhizadeh, M. and Saberi, S. (2024) 'Blockchain governance and legal compliance for cybersecurity resilience', Computer Law & Security Review, 54, 102031.

Braun, V. and Clarke, V. (2006) 'Using thematic analysis in psychology', Qualitative Research in Psychology, 3(2), pp. 77–101.

Bryman, A. (2016) Social Research Methods, 5th edn. Oxford: Oxford University Press.

Cernomoreț, V. and Nastas, A. (2023) 'Cybercrime attribution and legal challenges in emerging democracies', Journal of Information Law and Technology, 29(1), pp. 1–19.

Chainalysis (2022) Crypto crime report 2022. Available at: https://www.chainalysis.com (Accessed 30 July 2025).

Chynoweth, P. (2009) 'Legal research', in Knight, A. and Ruddock, L. (eds.) Advanced Research Methods in the Built Environment. Oxford: Wiley-Blackwell, pp. 28–38.

Council of Europe (2001) Convention on Cybercrime (Budapest Convention). Budapest: Council of Europe.

Curtis, S. and Oxburgh, E. (2022) 'Evidentiary challenges in digital investigations', International Journal of Law and Information Technology, 30(3), pp. 219–236.

European Commission (2016) General Data Protection Regulation (Regulation (EU) 2016/679). Official Journal of the European Union.

European Commission (2023) Directive (EU) 2022/2555 on measures for a high common level of cybersecurity (NIS2 Directive). Official Journal of the European Union.

European Union (2024) Artificial Intelligence Act (AI Act). Brussels: European Parliament and Council.

Freedom House (2021) Freedom on the Net 2021: The global drive to control big tech. Available at: https://freedomhouse.org/report/freedom-net/2021 (Accessed 30 July 2025).

Government of India (2023) Digital Personal Data Protection Act (DPDPA). New Delhi: Government Press.

Government of Singapore (2018) Cybersecurity Act 2018. Singapore: Government Gazette.

Government of Sri Lanka (2006) Electronic Transactions Act No. 19 of 2006. Colombo: Government Press.

Government of Sri Lanka (2007) Computer Crimes Act No. 24 of 2007. Colombo: Government Press.

Government of Sri Lanka (2022) Personal Data Protection Act No. 9 of 2022. Colombo: Government Press.

Government of Sri Lanka (2024) Online Safety Act 2024. Colombo: Government Press.

Haddaji, A., Boulila, W. and Gargouri, F. (2024) 'A comparative study of cyber law frameworks and AI-enabled crime prevention', Information & Computer Security, 32(2), pp. 143–160.

Kemp, R. (2020) 'Building resilience through legal design: cybercrime law reform in developing economies', Computer Law Review International, 21(4), pp. 97–110.

Kulesza, J., McDermott, Y. and Galperin, H. (2022) 'Human rights and cybersecurity: bridging gaps in digital governance', Computer Law & Security Review, 46, 105733.

Lampe, R. and Meng, J. (2023) 'Institutional capacity and governance of cybersecurity in Asia', Asian Journal of Public Policy, 13(1), pp. 65–84.

Lee, J., Kim, S. and Park, Y. (2023) 'Cybersecurity policy harmonisation under NIS2: Lessons for emerging economies', Telecommunications Policy, 47(8), 102567.

Perera, A. and Mahanamahewa, P. (2017) 'Revisiting Sri Lanka's cybercrime regime', Sri Lanka Journal of Law, 9(2), pp. 115–132.

Raghavan, S. (2023) 'Cybercrime law enforcement and due process in South Asia', International Journal of Law and Information Technology, 31(4), pp. 412–433.

United Nations (1966) International Covenant on Civil and Political Rights (ICCPR). New York: UN General Assembly.

Venkatasamy, V., Govender, I. and Moodley, S. (2024) 'Digital rights, privacy, and governance reforms in developing countries', Information & Communications Technology Law, 33(1), pp. 87–108.

van Hoecke, M. (2018) Methodologies of Legal Research: What Kind of Method for What Kind of Discipline? Oxford: Hart Publishing.

West, D. (2023) 'Ransomware economics and policy gaps', Brookings Institution Tech Policy Series, pp. 1–14.

Whitty, M., Moustafa, N. and Grobler, M. (2024) 'AI-enabled cyberattacks and policy responses', Journal of Cyber Policy, 9(1), pp. 25–42.

Appendices

Appendix A – Abbreviations

AI	Artificial Intelligence
CCA	Computer Crimes Act
CERT	Computer Emergency Readiness Team
GDPR	General Data Protection Regulation
MLAT	Mutual Legal Assistance Treaty
NIS2	Network and Information Systems Directive
PDPA	Personal Data Protection Act
OSA	Online Safety Act
ICTA	Information and Communication Technology Agency
NCC	National Cybersecurity Commission
STRIDE	Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, Elevation of Privilege

Appendix B – Summary of Key Informant Insights

Stakeholder Group	Key Observations
Judiciary	Lack of judicial training in digital evidence handling and international cooperation.
Law Enforcement	Limited forensic tools and overlapping authority among investigative units.
Legal Practitioners	Absence of clear procedural safeguards for privacy and due process.
Academia	Need for integration of digital rights and ethics in legal education.
Policymakers	Urgent need to harmonise domestic laws with Budapest Convention and NIS2.

Appendix C – Layered Reform Framework Summary

Layer	Core Focus	Key Measures
1	Legal and Rights-Based Foundation	Amend CCA; operationalise PDPA; constitutional digital rights clause.
2	Institutional Capacity and Coordination	Establish NCC; train judiciary; build national digital forensics lab.
3	Global Engagement and Harmonisation	Ratify MLATs; adopt NIS2-equivalent obligations; join ASEAN cooperation.
4	Adaptive Governance	Triennial review; Cyber Law Research Centre; annual cybersecurity white paper.