Governing Next-Generation Cyber Threats: Evaluating Legal Preparedness for AI-Enabled Fraud, Ransomware, and Corporate Liability in Malaysia

Muhammad Izzat Haziq Rosli[1], Muhammad Amsyar Ku Ahmad Adzam[2], Muhammad Haziq Azman[3], Khairun Sazwani Ibrahim[4], Maryam Jameelah Mohamad Isa[5], Nuramalina Azman[6]*, Syajaratudur Abd Rahman[7]

[1,2,3,4,5,6]Faculty of Law, Universiti Teknologi MARA (UiTM), Shah Alam, Selangor, Malaysia

[7]Jabatan Peguam Negara, Cawangan Wilayah Persekutuan Kuala Lumpur, Malaysia

***Corresponding Author**

DOI: https://doi.org/10.47772/IJRISS.2026.101000189

Received: 15 October 2026; Accepted: 21 October 2026; Published: 31 October 2026

ABSTRACT

As rapid technological advancement accelerates the global digital economy, modern cybercrime in Malaysia has increasingly shifted toward automated, high-impact threat vectors, including Artificial Intelligence (AI)-enabled fraud, voice cloning, deepfakes, ransomware extortion, and Internet of Things (IoT) vulnerabilities. However, Malaysia's primary cybercrime legislation, the Computer Crimes Act 1997 (CCA 1997), has remained static since its enactment, raising critical questions regarding its legal adequacy to govern next-generation cyber threats. This study evaluates Malaysia's legal preparedness against modern cyber threats by examining statutory gaps within the CCA 1997 and identifying necessary legislative reforms. Adopting a qualitative socio-legal research methodology, this paper synthesizes doctrinal legal analysis of Malaysian cyber laws and the comparative UK framework under the Computer Misuse Act 1990 (CMA 1990) with semi-structured empirical interviews conducted across five individual institutional stakeholders spanning four core sectors (digital forensics/academia, regulatory enforcement, prosecution/state legal advisory, and defence litigation). The findings indicate that while Sections 3 and 4 of the CCA 1997 maintain basic functional utility for unauthorized access, the statute exhibits severe deficiencies in addressing AI-assisted deception, preparatory malware/hacking tools, system impairment, and corporate liability for systemic cybersecurity failures. Furthermore, enforcement is heavily hindered by difficulties in digital attribution, cloud evidence preservation, and cross-border Mutual Legal Assistance (MLA) delays. The study concludes that Malaysia urgently requires a technology-neutral legislative framework that criminalizes preparatory cybercrime tools, establishes corporate liability, introduces tiered sentencing for critical national infrastructure, and harmonizes domestic law with the Budapest Convention on Cybercrime and the newly passed Cybercrimes Bill 2026 (D.R. 8/2026).

Keywords: Computer Crimes Act 1997, Artificial Intelligence, Ransomware, Legal Reform, Cybercrimes Bill 2026, Corporate Liability

INTRODUCTION

The rapid proliferation of Information and Communication Technology (ICT) has fundamentally reshaped the global legal and economic landscape. As nations transition toward digitized governance and automated commercial ecosystems, the nature of criminality in cyberspace has evolved at an unprecedented velocity. Traditional computer-assisted offences such as simple unauthorized access and basic electronic fraud have increasingly given way to sophisticated, high-impact threat vectors. Today, cybercrime in Malaysia is defined by Artificial Intelligence (AI)-driven social engineering, automated phishing kits, voice-cloning extortion,

ransomware-as-a-service (RaaS) networks, and critical national infrastructure targeted intrusions (Lusthaus, 2024; Cybersecurity Ventures, 2024).

Despite these profound technological shifts, Malaysia's primary statutory shield against computer-related offences remains the Computer Crimes Act 1997 (Act 563) ('CCA 1997'). Enacted nearly three decades ago during the genesis of the Multimedia Super Corridor (MSC), Act 563 provided a pioneering statutory framework modeled largely on early Commonwealth legislation (Beatty, 1998; Lee, 2022). However, while the digital ecosystem has undergone multiple paradigm shifts, the CCA 1997 has remained static, devoid of substantive legislative amendments (Hamin & Abu Hassan, 2009). This legislative inertia has created significant statutory lacunae, exposing critical gaps in Malaysia's legal defence when confronted with next-generation threats.

This paper examines the legal adequacy of Malaysia's cybercrime framework in governing next-generation threats. By conducting a comparative doctrinal analysis against the United Kingdom's frequently updated Computer Misuse Act 1990 ('CMA 1990') and evaluating empirical qualitative insights from key institutional stakeholders including the Attorney General's Chambers (AGC), the Malaysian Communications and Multimedia Commission (MCMC), digital forensics experts, and defence practitioners, this study identifies core statutory deficiencies, evaluates ongoing legislative initiatives like the Cybercrimes Bill 2026 (D.R. 8/2026), and proposes evidence-based policy recommendations.

LITERATURE REVIEW

2.1 Conceptualizing Modern Cybercrime: Cyber-Dependent vs. Cyber-Enabled Threats

In legal and criminological literature, defining computer crime requires a clear distinction between 'cyber-dependent' and 'cyber-enabled' offences (Phillips et al., 2022; Clough, 2015). Cyber-dependent crimes are offences that can only be committed through the use of Information and Communication Technology (ICT) devices, where the computer system is both the tool and the target of the offence (e.g., unauthorized access, malware dissemination, denial-of-service attacks, and ransomware extortion). Conversely, cyber-enabled crimes are traditional offences such as fraud, extortion, theft, and criminal defamation that are scaled or facilitated in volume and reach by digital networks (Wall, 2004; Payne, 2020; Grabosky, 2001).

Clough (2015) notes that legal analysis of computer misuse statutes must focus primarily on cyber-dependent integrity and availability offences. When evaluating statutes like Malaysia's CCA 1997 and the UK's CMA 1990, legal scholars emphasize that computer misuse acts were specifically designed as targeted penal instruments to protect the confidentiality, integrity, and availability (CIA triad) of computer data and processing systems, rather than general online content or financial crime regimes (Koops, 2010; Fafinski, 2008). Understanding this distinction is vital to avoid conflating computer misuse legislation with broader regulatory statutes such as the Communications and Multimedia Act 1998 (Act 588) or general fraud provisions under the Penal Code (Act 574).

2.2 The Evolution of Threat Vectors: From Basic Hacking to AI Deception and System Impairment

The historical literature illustrates that early computer crime legislation was drafted around two primary threat vectors: unauthorized entry ('hacking') and unauthorized modification of computer data ('virus dissemination') (Beatty, 1998; Brenner, 2010; Hamin, 2004). However, modern cybercrime threat vectors have expanded into automated, highly decentralized operational models (McIntyre, 2016).

A critical area of emerging legal uncertainty involves Artificial Intelligence (AI)-enabled cybercrime and automated online fraud networks (Lusthaus, 2024; Ismail et al., 2025). AI technologies empower malicious actors to execute automated vulnerability scanning, craft hyper-realistic deepfake video/audio for executive impersonation and voice-cloning fraud, and bypass biometric security controls. It must be noted, however, that while AI-automated vulnerability scanning constitutes a cyber-dependent preparatory threat, AI deepfakes and voice-cloning operate primarily as cyber-enabled frauds. As such, they largely fall outside the strict purview of computer misuse statutes like the CCA 1997 unless accompanied by a direct unauthorized system breach and

are instead prosecuted under general penal fraud provisions (e.g., Sections 415, 417, or 420 of the Penal Code) or Section 233 of the Communications and Multimedia Act 1998. Furthermore, the rise of the Internet of Things (IoT) has expanded the physical attack surface, exposing vulnerable smart-home systems, connected industrial machinery, and medical devices to remote takeover (Taylor et al., 2015).

Another major area of evolution concerns Distributed Denial-of-Service (DDoS) attacks and ransomware extortion networks. Unlike simple unauthorized access, ransomware attacks disrupt operational continuity by encrypting critical data and threatening double-extortion through public leak sites (McIntyre, 2016). As noted by United Nations Office on Drugs and Crime (UNODC, 2013), modern cyber syndicates operate as sophisticated multinational commercial enterprises, exploiting cross-border cloud infrastructure and cryptocurrency mixing services to evade national law enforcement.

2.3 Critiques of Malaysia's Computer Crimes Act 1997: Legislative Stagnation and Statutory Gaps

The Malaysian legal literature consistently characterizes the Computer Crimes Act 1997 as a static, outdated legal instrument (Hamin & Abu Hassan, 2009; Hamin et al., 2011). While Act 563 provided a pioneering framework during the launch of the Multimedia Super Corridor (MSC), Parliament's failure to enact periodic statutory amendments has left severe legal lacunae (Beatty, 1998; Lee, 2022).

Scholars identify several major structural gaps within the CCA 1997:

a. Absence of Express Provisions for System Impairment and DDoS: While Section 2(7)(c) includes 'an event impairing the normal operation of a computer' within the definition of modification, Act 563 lacks an explicit, standalone offence for system impairment or Denial-of-Service attacks. Crucially, pure volumetric DDoS attacks overload network bandwidth or processing queues without actually altering, deleting, or adding to any computer data contents. Consequently, prosecuting such temporary availability disruptions forces prosecutors to rely on a statutory legal fiction, stretching older 'modification' concepts to fit scenarios where no actual data modification has occurred (Hamin et al., 2011; Appudurai, 2007).

b. Omission of Preparatory Cybercrime Tools: Unlike modern cyber statutes, the CCA 1997 contains no general offence penalizing the production, adaptation, supply, or possession of hacking tools, malware binaries, or exploit kits (beyond credentials under Section 6). Consequently, possessing or distributing malicious software builders remains unpunished until an actual intrusion occurs.

c. Lack of Tiered Sentencing for Critical National Infrastructure (CNI): The penalty regime under the CCA 1997 treats intrusions into personal computers identically to attacks targeting critical energy, financial, or healthcare infrastructure, lacking aggravated statutory tiers for severe public harm.

d. Nuanced Analysis of Corporate Criminal Liability and Regulatory Overlap: A major critique raised in the literature concerns the CCA 1997's exclusive focus on individual natural persons (Balasingam, 2022). While Section 17A of the Malaysian Anti-Corruption Commission Act 2009 (MACC Act) introduced corporate liability for bribery, Act 563 contains no 'failure to prevent cybercrime' mechanism. Corporations whose gross failure to maintain adequate cybersecurity safeguards facilitates massive data breaches or system compromise face no direct corporate criminal liability under primary penal legislation.

Furthermore, international legal scholars highlight that Malaysia has not accessioned to the Council of Europe's Budapest Convention on Cybercrime (ETS No. 185) (Khan et al., 2022; UNODC, 2013). This omission impairs international cooperation, digital evidence preservation, and Mutual Legal Assistance (MLA) requests during transnational cybercrime investigations (Mohamad et al., 2024; OECD, 2015).

2.4 Comparative Benchmarking: The Adaptive Legislative Path of the UK Computer Misuse Act 1990

In contrast to Malaysia's static approach, the United Kingdom has consistently modernized its Computer Misuse Act 1990 (c. 18) to ensure statutory alignment with technological change (Fafinski, 2008). Enacted following the landmark decision in R v Gold & Schifreen [1988] 1 AC 1063 where 19th-century forgery laws failed to

convict hackers who accessed the Telecom Prestel network, the CMA 1990 established a dedicated computer misuse framework.

Recognizing the limitations of its original 1990 text, the UK Parliament introduced major statutory amendments through subsequent legislation:

a. Police and Justice Act 2006: Replaced the narrow 'modification' requirement under Section 3 with an express offence covering system impairment and denial-of-service attacks. Crucially, Section 37 inserted Section 3A, criminalizing the making, supplying, or obtaining of articles (hacking tools and malware) intended for use in computer misuse offences.

b. Serious Crime Act 2015: Inserted Section 3ZA into the CMA 1990, creating an aggravated offence for computer misuse resulting in severe damage to human welfare, public safety, national security, or critical infrastructure, carrying a maximum penalty of life imprisonment. Furthermore, ongoing statutory reviews continue to evaluate the threshold and protective scope of computer misuse offences in the UK (Home Office, 2023; House of Commons Library, 2022).

2.5 Gaps in Existing Scholarship

A rigorous review of current scholarship reveals three significant gaps that this study addresses:

First, existing Malaysian literature is overwhelmingly descriptive rather than evaluative, frequently summarizing statutory provisions without critically testing their operational sufficiency against modern technological phenomena such as AI deepfakes, IoT attacks, and cloud computing (Laidey, 2021; Appudurai, 2007).

Second, there is a distinct lack of up-to-date comparative empirical research bridging the Malaysian framework with international developments, particularly regarding how law enforcement agencies and prosecutors manage emerging threats in practice (Khan et al., 2022).

Third, legal literature rarely incorporates primary stakeholder perspectives across judicial, regulatory, prosecutorial, forensic, and defence sectors. Academic commentary often analyzes statutory text in isolation, ignoring real-world evidentiary hurdles such as digital attribution beyond reasonable doubt, IP address fallacies (PP v Loh Guo Shi [2016] 1 SMC 190), cloud evidence preservation, and cross-border Mutual Legal Assistance delays (Mohamad et al., 2024; Foong, 2024).

METHODOLOGY

This study employs a qualitative socio-legal research design combining doctrinal legal analysis with empirical stakeholder inquiry (Stewart, 2025). Doctrinal research involved systematic analysis of primary statutory sources including Malaysia's Computer Crimes Act 1997 (Act 563), Cyber Security Act 2024 (Act 854), Personal Data Protection Act 2010 (Act 709), Communications and Multimedia Act 1998 (Act 588), and the proposed Cybercrimes Bill 2026 (D.R. 8/2026), alongside the UK's Computer Misuse Act 1990 and judicial precedents from Malaysian and Commonwealth courts.

To evaluate how these legal frameworks operate in practice ('law in action'), the empirical phase comprised semi-structured qualitative interviews conducted across five individual institutional stakeholders spanning four core expert categories:

1. **Category 1 (Digital Forensics & Academia):** Respondent A (Academic & Digital Forensic Expert) is a senior university professor and active digital forensics consultant possessing over 15 years of operational experience in evidence extraction, malware analysis, and expert witness testimony in Malaysian courts.
2. **Category 2 (Regulatory & Telecommunications Enforcement):** Respondent B (Regulatory & Enforcement Representative, MCMC) is a senior enforcement officer detailing regulatory oversight under Section 233 of the Communications and Multimedia Act 1998 (Act 588), digital evidence collection, service provider engagement, and technical forensic support.

3. **Category 3 (Prosecution & State Legal Advisory):** Respondent C (Prosecutorial Representative, AGC Putrajaya) is a Deputy Public Prosecutor specializing in economic and cyber-offences, providing insights into burden of proof, Section 3 and 4 statutory applications, digital evidence integrity, and international Mutual Legal Assistance (MLA) challenges; and Respondent E (Prosecutorial / Judicial Legal Officer, *Jabatan Peguam Negara* WPKL) is a senior legal officer contributing operational perspectives on prosecutorial readiness, charge framing, and inter-agency coordination.
4. **Category 4 (Cyber Litigation & Defence Bar):** Respondent D (Active Legal Practitioner & Defence Advocate) is a senior criminal defence advocate and civil litigation lawyer with extensive court experience in landmark cybercrime litigation (including PP v Loh Guo Shi), offering critical analysis on IP/MAC address attribution fallacies, standard of proof beyond reasonable doubt, civil lacunae, and commercial scam realities.

3.1 Participant Selection and Sampling Criteria

Data collection utilized purposive expert sampling to recruit institutional actors with direct operational involvement in Malaysia's cybercrime governance landscape. To ensure data credibility and interpretive depth, participants were required to meet two strict eligibility benchmarks: (i) a minimum professional threshold of 10 to 15 years of specialized institutional experience in cybercrime prosecution, telecommunications regulation, digital forensics, or criminal defence litigation, and (ii) direct institutional experience in drafting, enforcing, or litigating cyber offences under Act 563 or Act 588.

Interviews were conducted using a standardized semi-structured protocol covering statutory adequacy, digital evidence preservation, attribution hurdles, cross-border jurisdiction, and policy recommendations. Each interview session lasted between 45 and 60 minutes and was administered either in person or via secure videoconferencing platforms (Zoom and Google Meet). All sessions were audio-recorded with prior informed consent and transcribed verbatim. The qualitative data were analyzed using Braun & Clarke's six-phase thematic analysis framework, wherein initial code generation and subsequent theme development were conducted independently by two researchers to ensure inter-coder consistency. Methodological rigor and analytical validity were maintained through systematic data triangulation across primary statutory provisions, judicial case law, secondary academic literature, and stakeholder interview transcripts.

FINDINGS AND DISCUSSION

4.1 Practical Utility vs. Operational Obsolescence of Sections 3 and 4 CCA 1997

A central finding from the empirical interviews is that while Sections 3 and 4 of the CCA 1997 retain functional utility for basic unauthorized access, they are increasingly strained by contemporary threat mechanisms. AGC (Respondent C) and MCMC (Respondent B) confirmed that Section 3 remains applicable to modern intrusion techniques such as credential theft, session hijacking, API abuse, and cloud account takeovers because the core legal inquiry centers on whether access was 'unauthorized' or exceeded granted permission, regardless of the underlying technical medium.

However, institutional stakeholders unanimously acknowledged that the CCA 1997 exhibits severe operational gaps when confronted with modern threat vectors. The prosecution of ransomware, automated botnets, AI-assisted phishing, and cryptocurrency extortion requires stretching broad 1990s statutory language to fit complex 2020s phenomena. As noted by Respondent C (AGC) and Respondent E (Legal Officer), while Section 4 effectively links unauthorized access to a further intent to commit fraud or dishonesty, proving specific criminal intent beyond reasonable doubt in automated or fileless cyber-attacks presents immense evidentiary challenges.

4.2 Comparative Statutory Analysis: CCA 1997 vs. CMA 1990

To systematically evaluate legal adequacy, Table 1 provides a comparative synthesis between Malaysia’s CCA 1997 and the UK’s amended CMA 1990 across key statutory dimensions:

Table 1: Comparative Statutory Synthesis between CCA 1997 (Malaysia) and CMA 1990 (UK).

Statutory Dimension	Malaysia: Computer Crimes Act 1997	United Kingdom: Computer Misuse Act 1990 (Amended)
Basic Unauthorized Access	Section 3: Covers unauthorized access. Penalty: Fine up to RM50,000 / 5 yrs imprisonment.	Section 1: Covers unauthorized access. Penalty: Up to 2 yrs imprisonment on indictment.
Aggravated Access (Further Offence)	Section 4: Requires intent to commit/facilitate fraud/dishonesty. Penalty: Fine up to RM150,000 / 10 yrs.	Section 2: Requires intent to commit/facilitate further arrestable offence. Penalty: Up to 5 yrs.
System Impairment & DDoS	Section 5: Indirectly covered under 'modification' definition (s.2(7)(c)). No standalone DDoS provision.	Section 3 (as amended by Police and Justice Act 2006): Explicit standalone offence for unauthorized acts impairing operation/access. Penalty: Up to 10 yrs.
Preparatory Tools & Malware	No general provision penalizing creation, adaptation, supply, or possession of hacking tools/malware.	Section 3A (inserted by Police and Justice Act 2006): Criminalizes making, supplying, or obtaining tools for misuse. Penalty: Up to 2 yrs.
Critical National Infrastructure (CNI) Protection	No aggravated statutory tiers for CNI; attacks on critical infrastructure are penalized under general static provisions.	Section 3ZA (inserted by Serious Crime Act 2015): Explicit aggravated offence for CNI damage risking severe human or national security harm (up to life imprisonment).
Corporate Criminal Liability	Exclusive statutory focus on individual natural persons; Act 563 contains no corporate criminal liability or failure to prevent mechanism.	CMA 1990 relies on general corporate attribution principles (identification doctrine / directing mind and will); no statutory failure-to-prevent cybercrime offence.

Table 1 illustrates that while the original 1990s provisions of both statutes were structurally similar, the UK's iterative statutory revisions (Police and Justice Act 2006; Serious Crime Act 2015) successfully closed gaps regarding DDoS attacks, malware tools, and critical infrastructure harm-areas where Malaysia's CCA 1997 remains static.

4.3 Digital Evidence, Attribution Fallacies, and Judicial Precedents

A major empirical finding highlighted by prosecutorial respondents (Respondents C and E) and defence counsel (Respondent D) concerns digital evidence and attribution. In cybercrime prosecutions, establishing that a specific IP address or MAC address was involved in an attack does not equate to proving the identity of the human operator beyond reasonable doubt.

As demonstrated in the landmark decision Public Prosecutor v Loh Guo Shi [2016] 1 SMC 190, proving that an illicit transmission originated from a specific IP address registered to an accused is insufficient to establish guilt without corroborative evidence showing that the accused was the physical operator of the terminal at the material time. Respondent D emphasized that anti-forensic tools, open Wi-Fi networks, malware infection, and IP spoofing create significant attribution fallacies. Consequently, prosecutors must rely heavily on circumstantial evidence, physical device seizure, session logs, and witness testimony to bridge the gap between digital terminal identification and human attribution.

4.4 Cross-Border Enforceability, Cloud Computing, and Mutual Legal Assistance (MLA)

Both MCMC (Respondent B) and AGC (Respondent C) flagged cross-border jurisdiction as a primary operational bottleneck. Although Section 9 of the CCA 1997 confers extra-territorial jurisdiction where the target or computer is in Malaysia, extra-territorial statutory reach is virtually meaningless without international cooperation.

Because modern cybercriminals host infrastructure on overseas multi-tenant cloud servers and utilize encrypted communications, gathering evidence requires foreign service provider compliance. Respondent C explained that Mutual Legal Assistance (MLA) requests often take 6 to 18 months to process. By the time foreign authorities respond, volatile server logs have been overwritten. Furthermore, Malaysia's non-ratification of the Budapest Convention creates 'dual criminality' friction, forcing prosecutors to reframe charges to establish common legal ground, delaying evidence retrieval while foreign suspects conceal assets or delete digital traces.

4.5 Corporate Cybersecurity Negligence and the Enforcement Scope of Act 854 and PDPA 2010

When contextualizing corporate accountability within Malaysia's broader statutory landscape, a comprehensive legislative audit reveals that while corporate obligations exist under specialized regulatory frameworks, they possess critical enforcement limitations:

a. Cyber Security Act 2024 (Act 854): Part IV (Sections 15 to 26) imposes mandatory cybersecurity compliance, risk assessments (Section 22), and 6-hour incident reporting duties (Section 23) on designated National Critical Information Infrastructure (NCII) entities across 11 critical sectors, backed by corporate officer liability under Section 61 (NACSA, 2024). However, Act 854 functions primarily as a regulatory licensing and infrastructure protection regime for NCII entities, leaving non-NCII commercial enterprises completely outside its purview.

b. Personal Data Protection Act 2010 (Act 709): Section 9 imposes a data security principle on data users to protect personal data from loss or unauthorized access. However, Act 709 is strictly confined to processing personal data in commercial transactions; it does not criminalize systemic security failures that lead to proprietary corporate espionage, operational disruption, or industrial ransomware extortion.

As noted by Balasingam (2022) and supported by Respondent D, commercial enterprises currently operate in a regulatory shadow where the CCA 1997 cannot prosecute the company, Act 854 does not apply to non-NCII firms, and PDPA 2010 only addresses personal data. Introducing a corporate 'failure to prevent cybercrime' framework under primary cyber legislation would incentivize systemic corporate investment in cybersecurity resilience.

4.6 Substantive Evaluation of the Cybercrimes Bill 2026 (D.R. 8/2026)

To evaluate ongoing legislative reform efforts, this study examined the proposed Cybercrimes Bill 2026 (D.R. 8/2026), introduced in the Dewan Rakyat on 22 June 2026 for its first reading to repeal and replace Act 563. Having successfully passed both houses of Parliament (the Dewan Rakyat on 1 July 2026 and the Dewan Negara on 20 July 2026), the Bill has concluded parliamentary debate and is currently awaiting Royal Assent and Gazetting. A substantive analysis of the Bill reveals several significant statutory advancements that directly cure long-standing CCA 1997 lacunae:

a. Standalone System Impairment & DDoS Offence: Section 14 of D.R. 8/2026 introduces an express offence for unauthorized acts causing interference, system impairment, or denial-of-service, directly resolving the statutory ambiguity under Section 5 of the CCA 1997.

b. Criminalization of Cybercrime Tools: Section 15 models Section 3A of the UK CMA 1990 by explicitly penalizing the production, adaptation, supply, or possession of malware, exploit kits, and hacking tools.

c. Increased Penalty Thresholds: Sections 10 and 11 replace Sections 3 and 4 of the CCA 1997, increasing financial fines up to RM500,000 for aggravated intrusion offences.

d. Data Preservation Orders: Section 24 empowers law enforcement to issue 90-day digital data preservation orders to electronic service providers, bridging cross-border delays during international investigations.

However, respondents cautioned that D.R. 8/2026 exhibits potential statutory overbreadth if enacted without precise safeguards. Respondent A (digital forensic expert) observed that clauses penalizing malware handling must incorporate explicit *mens rea* protections for ethical hackers and penetration testers. Respondent D added

that the Bill's proposed corporate liability provisions must clearly harmonize with existing obligations under Act 854 and PDPA 2010 to avoid double jeopardy while ensuring clear statutory defence.

4.7 Critical Evaluation of UK Comparative Suitability and Local Institutional Context

A crucial nuance emerged from empirical interviews regarding comparative law adoption. While the UK CMA 1990 offers valuable benchmark models, respondents strongly cautioned against blindly copy-pasting foreign statutory frameworks. As emphasized by Respondent D (legal practitioner), Malaysia's legal response must reflect local enforcement realities, police forensic capacity, differences between Crown Prosecution Service (CPS) guidelines (Crown Prosecution Service, 2023) and AGC prosecutorial discretion, and local judicial evidentiary standards under the Evidence Act 1950. Respondent D pointed to regional comparators like Singapore (e.g., Cybersecurity Act 2018 and Computer Misuse Act) as pragmatic reference points. Consequently, adopting UK provisions–such as Section 3ZA CNI penalties or Section 3A tool prohibitions–requires tailoring statutory language to fit Malaysia's procedural framework and local judicial standards.

CONCLUSION AND POLICY RECOMMENDATIONS

This study demonstrates that while Malaysia’s Computer Crimes Act 1997 provided a pioneering statutory foundation in 1997, its static design has rendered it inadequate to govern the modern cyber threat landscape. The emergence of AI-driven social engineering, ransomware networks, IoT vulnerabilities, and corporate security negligence necessitate a comprehensive modernization of Malaysia's cyber law architecture.

The following evidence-based policy recommendations are submitted to establish a resilient, legally sound, and future-ready framework:

5.1 Expedite Gazetting and Implementation of the Cybercrimes Bill 2026: Following the successful passage of the Cybercrimes Bill 2026 (D.R. 8/2026) through both houses of Parliament, executive authorities should prioritize securing Royal Assent and Gazetting to replace the static CCA 1997 framework. Implementation must ensure a 'technology-neutral' operational approach that penalizes criminal behaviour and systemic harm rather than specific transient technologies, maintaining long-term adaptability against AI-driven threats (as urged by Respondent A).

5.2 Criminalize Preparatory Cybercrime Tools with Strict *Mens Rea* Safeguards: Malaysia must insert explicit provisions criminalizing the creation, possession, adaptation, supply, and distribution of malware, exploit kits, ransomware builders, and botnet software (modelling UK s.3A). Crucially, to protect legitimate cybersecurity practices, ethical hackers, and penetration testers, the statutory offence must incorporate a strict *mens rea* threshold requiring proof of 'intent or belief that the tool will be used for criminal computer misuse', accompanied by an explicit statutory defence for authorized vulnerability research and penetration testing.

5.3 Establish a Corporate Criminal Liability Framework: Statutory amendments should introduce corporate criminal liability for commercial organizations that fail to maintain adequate cybersecurity safeguards or enable insider breaches through gross negligence. To maintain proportionality, the framework should adopt a 'failure to prevent cybercrime' model combined with a statutory defence of maintaining 'adequate procedures and cybersecurity safeguards', harmonizing with Act 854 and MACC Act Section 17A principles.

5.4 Introduce Proportionate Tiered Sentencing for Critical Infrastructure: Aligning with Section 3ZA of the UK CMA 1990, Malaysia should establish an aggravated sentencing tier for cyber-attacks against Critical National Infrastructure (CNI). To satisfy legal proportionality, maximum penalties (up to life imprisonment) should be strictly reserved for catastrophic attacks causing or risking direct severe harm to human welfare, public safety, or national security.

5.5 Harmonize Laws with the Budapest Convention on Cybercrime: Malaysia should formally accession to the Budapest Convention ETS No. 185 to streamline cross-border digital evidence preservation, extraditions, and Mutual Legal Assistance (MLA), eliminating dual criminality friction.

5.6 Institute Mandatory Periodic Legislative Reviews: Parliament should establish a statutory mechanism mandating comprehensive review of cybercrime legislation every three to five years, engaging multi-disciplinary panels of prosecutors, judges, cybersecurity experts, and legal scholars.

DECLARATION

Ethics approval for the primary data collection was obtained from the relevant institutional review/ethics committee at Universiti Teknologi MARA (UiTM). Informed consent was secured from all five interview respondents prior to recording. The authors declare no conflict of interest.

ACKNOWLEDGEMENT

This publication stems from a group project undertaken by students of the Faculty of Law, Universiti Teknologi MARA (UiTM), Shah Alam, under the supervision of Mdm. Nuramalina Azman. The authors express sincere gratitude to the research participants from the Attorney General's Chambers, MCMC, digital forensics sector, and the criminal defence bar for their invaluable insights.

REFERENCES

1. Appudurai, J. (2007). Computer Crimes: A Case Study of What Malaysia Can Learn from Others? Journal of Digital Forensics, Security and Law, 2(2), 7–24.
2. Balasingam, U. (2022). Corporate Criminal Liability: Some Reflections for Malaysia. Jurnal Institutions and Economies, 14(4), 115–141.
3. Beatty, D. L. (1998). Malaysia's 'Computer Crimes Act 1997' Gets Tough on Cybercrime But Fails to Advance the Development of Cyberlaws. Pacific Rim Law & Policy Journal, 7(2), 351–377.
4. Brenner, S. (2010). Cybercrime: Criminal Threats from Cyberspace. Praeger.
5. Clough, J. (2015). Principles of Cybercrime (2nd ed.). Cambridge University Press.
6. Crown Prosecution Service. (2023). Computer Misuse Act Prosecution Guidance. CPS Guidelines.
7. Cybersecurity Ventures. (2024). Cybercrime Damages Report 2024. Cybersecurity Ventures.
8. Fafinski, S. (2008). Access Denied: Computer Misuse in an Era of Technological Change (Doctoral dissertation, University of Leeds).
9. Foong, C. L. (2024). Foong's Malaysia Cyber, Electronic Evidence and Information Technology Law (2nd ed.). Sweet & Maxwell Asia.
10. Grabosky, P. N. (2001). Virtual Criminality: Old Wine in New Bottles? Social & Legal Studies, 10(2), 243–249.
11. Hamin, Z. (2004). The Legal Response To Computer Misuse In Malaysia - The Computer Crimes Act 1997. Universiti Teknologi MARA.
12. Hamin, Z., & Abu Hassan, R. (2009). Computer Crimes Act 1997: Adequacy and Challenges. Journal of Malaysian and Comparative Law, 36, 45–68.
13. Hamin, Z., Saripan, H., & Abu Hassan, R. A. (2011). The Legal Critiques of the Computer Crimes Act 1997 in Regulating Cyber Crime. UiTM Institutional Repositories.
14. Home Office. (2023). Review of the Computer Misuse Act 1990: Call for Information. UK Government.
15. House of Commons Library. (2022). Westminster Hall Debate on the Computer Misuse Act 1990. Parliament UK.
16. Ismail, N., Hassan, S. A., Zakuan, Z. Z. M., & Yusoff, R. M. (2025). Between Law and Technology: Online Scam Challenges and Legal Responses in Malaysia. International Journal of Research and Innovation in Social Science, 9(9), 4013–4022.
17. Khan, S., Saleh, T., Dorasamy, M., Khan, N., Tan, O. S. L., & Vergara, R. G. (2022). A Systematic Literature Review on Cybercrime Legislation. F1000Research, 11, 971.
18. Koops, B. J. (2010). The Internet and its Opportunities for Cybercrime. SSRN Electronic Journal.
19. Laidey, N. (2021). The Analysis of Computer Crimes Act 1997 in the Circumvention and Prevention of Computer Crimes in Malaysia. SSRN Electronic Journal.
20. Lee, C. (2022). Economic Transformation of Malaysia: The Role of the Multimedia Super Corridor. ISEAS Economics Working Paper.

21. Lusthaus, J. (2024). Reconsidering crime and technology: What is this thing we call cybercrime? Annual Review of Law and Social Science, 20(1), 369–385.
22. McIntyre, T. (2016). Cyber Law in Ireland. SCRIPTed, 13(3), 398–400.
23. Mohamad, A. R., Yaakop, M. R., & Razif, M. A. M. (2024). The Efficacy of the Malaysian Government's Response towards Cybercrime. Open Journal of Political Science, 14(1), 166–176.
24. National Cyber Security Agency (NACSA). (2024). Cyber Security Act 2024 (Act 854) Overview. NACSA Malaysia.
25. Organisation for Economic Co-operation and Development (OECD). (2015). Recommendation of the Council on Digital Security Risk Management for Economic and Social Prosperity. OECD Legal Instruments.
26. Payne, B. K. (2020). Defining Cybercrime. In The Palgrave Handbook of International Cybercrime and Cyberdeviance.
27. Phillips, K., Davidson, J. C., Farr, R. R., Burkhardt, C., Caneppele, S., & Aiken, M. (2022). Conceptualizing Cybercrime: A Systematic Review of Cybercrime Definitions. Forensic Sciences, 2(2), 379–398.
28. Stewart, L. (2025). Primary Data Collection Methods in Legal Research. ATLAS.ti Research Hub.
29. Taylor, R. W., Fritsch, E. J., & Liederbach, J. (2015). Digital Crime and Digital Terrorism (3rd ed.). Pearson.
30. United Nations Office on Drugs and Crime (UNODC). (2013). Comprehensive Study on Cybercrime. UNODC Publication.
31. Wall, D. S. (2004). What are Cybercrimes? Criminal Justice Matters, 58(1), 20–21.