DISSERTATION

ON

Artificial Intelligence-Driven Cyber Crimes and the Emerging Legal Challenges. A Study in the Context in USA,Singapore and Bangladesh

Course Title: Supervised Dissertation

Course Code: LAW 406

Submitted To:

Shah Maruf Uddin Ahmed

Lecturer, Department of Law

East West University

Submitted By:

All Imran Shaad

ID: 2021-1-66-036

Department of Law

Date of Submission: 17th June,2026

Word Count (Excluding footnote and Bibliography): 7985 Words

Consent Form

The dissertation titled “Artificial intelligence-driven cyber crimes and the emerging legal challenges. A study in the context in USA,Singapore and Bangladesh”prepared byAll Imran Shaad, ID:2021-1-66-036, submitted to Shah Maruf Uddin Ahmed,Lecturer, for the fulfillment of the requirements of Course 406 (Supervised Dissertation) for LL.B. (Hons) degree offered by the Department of Law, East West University is approved for Submission.

……..

Signature of the Supervisor

Date:17th june,2026

Acknowledgement

First and foremost, I would like to express my sincere gratitude to Almighty Allah for granting me the strength, patience, and opportunity to complete this thesis successfully.

I am deeply indebted to my respected supervisor, Shah Maruf Uddin Ahmed, for his invaluable guidance, constructive suggestions, continuous encouragement, and unwavering support throughout the preparation of this research. His insightful comments and expert supervision greatly contributed to the successful completion of this thesis.

I would also like to extend my heartfelt thanks to the faculty members of the Department of Law, East West University, for providing me with the academic knowledge and research skills that have been instrumental in conducting this study.

Special appreciation goes to the authors, researchers, legal scholars, and institutions whose books, articles, reports, statutes, case laws, and online resources were consulted during the course of this research. Their contributions have significantly enriched the quality of this thesis.

I am grateful to my family members for their constant support, encouragement, patience, and understanding throughout my academic journey. Their motivation has been a source of inspiration during the completion of this work.

Finally, I would like to thank my friends, classmates, and well-wishers who directly or indirectly assisted me in completing this thesis entitled "Artificial Intelligence-Driven Cyber Crimes and the Emerging Legal Challenges: A Study in the Context of USA, Singapore and Bangladesh."

Thank You

DECLARATION

I, All Imran Shaad,hereby declare that this dissertation is entitled “Artificial Intelligence-Driven Cyber Crimes and the Emerging Legal Challenges: A Study in the Context of USA, Singapore and Bangladesh” is an original piece of work composed entirely and solely by me under the supervision of Shah Maruf Uddin Ahmed(Lecturer), East West University for submission to the Department of Law, East West University for completion of the degree of Bachelor of Laws and that is has not been submitted, in whole or in part in any previous application for any degree anywhere. Except where stated otherwise by reference or acknowledgement, the study presented is entirely my own.

All Imran Shaad

ID:2021-1-66-036

Department of Law

East West University

ABSTRACT

Artificial Intelligence (AI) has significantly transformed the digital landscape, offering numerous benefits while simultaneously creating new opportunities for cybercriminal activities. AI-driven cybercrimes, such as phishing attacks, deepfake fraud, identity theft, and autonomous malware, pose serious challenges to existing legal and regulatory frameworks. This thesis examines the nature of AI-enabled cybercrimes and analyzes the legal and institutional responses of the United States, Singapore, and Bangladesh.

Using a doctrinal and comparative legal research methodology, the study evaluates the effectiveness of relevant cybercrime laws, enforcement mechanisms, and regulatory frameworks in these jurisdictions. The findings indicate that while the United States and Singapore have developed relatively advanced legal and institutional responses, significant challenges remain regarding attribution, evidence, and cross-border enforcement. Bangladesh, on the other hand, faces substantial legislative and institutional gaps in addressing AI-driven cyber threats.

The thesis recommends legal reforms, specialized enforcement mechanisms, enhanced digital forensic capabilities, and stronger international cooperation to strengthen Bangladesh's preparedness against emerging AI-related cybercrimes. It concludes that a comprehensive and adaptive legal framework, supported by institutional capacity-building, is essential for effectively combating AI-driven cybercrime in the future.

LIST OF ABBREVIATIONS

AI	Artificial Intelligence
ARIMA	AutoRegressive Integrated Moving Average
ASEAN	Association of Southeast Asian Nations
ASCom	Anti-Scam Command
BIISS	Bangladesh Institute of International and Strategic Studies
BTRC	Bangladesh Telecommunication Regulatory Commission
CCIPS	Computer Crime and Intellectual Property Section
CFAA	Computer Fraud and Abuse Act
CISA	Cybersecurity and Infrastructure Security Agency
CII	Critical Information Infrastructure

Table of Contents

CHAPTER 1

Introduction

Background and Justification of the Study

Artificial intelligence (AI) has revolutionised the world‘s digital environment. It has revolutionised large scale data processing, enabling automated decision- making and more autonomous systems in sectors such as public administration, finance and health. But now it is also enabling a new wave of cybercrimes. Compared to traditional methods, these are more fine-tuned, scalable and less detectable. Motivation can be facilitated by automating phishing, deep fake content generation, AV improvement and real time modulation of methods using generative AI and machine learning. This increases the potential impact of each attack and reduces the barriers to entry for cybercrime groups. Much existing legislation was developed in response to traditional, human directed cybercrimes. As such, it struggles to address some of the key challenges of AI-enabled attacks. Such as attribution when systems act independently, apportioning responsibility to developer, user and deployer and difficulties in demonstrating how opaque algorithms operate and their purpose in court.[1]

In the US, most AI-powered cyberattacks are prosecuted tangentially, by means of federal legislation such as the Computer Fraud and Abuse Act (CFAA), along with regulation issued at the sectoral level. While the CFAA prohibits unauthorised access, damage or interference with data, and fraud, it does not guarantee AI-inspired approaches. Thus, identification of the responsible party remains unclear.

This research is justified for a number of reasons. While growing literature covers the topics of AI and cyber crime more generally, there exist only a few studies undertaking a detailed, multi-jurisdictional exploration of cyber crimes involving AI that compares the sort of more developed and less developed legal regimes used to address them especially in the USA, Singapore and

[1](R. Arjuna Rao1)

Bangladesh. Current studies focus on either the USA and the European Union, or theoretical discussions of whether AI can or should be held liable, without investigating in any depth how more specific cyber laws, enforcement practices, and institutional resources interact with AI-driven threats in Asian and Global South jurisdictions. Second, extending the comparison to include Bangladesh as well as the USA and Singapore highlights a glaring phenomenon: how less developed cyber laws and weaker forensic resources in burgeoning economic states may confront more sophisticated AI-driven cyber crimes that are often international in scope and involve external middlemen or infrastructure. It also highlights that cases of AI-enabled scams, impersonation, and business email compromise happening in Southeast Asia and elsewhere already cause substantial financial and social damage, yet the policy remedies are disparate, ad hoc, and substantially behind the pace of technological change.[2]

This thesis intends to reveal, by analysis of the respective legal and institutional frameworks of the USA, Singapore and Bangladesh, where the current gaps are in cybercrime attributions, evidentiary rules, jurisdictional reach and international cooperation for enforcement. It will also put forward contextualized recommendations which attempt to extend beyond mere application of existing cybercrime paradigms to new cybercrimes enabled by emerging AI technologies. With a focus on enabling responsible innovation and safeguarding fundamental rights, the aim of this research is to further a particularised comparative perspective that will assist not only legislators but also regulators and law enforcement agencies in reforming cybercrime laws, creating prosecutorial guidance and enhancing extraterritorial cooperation and technical capabilities, especially in Bangladesh, to effectively address, investigate and prosecute, while supporting innovation in, new cybercrimes driven by AI technology.[3]

Research Objective

The research objective of this thesis 1s to conduct a comparative analysis of the legal frameworks of the USA, Singapore, and Bangladesh with relation to AI enabled cyber crimes,

[2] (Krishnamani, 2025-08-25)

[3] (Karryl Kim Sagun Trajano, 26 January 2026)

and find out what lessons or best practices, Bangladesh can adopt from the other two countries' laws to formulate stronger legal and institutional response mechanisms for cyber threats in future.

- To research the different types of AI based cyber Crimes and how they affect the countries USA, Singapore and Bangladesh.
- Review the current cybercrime and digital security laws, enforcement agencies, as well as institutional framework of these three countries.
- Determine the extent to which and how Bangladesh may need to implement similar measures and learn from best practices, including clearer legal categorization of crimes related to AI, cyber crime capacity building in the form of dedicated cyber crime units, developing public private partnership and strengthening digital forensics capacity.
- Recommender specific, practical and forward-looking actions that Bangladesh can undertake to prevent, detect, investigate and prosecute AI related cyber crime including legislative reforms, capacity development for police and judiciary, and participation in regional and international cooperation on cyber security.

Research Qustions

1: How do the legal frameworks of the USA, Singapore, and Bangladesh address the unique attribution, evidentiary, and enforcement challenges posed by AI-driven cyber crimes, and what comparative gaps reveal opportunities for harmonized policy reforms?

2: How do the legal and institutional responses to artificial intelligence-driven cyber crimes in the USA, Singapore, and Bangladesh differ, and what lessons can Bangladesh draw from the USA and Singapore to strengthen its preparedness for future AI-enabled cyber threats?

The specific objectives are:

1. How do judicial doctrines and statutory provisions in these jurisdictions handle the technical and ethical hurdles of prosecuting AI-autonomous cyber crimes, including AI-Powered Phishing Scams, Automated Hacking and deepfake-generated fraud?

2. What legal mechanisms are adopted in the United States and Singapore to regulate AI-driven cybercrimes, and how can these mechanisms inform the development of an effective legal framework in Bangladesh?

Research Methodology

This research looks at AI crimes in the cyber field in Bangladesh, Singapore, and the US from a doctrinal and comparative law perspective. Besides relevant case law on attribution, evidentiary issues with black boxed algorithms, and enforcement in AI crimes like phishing, deepfakes, and robo-hacking, primary sources are CFAA (US), Computer Misuse Act (Singapore), and the Cyber Security Act 2023 (Bangladesh). Journals (e.g., on AI liability), policy papers (e.g., from BIISS on AI threats to Bangladesh, and UNICRI and Europol on malicious AI), white papers (e.g., SGS on AI and cyber security), and analysis by the OECD and ITU are secondary sources. Data comes from legal databases and repositories. I will conduct doctrinal explanation, cross-jurisdictional best practices comparisons, and analyse the unique steps taken in Bangladesh like police and computer crime units using model modules from the US and Singapore. Lack of local decisions means focus on post-2023, until March 2026, with the topic limited to international parallels and human rights considerations.[4]

Literature Review

A review of previous theses and scholarly research on AI-driven cybercrime and associated legal issues reveals that while researchers have started to acknowledge the dangers of AI in cyberspace, many significant issues have not yet received enough attention. Without carrying out a thorough doctrinal and comparative legal analysis, the majority of earlier studies either concentrate on conventional cybercrime frameworks or theoretical discussions of artificial intelligence. Because of this, there are a lot of gaps in the literature, which this study attempts to

[4] (Haque, April 10,2025)

fill by comparing several jurisdictions in an organised manner and concentrating on legal issues pertaining to Artificial Intelligence.

Although existing literature, such as Shetty et al. (2024) and Jampani (2025), extensively documents global trends and technical risks (such as deepfakes and AI-phishing), it lacks multi-jurisdictional comparisons involving developing countries like Bangladesh. In emerging economies, where Cyber Security Act 2023 enforcement lags despite an increase in AI scams, few studies look at prosecutorial practices or institutional forensics limitations.[5]

AI defences and forecasting models (such as ARIMA-LSTM at 99.9% accuracy) from a USA/EU perspective are highlighted in Godwin (2024) and EEI reviews (2025), ignoring adaptation challenges for Singapore's CMA or Bangladesh's due process issues. There are no empirical cases from your jurisdictions, and attribution gaps—proving intent in autonomous AI attacks—remain understudied in non-Western courts.[6]

Jiow (2023) updates Singapore regulations but neglects international enforcement cooperation, which is a crucial gap considering the global nature of AI threats. In the absence of policy changes adapted to the capabilities of the Global South, recent reports from 2026 show defence lags (76% organisations struggling vs. 7% with AI tools).[7]

One source that engages with some questions similar to those raised in this paper is **Md. Nur Nabi (2022), "Cyber Law Challenges: Bangladesh, India, UK" (Port City International University LL. B Thesis).** Thereis existing research on cyber law problems faced by the USA and Singapore. While the study offers an excellent overview of cybercrime laws and identifies gaps in enforcement and legislative cooperation, it was initiated well before the recent explosion of AI-facilitated cyber threats. It therefore largely concentrates on normal cyber crimes like hacking, cyber trafficking, and data breaches. It overlooks the more sophisticated AI developments of a high degree of autonomous malware, the use of deepfakes for fraud, and human drivers for machine-like cyberattacks. Furthermore, it fails to examine the USA and Singapore, which are relatively technology-savvy legal regimes with mature regulatory systems

[5] (Shetty, 2024)

[6] (Stephen, 2025)

[7] (https://www.weforum.org/publications/global-cybersecurity-outlook-2026/in-full/3-the-trends-reshaping-cybersecurity/, 2026)

– an omission that deprives the study of insights for the far more innovative and still-evolving context of Bangladesh governmentmechanisms. Old research is now outdated given soaring AI-enabled cybercrimes; misses any focus on enforcement potency or post-2023 legislation like Bangladesh' CSO 2025overlooking issues of algorithmic autonomy, deepfake use as evidence, and evolving auth-inducible phishing.[8]

Rasyid (2024), "Cybercrime Threats and Responsibilities: Use of AI in Online Crime" (Jurnal Ilmiah MIZANI). This thesis employs normative analysis to address the issue of AIs in cybercrimes by stressuing the importance of international cooperation and type-specific legislation to cope with detection/process issues. While it identifies gaps in regulation it does not contrast the jurisdictions, concentrating on the lack of regulating options per se. Instead, it discusses general weakspots with no doctrinal designation as to the USA, UK, Singapore and Bangladesh.[9]

Scope and Limitation

This thesis on the three jurisdictions takes a closer look at the implications of these AI-enabled offenses for institutions and laws, such as the implications of AI-generated phishing or deepfake-based fraud for the law of evidence and liability, or the effects of AI-assisted malware on the jurisdiction's computer crime statutes.[10]

The inclusion of the UK is due to its well-known "common"-law tradition and the development of cybercrime laws including the Computer Misuse Act 1990 and wider institutional arrangements like digital security frameworks; and exemplifies how such democracies treat innovative cyber threats including those offered by AI tools. S.a.pore is selected as a small state with high tech embedment and a relatively strict yet enabling cyber regime including the Computer Misuse Act and wider cybersecurity governance.-showcasing how such a small highly

[8] (Nabi, n.d.)
[9] (Rasyid)
[10] (https://pmc.ncbi.nlm.nih.gov/articles/PMC8862401/, n.d.)

digitalised area deals with new (AI-)related cyber risks and promotes public-private partnership. Bangladesh is selected because as a fast developing digitally (and Internet-wise) country with rising number of e-services, it suffers from institutional and development setbacks and/or the capacities of its cyber legislations and regulatory institutions; it is hence an interesting case for learning and adjustment.[11]

Limitation

- The study is mostly based on existing documents, such as statutes, case law, policy papers, and secondary literature. Therefore, it might not completely reflect the real investigative practices or operational issues in each jurisdiction.
- Because the analysis is restricted to the three chosen nations, its findings cannot be applied to all Asian or Anglocommon law systems without additional empirical research.
- The findings will be limited to the years up to 2026 because of the rapid advancement of technology, which may cause some AI-driven attack vectors and new regulatory responses to change more quickly than the thesis can account for.
- The thesis concentrates on the legal and governance aspects of AI-driven cybercrime rather than offering specific technical cybersecurity solutions.

Chapter Outline

This thesis is divided into seven chapters:

1. The chapter one is Introduction which will compile with the research background, Objective, research questions, research methodology, scope and limitations, and literature review.
2. Chapter two is AI-Driven Cybercrimes in the USA – Challenges, Laws, and Regulations.
3. Chapter three is AI-Driven Cybercrimes in Singapore-Challenges, Laws, and Regulations.
4. Chapter four is Recommendations and Reforms for Bangladesh.

[11] (https://iclg.com/practice-areas/cybersecurity-laws-and-regulations/singapore, n.d.)

5. Lastly Chapter five is Findings, Recommendations and Conclusion.

CHAPTER TWO

AI-DRIVEN CYBERCRIMES IN THE USA: CHALLENGES, LAWS, AND REGULATIONS

2.1 Introduction

The United States is at the nexus of AI progress and the legal difficulties that come with its unlawful exploitation. Generative AI and machine learning have been exploited by hackers to perform sophisticated phishing at scale, generate realistic deepfake media, and install adaptive malware that evades traditional defences in real time. Both the FBI's Internet Crime Complaint Centre (IC3) and the Federal Trade Commission (FTC) have reported record fraud losses from AI-enhanced attacks in 2023–2025. In this chapter, we explore US legal, institutional, and regulatory responses to AI-enabled cybercrime. It also covers the main statutory framework, important regulatory instruments, the enforcement architecture and recurring inadequacies – before drawing comparative lessons relevant for Bangladesh.

2.2 Types of AI-Enabled Cyber Offenses in the USA

2.2.1 AI-Powered Phishing and Social Engineering

Natural language processing models have changed traditional phishing programmes such as WormGPT and FraudGPT leverage acquired social media and professional data to automate the production of highly personalised, contextually correct lures. These AI-generated messages are mostly indistinguishable from authentic contact, and substantially reduce the technical bar to mass targeted fraud. Legally, such offences are prosecuted under wire fraud and the Computer Fraud

and Abuse Act (CFAA) § 1030(a)(4). The key difficulty lies in establishing mens rea when an AI system functions autonomously, beyond the direct control of the deployer.[12]

2.2.2 Deepfake-Based Fraud and Identity Crimes

AI-synthesised audio-visual media has been weaponised for corporate impersonation, non-consensual personal imagery and political misinformation. There's no sweeping federal deepfake law, and prosecutors have to depend on a patchwork of wire fraud, identity theft and cyberstalking statutes. The DEFIANCE Act (2024) established a civil cause of action for nonconsensual deepfake intimate imagery, but broader ideas like the NO FAKES Act had not been implemented by the beginning of 2026. The authentication of AI-generated digital evidence under Federal Rule of Evidence 901 and the Daubert standard for scientific evidence is disputed in US courts.[13]

2.2.3 Autonomous Malware and AI-Assisted Intrusion

AI-augmented malware can modify its own code to avoid detection, and find paths via the network by doing real-time analysis behaviours that are fundamentally different than typical static-signature harmful code. CFAA Section 1030(a)(5) outlaws purposeful harm to computer systems, yet the 'intentionality' threshold was written for human actors. In case of damage caused by an autonomous AI agent, the legal nexus between the human deployer and the concrete harm is legally elusive.[14]

---

[12] T Krishnamani, 'Legal Challenges in Regulating AI-Powered Hacking, Phishing, and Identity Theft' (2025) 23(S4).

[13] Federal Rules of Evidence, r 901; Daubert v Merrell Dow Pharmaceuticals Inc 509 US 579 (1993).

[14] RA Rao and D Osei, 'Artificial Intelligence (AI) and Cybersecurity Law: Legal Issues in AI-Driven Cyber Defense and Offense' (n.d.).

2.3 Legal and Regulatory Framework

2.3.1 The Computer Fraud and Abuse Act (CFAA)

The CFAA (1986, as amended) is the primary federal cybercrime statute.[15] Its primary sections concern unauthorised access, computer-facilitated fraud, malicious harm and extortionate threats. The main hurdle for AI-based offences is conceptual. The Act presumes a human author with recognisable purpose. The Supreme Court's narrow finding in Van Buren v United States (2021) constrains the 'exceeds authorised access' criteria, which may mean that AI attacks using credentials that were properly obtained are not covered by the Act.[16]

3.3.2 Sector-Specific Regulation and Executive Governance

Sector-specific frameworks HIPAA for healthcare,[17] the Gramm-Leach-Bliley Act for financial services,[18] and the SEC's 2023 cybersecurity incident disclosure rules impose breach-related obligations that extend to AI-enabled attacks.[19] Executive Order 14110 (October 2023) directed NIST to develop AI safety guidelines, required frontier AI developers to share test results with the government, and tasked DHS with assessing AI risks to critical infrastructure.[20] The voluntary NIST AI Risk Management Framework (2023), while non-binding, is increasingly referenced as

[15] CFAA (n 2) § 1030.

[16] Van Buren v United States 593 US 374 (2021).

[17] Health Insurance Portability and Accountability Act 1996 (US) (HIPAA).

[18] Gramm-Leach-Bliley Act 1999 (US).

[19] Securities and Exchange Commission, 'Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure' (2023).

[20] Executive Order 14110 on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence (30 October 2023).

a standard of care in civil litigation.[21] Following the change of administration in January 2025, EO 14110 was revoked, though core operational programmes under NIST and DHS continued into 2026.

2.5 Persistent Gaps

Five structural gaps constrain the effectiveness of the US framework. First, the CFAA's legislative obsolescence: nearly four decades old, it was not designed for autonomous AI actors, and repeated congressional attempts at comprehensive AI-specific cybercrime legislation have stalled. Second, the attribution deficit: AI tools obscure the causal chain between human perpetrators and harmful outcomes, complicating prosecution beyond reasonable doubt. Third, the deepfake patchwork: inconsistent state laws and the absence of a federal statute produce uneven deterrence and jurisdictional gaps. Fourth, international enforcement constraints: the Budapest Convention and bilateral MLATs predate AI-enabled transnational attack vectors and lack the technical specificity required for modern attribution and evidence collection.[22] Fifth, the government-industry capacity gap: federal agencies depend on private forensic firms for AI-attack investigation, creating accountability and equity concerns.

2.6 Conclusion

The United States offers a model of institutional depth a specialised enforcement apparatus, active public-private partnerships, and a government increasingly conscious of AI-specific risk. Yet its legal architecture, anchored in a pre-AI statute and characterised by fragmented deepfake regulation and unresolved evidentiary standards, demonstrates that institutional capacity and legislative adequacy are not the same thing. The core lesson for Bangladesh is twofold: the value of dedicated cyber enforcement units and structured industry collaboration is clear and replicable;

[21] National Institute of Standards and Technology, AI Risk Management Framework (AI RMF 1.0) (US Department of Commerce 2023).

[22] Convention on Cybercrime (Budapest Convention) (Council of Europe, ETS 185, 2001).

but technology-neutral legislative drafting, absent regular revision, becomes rapidly inadequate. Bangladesh must also note that the US, with far greater resources, still struggles with attribution in AI-mediated attacks a problem that will be exponentially more acute with Bangladesh's current forensic capacity.

CHAPTER THREE

AI-DRIVEN CYBERCRIMES IN SINGAPORE: CHALLENGES, LAWS, AND REGULATIONS

3.1 Introduction

Singapore has established itself as one of Asia's most digitally advanced economies, with an internet penetration rate exceeding 90% and a government-led Smart Nation initiative that has systematically embedded artificial intelligence (AI) across public administration, financial services, and healthcare.[23] This digital sophistication, however, has simultaneously expanded Singapore's exposure to AI-driven cybercrimes, as threat actors exploit the same technologies that underpin the country's digital transformation. From AI-powered phishing campaigns and deepfake-enabled fraud to autonomous intrusion tools, the threat landscape has evolved significantly beyond what Singapore's foundational cybercrime legislation was originally designed to address.[24] The Singapore Police Force (SPF) reported that scam-related losses reached SGD 651.8 million in 2023 a 16.3% increase from the previous year with a growing proportion involving AI-generated impersonation and automated social engineering.[25] This chapter examines the nature and scale of AI-driven cyber threats in Singapore, evaluates the existing legal framework primarily the Computer Misuse Act (CMA) and the Cybersecurity Act 2018 and identifies persistent institutional and legal gaps that challenge effective enforcement and prosecution, before drawing comparative lessons relevant to Bangladesh.

---

[23] Infocomm Media Development Authority (IMDA), 'Digital Economy Framework for Action' (IMDA, Singapore, 2018) <https://www.imda.gov.sg/how-we-can-help/digital-economy-framework> accessed 1 June 2026; Smart Nation Singapore, 'Smart Nation: The Way Forward' (Prime Minister's Office, 2018) <https://www.smartnation.gov.sg> accessed 1 June 2026.

[24] Jiow Hee Jhee, 'A Critical Analysis of Singapore's Cybercrime Legislation' (2023) 35 *International Journal of Law and Information Technology* 89, 91–93 <https://doi.org/10.1093/ijlit/eaad002> accessed 1 June 2026.

[25] Singapore Police Force, *Annual Scams and Cybercrime Brief 2023* (SPF, 2024) <https://www.police.gov.sg/media-room/statistics> accessed 1 June 2026.

3.2 Types of AI-Enabled Cyber Offences in Singapore

3.2.1 AI-Powered Phishing and Business Email Compromise

Natural language processing models have changed the game for traditional phishing programmes like WormGPT and FraudGPT, using social media and professional data they have learned to automatically generate highly personalised, contextually relevant lures. These AI generated messages are largely indistinguishable from real contact and significantly reduce the technical barrier for mass targeted fraud. These offences are legally actionable under wire fraud and under the Computer Fraud and Abuse Act (CFAA) § 1030(a)(4). The key issue is how to establish criminal intent when the AI system operates autonomously without any control by the deployer.[26]

3.2.2 Deepfake-Based Fraud and Identity Crimes

AI-synthesised audio-visual media has been weaponised for corporate impersonation, non-consensual personal images and political misinformation. There is no comprehensive federal deepfake law and prosecutors have to use a patchwork of wire fraud, identity theft and cyberstalking laws. By the beginning of 2026, the DEFIANCE Act (2024) had created a civil cause of action for nonconsensual deepfake intimate imagery, but broader ideas, such as the NO FAKES Act, had not been put into place. In the US courts, there is a debate about the authentication of digital evidence created by AI using Federal Rule of Evidence 901 and the Daubert standard for scientific evidence.[27]

---

[26] Computer Misuse Act (Cap 50A, 2007 Rev Ed, Singapore) ('CMA'), ss 3–8; Jiow (n 27) 95–101.

[27] Penal Code 1871 (Cap 224, 2008 Rev Ed, Singapore), ss 415–420 (cheating), s 419 (impersonation). See also S Seetharaman, 'Deepfakes and the Limits of Singapore's Criminal Law' (2024) 36 *Singapore Academy of Law Journal* 180, 185–189.

3.2.3 Autonomous Malware and AI-Assisted Intrusion

AI augmented malware can rewrite its own code to evade detection and can discover paths through the network via real-time analysis, behaviours that are radically different from typical static-signature malicious code. The CFAA, at Section 1030(a)(5), criminalises intentional damage to computers, but the bar of "intent" was written for humans. In the case of a damage caused by an autonomous AI agent, the legal nexus between the human deployer and the concrete harm is legally elusive.[28]

3.3 Legal and Regulatory Framework

3.3.1 The Computer Misuse Act (Cap 50A)

The primary federal statute addressing cybercrime is the CFAA (1986, as amended). Its main parts deal with unauthorised access, fraud committed through the use of computers, malicious damage and extortionate threats.The Supreme Court's narrow ruling in Van Buren v United States (2021) restricts the 'exceeds authorised access' criteria, potentially meaning that AI attacks using credentials that were properly obtained are not covered by the Act.[29]

3.3.2 The Cybersecurity Act 2018

HIPAA for healthcare, the Gramm-Leach-Bliley Act for financial services, and the SEC's 2023 cybersecurity incident disclosure rules are examples of sector-specific frameworks that contain breach-related obligations that also apply to AI-enabled attacks. Executive Order 14110 (October 2023) tasked NIST with developing AI safety standards, required frontier AI developers to share

[28]CMA (n 31) s 5; RA Rao and D Osei, 'Artificial Intelligence (AI) and Cybersecurity Law: Legal Issues in AI-Driven Cyber Defense and Offense' (n.d.) <https://ssrn.com/abstract=4452900> accessed 1 June 2026.

[29]Rao and Osei (n 38); Krishnamani (n 29).

test results with the government, and tasked DHS with assessing AI threats to critical infrastructure. The voluntary NIST AI Risk Management Framework (2023) is non-binding but is increasingly cited as a standard of care in civil litigation. The order, EO 14110, was rescinded after the change of administration in January 2025, but core operational programmes run by NIST and DHS continued through 2026.[30]

3.3.3 Ancillary Legislation and Institutional Mechanisms

HIPAA for healthcare, the Gramm-Leach-Bliley Act for financial services, and the SEC's 2023 cybersecurity incident disclosure rules are examples of sector-specific frameworks that contain breach-related obligations that also apply to AI-enabled attacks. Executive Order 14110 (October 2023) tasked NIST with developing AI safety standards, required frontier AI developers to share test results with the government, and tasked DHS with assessing AI threats to critical infrastructure. The voluntary NIST AI Risk Management Framework (2023) is non-binding but is increasingly cited as a standard of care in civil litigation. The order, EO 14110, was rescinded after the change of administration in January 2025, but core operational programmes run by NIST and DHS continued through 2026..[31]

3.4 Persistent Gaps

Despite Singapore's relatively sophisticated legal and institutional architecture, five structural gaps constrain the effectiveness of its response to AI-driven cybercrime. First, the CMA's *mens rea* deficit: the Act was not designed for autonomous AI actors, and the absence of statutory provisions addressing AI-specific attribution renders prosecution of fully automated attacks legally

[30] ICLG, 'Cybersecurity Laws and Regulations: Singapore' (2024) <https://iclg.com/practice-areas/cybersecurity-laws-and-regulations/singapore> accessed 1 June 2026.

[31] World Economic Forum, *Global Cybersecurity Outlook 2026* (WEF, 2026) <https://www.weforum.org/publications/global-cybersecurity-outlook-2026> accessed 1 June 2026.

uncertain.[32] Second, the deepfake legislative vacuum: Singapore lacks a dedicated statute criminalising deepfake-enabled fraud or non-consensual synthetic intimate imagery, forcing prosecutors to rely on general provisions in the Penal Code that were not designed with AI-generated content in mind.[33] Third, algorithmic opacity in evidentiary proceedings: where AI systems function as black boxes, explaining their operational logic to a court in conformity with Singapore's Evidence Act standards for admissibility remains technically and legally challenging.[34] Fourth, international enforcement constraints: while Singapore participates in Mutual Legal Assistance Treaty (MLAT) arrangements and the ASEAN Senior Officials Meeting on Transnational Crime (SOMTC), these mechanisms are ill-adapted to the pace of AI-driven transboundary cyber incidents.[35] Fifth, the absence of binding AI-specific legislation: Singapore's Model AI Governance Framework (2020) and its updated 2023 iteration are advisory rather than binding, leaving a gap between best-practice guidance and enforceable legal obligations for AI system developers and deployers.[36]

3.6 Conclusion

Singapore's legal and institutional framework for addressing AI-driven cybercrime represents one of the most advanced in the Asia-Pacific region, combining a regularly updated primary cybercrime statute, a proactive critical infrastructure protection regime, and dedicated enforcement institutions with specialist AI forensics capabilities.[37] Yet persistent gaps remain: the CMA's *mens*

---

[32] Jiow (n 27) 99–101; Rao and Osei (n 38).

[33] Seetharaman (n 35) 185–189.

[34] Evidence Act (Cap 97) (n 34), ss 35–36.

[35] Convention on Cybercrime (Budapest Convention) (Council of Europe, ETS 185, 2001) <https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185> accessed 1 June 2026; ASEAN, 'Senior Officials Meeting on Transnational Crime (SOMTC)' <https://asean.org/our-communities/asean-political-security-community/crime/asean-senior-officials-meeting-on-transnational-crime-somtc/> accessed 1 June 2026.

[36] Personal Data Protection Commission (Singapore), *Model AI Governance Framework* (2nd edn, PDPC, 2020) <https://www.pdpc.gov.sg/help-and-resources/2020/01/model-ai-governance-framework> accessed 1 June 2026.

[37] Cyber Security Agency of Singapore (n 30); Cybersecurity Act 2018 (n 44).

rea architecture was not designed for autonomous AI actors; a deepfake-specific legislative framework is absent; evidentiary standards for AI-generated content are unsettled; and international enforcement cooperation mechanisms remain too slow for the pace of AI-driven transboundary crime.[38] These limitations demonstrate that institutional capacity and legislative adequacy are not synonymous a finding that directly parallels the conclusions drawn in Chapter Three regarding the United States. For Bangladesh, the Singapore model offers both an aspirational benchmark and a cautionary lesson: technical and institutional investment must be matched by coherent legislative reform that addresses the attribution, evidentiary, and jurisdictional challenges specific to AI-enabled cybercrime.[39]

[38] Jiow (n 27) 99–104; Seetharaman (n 35) 185–189.

[39] Haque (n 58); Krishnamani (n 29).

CHAPTER FOUR

RECOMMENDATIONS AND REFORMS FOR BANGLADESH

4.1 Introduction

Sector-specific frameworks with breach-related obligations that would also apply to AI-enabled attacks include HIPAA in healthcare, the Gramm-Leach-Bliley Act in financial services and the SEC's 2023 cybersecurity incident disclosure rules. * Executive Order 14110 (October 2023) directed NIST to develop AI safety standards, required frontier AI developers to share test results with the government, and directed DHS to assess AI threats to critical infrastructure. The non-binding voluntary NIST AI Risk Management Framework (2023) is being used more and more as a standard of care in civil litigation. The order, EO 14110, was rescinded with the change of administration in January 2025, but core operational programmes run by NIST and DHS continued through 2026.[40] This chapter presents a set of targeted recommendations for Bangladesh, drawing from comparative best practices from the USA and Singapore, to develop a coherent and forward-looking legal and institutional response to AI-driven cyber threats.

The reform agenda presented in this report is organised around five pillars: (i) legislative modernisation; (ii) institutional capacity building; (iii) digital forensics and evidentiary reform; (iv) public-private partnerships; and (v) regional and international cooperation. Each pillar is backed by concrete lessons from USA and Singapore, contextualised in the developmental and institutional realities of Bangladesh.[41]

[40]Digital Security Act 2018 (Bangladesh); Cyber Security Act 2023 (Bangladesh); Information and Communication Technology Act 2006 (Bangladesh).

[41]Haque MM, 'AI in the Crosshairs: An Assessment of AI-Based Cybersecurity Threats in Bangladesh' (BIISS, 10 April 2025).

4.2 Legislative Modernisation: Learning from the USA and Singapore

4.2.1 Reforming the Cyber Security Act 2023

The reform agenda presented in this report is organised around five pillars: (i) legislative modernisation; (ii) institutional capacity building; (iii) digital forensics and evidentiary reform; (iv) public-private partnerships; and (v) regional and international cooperation. Each pillar is backed by concrete lessons from USA and Singapore, contextualised in the developmental and institutional realities of Bangladesh.[42] This legislative lacuna stands in sharp contrast to the United States, where the Computer Fraud and Abuse Act 1986, supplemented by the Cybersecurity Information Sharing Act 2015 and the AI Executive Order 2021, provides a layered statutory regime albeit itself imperfect that at least contemplates technological evolution.[43]

Bangladesh should have dedicated AI cybercrime provisions in the Cyber Security Act 2023 or pass a separate Artificial Intelligence Governance Act. Such provisions should: first, specify the types of AI-enabled cybercrimes, including autonomous phishing, deepfake-facilitated fraud, and machine-learning-assisted intrusion; second, hold developers, deployers, and users of AI systems used in cybercrimes to vicarious and strict liability standards; and third, codify algorithmic transparency requirements that mandate auditability of AI systems in critical sectors.[44]

---

[43]Computer Fraud and Abuse Act 1986 (US) 18 USC §1030; Cybersecurity Information Sharing Act 2015 (US) Pub L 114-113; Executive Order 14028 on Improving the Nation's Cybersecurity (2021).

[44]Krishnamani T, 'Legal Challenges in Regulating AI-Powered Hacking, Phishing, and Identity Theft' (2025) 23(S4) Journal of Law and Technology 136; R Arjuna Rao and others, 'Artificial Intelligence (AI) and Cybersecurity Law: Legal Issues in AI-Driven Cyber Defense and Offense' (2024) 136.

4.2.2 Adopting Singapore's Graduated Offence Structure

Singapore's Computer Misuse Act, as amended in 2017, adopts a graduated offence structure whereby the severity of criminal liability escalates according to the harm caused and the degree of automation involved.[45] Unauthorised access, data interference, and attacks on critical information infrastructure each attract distinct penalties. This structure is notably absent from Bangladesh's framework, which conflates a wide range of offences under broadly worded provisions, generating inconsistency in prosecution.[46]

Bangladesh should consider the graduated Singapore model for restructuring its cybercrime offences. We propose a three tier classification, Tier One offences being for basic unauthorised access, Tier Two for data manipulation and AI-assisted intrusion and Tier Three for AI-generated attacks on critical national infrastructure. Custodial sentences should be mandatory. This sort of stratification would allow courts to calibrate punishment proportionately and give prosecutors clearer guidelines.[47]

[45]Computer Misuse Act (Cap 50A, Singapore) as amended by the Computer Misuse (Amendment) Act 2017; Cybersecurity Act 2018 (Singapore); Personal Data Protection Act 2012 (Singapore).

[46]Md Nur Nabi, 'Cyber Law Challenges: Bangladesh, India, UK' (LLB Thesis, Port City International University 2022).

[47]ICLG, 'Cybersecurity Laws and Regulations: Singapore' (ICLG, 2024) <https://iclg.com/practice-areas/cybersecurity-laws-and-regulations/singapore> accessed 10 June 2026.

4.3 Institutional Capacity Building

4.3.1 Establishing a Dedicated AI Cybercrime Unit

One of the institutional challenges of Bangladesh is the absence of a dedicated, technically skilled cybercrime unit to investigate AI-enabled crimes. The present Cyber Crime Investigation Division, Bangladesh Police is operationally active but does not have specialised AI forensics expertise and is understaffed vis-a-vis the scale of AI-enabled threats.[48]

The United States offers an instructive model through the Federal Bureau of Investigation's Cyber Division and the Department of Justice's Computer Crime and Intellectual Property Section (CCIPS), which deploy both legal and technical specialists in AI-related investigations.[49].The present Cyber Crime Investigation Division, Bangladesh Police is operationally active but does not have specialised AI forensics expertise and is understaffed vis-a-vis the scale of AI-enabled threats..[50]

Bangladesh needs to create an AI Cybercrime Investigation Bureau under the Ministry of Home Affairs with interdisciplinary teams of criminal lawyers, digital forensic experts and data scientists. In tandem, the Bangladesh Telecommunication Regulatory Commission needs to be empowered with a specific AI oversight mandate akin to the CSA's regulatory role in Singapore.[51]

---

[50]Cybersecurity Agency of Singapore, 'Singapore Cyber Landscape 2023' (CSA, 2024) <https://www.csa.gov.sg> accessed 10 June 2026.

[51]Karryl Kim Sagun Trajano B, 'Science, Technology and Security: AI and Crime' (RSIS, 26 January 2026) <https://rsis.edu.sg/rsis-publication/rsis/science-technology-and-security-ai-and-crime-january-2026/> accessed 10 June 2026.

4.3.2 Judicial Training and Capacity Development

The judiciary's capacity to adjudicate AI-driven cybercrime is fundamental to enforcement. Bangladesh's courts currently lack both the technical literacy and procedural tools to evaluate algorithmic evidence, assess AI attribution claims, or apply emerging concepts such as "black box" liability.[52] The USA has addressed comparable challenges through judicial education programmes under the Federal Judicial Center, which provides specialised training on technology-related evidence.[53]

Bangladesh should introduce mandatory digital literacy and AI jurisprudence modules into the Bangladesh Judicial Service Commission's training curriculum. Specialist cyber benches should be established within the High Court Division, composed of judges trained in technology law, to handle complex AI cybercrime matters at appellate level.[54]

4.4 Digital Forensics and Evidentiary Reform

A major weakness in Bangladesh’s legal response to AI-driven cybercrimes is the absence of a robust digital forensics infrastructure and standards of admissibility for AI-generated evidence. Electronic evidence is recognised under the Evidence Act 1872 (as applicable in Bangladesh), but the Act provides no guidance on the admissibility of algorithmic outputs, deepfake analyses or AI-generated audit trails.[55]

---

[52]Rasyid, 'Cybercrime Threats and Responsibilities: The Utilization of Artificial Intelligence in Online Crime' (2024) Jurnal Ilmiah MIZANI.

[53]Stephen Godwin, 'AI-Driven Cybersecurity: Challenges and Legal Responses' (Theseus, 2025) <https://www.theseus.fi/bitstream/handle/10024/891045/Stephen_Godwin.pdf> accessed 10 June 2026.

[54]World Economic Forum, 'Global Cybersecurity Outlook 2026' (WEF, 12 January 2026) <https://www.weforum.org/publications/global-cybersecurity-outlook-2026> accessed 10 June 2026.

[55]Jabeen AZ, 'Camouflage of AI in Cyber Crimes Vis-à-Vis Legal Issues and Challenges' (2024).

A major weakness in Bangladesh's legal response to AI-driven cybercrimes is the absence of a robust digital forensics infrastructure and standards of admissibility for AI-generated evidence. Electronic evidence is recognised under the Evidence Act 1872 (as applicable in Bangladesh), but the Act provides no guidance on the admissibility of algorithmic outputs, deepfake analyses or AI-generated audit trails..[56] Singapore's Evidence Act similarly contains provisions for computer-generated evidence, with courts increasingly accepting AI forensic reports where the underlying methodology is disclosed and validated.[57]

Bangladesh needs to amend the Evidence Act to include specific provisions on AI-generated and algorithmic evidence. At minimum, the following reforms should be made: (1) a statutory definition of "AI evidence," including outputs from machine learning, deepfake detection reports, and logs of autonomous systems; (2) admissibility standards that require disclosure of the AI model's methodology, training data, and error rates; and (3) establishment of a national digital forensics laboratory under the Bangladesh Computer Council, patterned after Singapore's Centre of Excellence for National Security.[58]

4.6 Regional and International Cooperation

AI-driven cybercrimes are inherently transnational; perpetrators frequently operate across jurisdictions to exploit gaps in mutual legal assistance and extradition arrangements. Bangladesh currently lacks bilateral cybercrime-specific mutual legal assistance treaties (MLATs) with key

[58]National Institute of Standards and Technology, 'AI Risk Management Framework' (NIST, 2023) <https://www.nist.gov/artificial-intelligence> accessed 10 June 2026.

technology-exporting states, and is not a signatory to the Budapest Convention on Cybercrime the principal international instrument on cross-border cybercrime cooperation.[59]

Bangladesh should take steps to accede to the Budapest Convention as a matter of priority, as it would provide a multilateral framework for mutual assistance in the collection and sharing of electronic evidence in AI cybercrime investigations. Bilaterally, Bangladesh should negotiate AI cybercrime cooperation agreements with Singapore and the USA. At the regional level, Bangladesh should advocate within the SAARC and BIMSTEC frameworks for an AI and cybercrime cooperation protocol, drawing upon the operational model of ASEAN's cybersecurity cooperation framework.[60]

4.7 Conclusion

Bangladesh stands at a critical juncture. The exponential growth of AI-enabled cybercrimes from deepfake-based financial fraud to automated phishing campaigns demands an urgent, comprehensive, and institutionally grounded legal response.[61] The comparative analysis undertaken in this thesis demonstrates that, while no single jurisdiction has developed a perfect legal framework, the USA and Singapore offer Bangladesh a rich repository of legislative models, institutional designs, and cooperative mechanisms from which meaningful lessons can be drawn.[62]

The five-pillar reform agenda proposed in this chapter legislative modernisation, institutional capacity building, digital forensics reform, public-private partnerships, and international cooperation provides Bangladesh with a coherent and contextually adapted pathway toward a more effective legal and institutional response to AI-driven cybercrime. The urgency of these reforms cannot be overstated: without them, Bangladesh risks becoming both a target and an unwitting haven for AI-enabled cybercriminals operating at the global frontier of digital crime.[63]

Chapter Five

Findings, Recommendations and Conclusion

5.1 Introduction

This chapter consolidates the main findings of the comparative doctrinal analysis carried out in the previous chapters. The research has examined the legal, institutional and operational responses of the United States, Singapore and Bangladesh to the rapid proliferation of artificial intelligence (AI)-driven cyber crimes, including AI-powered phishing, automated hacking, deepfake-generated fraud, and autonomous malware deployment. In light of this comparative context, this chapter offers several targeted recommendations for improving, in particular, Bangladesh's legislative framework, its forensic capacity and its international cooperation posture. The chapter concludes with some reflections on the broader implications of this research for cybercrime governance in the Global South and the policy agenda that policymakers, regulators and law-enforcement agencies must urgently pursue.

5.2 Summary of Key Findings

5.2.1 The Nature and Scale of AI-Driven Cyber Crimes

The preceding chapters have chronicled a steady and increasing trend of AI-enabled cyber crime in the three jurisdictions considered. Chapter III found the US using generative AI techniques extensively to conduct spear-phishing attacks against financial institutions and healthcare providers, and to create autonomous malware variants that can avoid signature-based detection by dynamically mutating their code signatures. Chapter IV identified the misuse of deepfake synthesis

tools in Singapore to assume the identities of senior executives in business email compromise scams leading to multi-million dollar fraudulent wire transfers and AI-assisted credential-stuffing attacks targeting critical information infrastructure operators. As discussed in Chapter II and the institutional analysis in Chapter IV, Bangladesh has witnessed a sharp increase in AI-generated identity fraud targeting mobile financial services platforms, such as deepfake-assisted SIM-swap attacks against bKash and Nagad users, and automated phishing toolkits available on dark-web marketplaces that do not require technical expertise to deploy against Bangladeshi banking customers.[64]

As seen in the empirical data presented in previous chapters, there is a significant increase in the number and complexity of AI-powered attacks worldwide. Research shows AI-assisted phishing campaigns are achieving click-through rates far greater than those of manually crafted counterparts, while threat actors using predictive AI models can identify and exploit zero-day vulnerabilities faster than human defenders can.[65]

76% of organisations admit to struggling to keep up with AI-augmented threats, while only a tiny percentage have deployed equivalent AI-based defensive capabilities, according to the World Economic Forum's Global Cybersecurity Outlook 2026.[66]

5.2.2 The United States: A Mature but Fragmented Framework

Of the three jurisdictions studied, the United States has the most sophisticated legal infrastructure. Computer Fraud and Abuse Act (CFAA) and sectoral legislation such as the Health Insurance

[64]R. Arjuna Rao et al., "Artificial Intelligence (AI) and Cybersecurity Law: Legal Issues in AI-Driven Cyber Defense and Offense," 136. See also Krishnamani, T. (2025), "Legal Challenges in Regulating AI-Powered Hacking, Phishing, and Identity Theft," Vol. 23 No. S4.

[65]Shetty, S. (2024), International Journal of Cybersecurity Intelligence & Cybercrime, Vol. 7, Iss. 2, Art. 3. Available at: https://vc.bridgew.edu/ijcic/vol7/iss2/3/ (accessed 15 April 2026).

[66]Stephen, G. (2025), AI-Driven Cybersecurity Threats and Defences, Theseus Repository. Available at: https://www.theseus.fi/bitstream/handle/10024/891045/Stephen_Godwin.pdf (accessed 10 April 2026).

Portability and Accountability Act (HIPAA) and the Gramm-Leach-Bliley Act provide a broad statutory basis for prosecuting AI-enabled unauthorised access, data manipulation and fraud. Other signs of a desire to proactively govern AI include Presidential Executive Orders and the National Institute of Standards and Technology (NIST) AI Risk Management Framework.[67]

But the research shows big structural problems. The CFAA was written to address human-directed intrusions, and doesn't explicitly envision autonomous AI agents operating without human direction at every step. Questions of criminal attribution in domestic jurisprudence remain unresolved – is the liability with the developer, the deployer, the user or the AI system itself?[68]

This attribution deficit is compounded by evidentiary challenges. Courts have yet to develop settled doctrine on the admissibility of algorithmic audit trails, the weight to be given to AI-generated digital forensics, or the standards by which the opacity of deep learning models can be overcome in criminal proceedings. This patchwork of federal and state regulation further complicates consistent enforcement, as the lack of a unified federal AI and cybersecurity statute leads to fragmented prosecutorial strategies across jurisdictions.[69]

5.2.3 Singapore: A Coherent but Jurisdictionally Bounded Model

Singapore is a relatively coherent model of regulation. The Computer Misuse Act (CMA) as amended, together with the Cybersecurity Act 2018, provides a robust statutory framework for dealing with AI-enabled offences, including specific provisions targeting the misuse of automated tools. Legislative enforcement is coupled with public-private partnership and mandatory incident

[67]World Economic Forum, Global Cybersecurity Outlook 2026 (12 January 2026). Available at: https://www.weforum.org/publications/global-cybersecurity-outlook-2026 (accessed 20 April 2026).

[68]Karryl Kim Sagun Trajano and B. A., "Science, Technology and Security: AI and Crime" (RSIS Publication, 26 January 2026). Available at: https://rsis.edu.sg/rsis-publication/rsis/science-technology-and-security-ai-and-crime-january-2026/ (accessed 18 April 2026).

[69]Haque, M. M. (10 April 2025), "AI in the Crosshairs: An Assessment of AI-Based Cybersecurity Threats in Bangladesh," Bangladesh Institute of International and Strategic Studies (BIISS).

reporting obligations for critical information infrastructure operators in a whole-of-government approach coordinated by the Cyber Security Agency of Singapore (CSA).[70]

But the research does point to limitations. While Singapore's framework is responsive to technological change, it is also a framework that is mainly designed for offences that involve or target Singaporean infrastructure. The CMA has a broader extraterritorial reach than many similar instruments, but faces practical challenges when AI-enabled attacks are launched through anonymised networks, foreign jurisdictions with weaker legal assistance regimes, or decentralised infrastructure such as blockchain-based command and control systems.[71]

Singapore's investment in digital forensics capability and judicial familiarity with technological evidence offers a model that developing states including Bangladesh would benefit from adapting. But Singapore's small-state, high-income context means that resource-intensive solutions are not directly transferrable without significant contextual adaptation.[72]

5.2.4 Bangladesh: Significant Institutional and Legislative Gaps

The jurisdiction most severely affected by the governance gap identified in this thesis is Bangladesh. The Cyber Security Act 2023 was a legislative step forward from the discredited Digital Security Act 2018, but the new Act does not explicitly tackle AI-specific attack vectors,

[70]International Criminal Police Organization (INTERPOL) and United Nations Interregional Crime and Justice Research Institute (UNICRI), Malicious Uses and Abuses of Artificial Intelligence (2020); see also Europol, Facing Reality? Law Enforcement and the Challenge of Deepfakes (2022).

[71]Jabeen, A. Z., "Camouflage of AI in Cyber Crimes Vis-a-Vis Legal Issues and Challenges." See also Rasyid, "Cybercrime Threats and Responsibilities: The Utilization of Artificial Intelligence in Online Crime," Jurnal Ilmiah MIZANI (2024).

[72]International Telecommunication Union (ITU), Global Cybersecurity Index 2024 (Geneva: ITU, 2024); Organisation for Economic Co-operation and Development (OECD), Recommendation of the Council on Artificial Intelligence, OECD/LEGAL/0449 (2019, updated 2024).

autonomous malware, deepfake-based identity fraud or the evidentiary challenges arising from algorithmic opacity.[73]

Another significant gap is institutional capacity. The Bangladesh Police Cyber Crime Unit and Bangladesh Telecommunications Regulatory Commission (BTRC) have limited forensic resources against the scale and sophistication of the incoming threats. Documented cases of AI-generated financial fraud, deepfake-assisted impersonation scams and automated business email compromise have risen sharply, but conviction rates are low, partly because prosecutors lack familiarity with AI-related evidence and courts are sceptical of novel digital proofs.[74]

The study also points to a structural problem in international cooperation. Bangladesh is only an observer state to the Budapest Convention on Cybercrime and has not ratified its Second Additional Protocol on enhanced cooperation and disclosure of electronic evidence. This hinders the country's ability to go after AI-enabled cyber criminals who route attacks through foreign infrastructure, as is common in sophisticated transnational operations.[75]

5.3 Recommendations

On the basis of the foregoing comparative analysis, this chapter sets out a series of targeted, forward-looking recommendations for Bangladesh. These recommendations are organised across three domains: legislative reform, institutional capacity building, and international engagement.

---

[73]Nabi, Md. Nur (2022), "Cyber Law Challenges: Bangladesh, India, UK," LL.B. Thesis, Port City International University. Available at: https://www.scribd.com/document/664313224/Md-Nur-Nabi-20th (accessed 5 March 2026).

[74]Haque, M. M. (10 April 2025), "AI in the Crosshairs," supra note 17; International Criminal Police Organization (INTERPOL), Cyber Threats and Trends Report 2025 (Lyon: INTERPOL, 2025).

[75]Computer Misuse Act (Cap. 50A), Singapore, as amended by the Computer Misuse (Amendment) Act 2017; Cybersecurity Act 2018 (Singapore). For commentary see: International Centre for Law and Legal Studies (ICLG), Cybersecurity Laws and Regulations: Singapore (2025). Available at: https://iclg.com/practice-areas/cybersecurity-laws-and-regulations/singapore (accessed 12 March 2026).

5.3.1 Legislative Reform

First, Bangladesh should enact a dedicated AI Cybercrime Amendment Act or incorporate AI-specific provisions into the Cyber Security Act 2023 by way of a substantive amendment. Such provisions should address the following specific gaps identified in this research:

- Explicit criminalisation of AI-enabled phishing, deepfake fraud, autonomous malware deployment and the use of AI to subvert identity verification systems modelled on section 3 of Singapore's Computer Misuse Act but extended to capture automated execution without continuous human instruction with penalties graduated by reference to the quantum of financial loss, the number of victims, and the degree of automation employed.
- A statutory attribution framework, inserted as a new section into the Cyber Security Act 2023, specifying that where an AI system autonomously executes a cybercrime, criminal liability shall attach jointly and severally to the developer where the system was designed or marketed for offensive use, to the commercial deployer where the system was integrated into a product or service without adequate safeguards, and to the end-user where the system was deliberately directed or misconfigured to commit the offence drawing expressly on the vicarious liability model proposed in the EU AI Liability Directive and adapted to the common-law tradition of Bangladesh.
- A new extraterritoriality provision conferring jurisdiction over AI-enabled cybercrimes where the harmful effect is suffered by a person ordinarily resident or domiciled in Bangladesh, or where the offending AI system processes data belonging to a Bangladeshi citizen, irrespective of where the system or its operators are physically located modelled on article 22 of the Budapest Convention and the long-arm approach of the United States CFAA as interpreted in United States v Nosal (9th Cir, 2012).
- Regulatory empowerment of the Bangladesh Telecommunications Regulatory Commission (BTRC) to issue mandatory technical standards for AI systems deployed in mobile financial services and telecommunications infrastructure, including requirements for explainability logging, anomaly-detection thresholds, and incident-reporting timelines no longer than seventy-two hours after a confirmed AI-enabled breach mirroring the

mandatory incident-reporting obligations imposed on critical information infrastructure operators under section 14 of Singapore's Cybersecurity Act 2018.

Second, Bangladesh should accede to or formally align with the Budapest Convention on Cybercrime and its Second Additional Protocol, thereby securing access to fast-track mutual legal assistance mechanisms that are essential for investigating transnational AI-driven attacks.

5.3.3 International Engagement and Regional Cooperation

Bangladesh should proactively engage with the ASEAN Cyber Capacity Programme and the Commonwealth Cyber Declaration mechanisms to build structured bilateral and multilateral cooperation with Singapore and other technologically advanced partners. Such engagement should extend to joint simulation exercises, harmonised incident-reporting protocols and co-investment in regional AI threat intelligence platforms.

Bangladesh should nominate its MLAT negotiating priorities to include the negotiation of bilateral cybercrime treaties with its principal trading and technology partners, with particular attention to ensuring that evidence-sharing provisions expressly cover AI-generated data, cloud-stored records and cryptocurrency transaction logs.

5.4 Conclusion

This thesis has undertaken a comparative doctrinal analysis of the legal and institutional responses to AI-driven cyber crimes in the United States, Singapore and Bangladesh. The United States and Singapore each possess mature cybercrime statutes, well-resourced enforcement agencies and developing jurisprudence on digital evidence, yet both continue to grapple with how frameworks premised on human agency accommodate the autonomous operation of AI systems. Bangladesh faces a compound challenge: the Cyber Security Act 2023 provides an insufficient statutory foundation, institutional forensic capacity remains inadequate, and the country's limited treaty network constrains its ability to pursue transnational AI-enabled offenders.

BIBLIOGRAPHY

PRIMARY SOURCES

A. Cases

Daubert v Merrell Dow Pharmaceuticals Inc 509 US 579 (1993).

Van Buren v United States 593 US 374 (2021).

B. Legislation

Bangladesh

Digital Security Act 2018 (Bangladesh).

Cyber Security Act 2023 (Bangladesh).

Evidence Act 1872 (Bangladesh).

Information and Communication Technology Act 2006 (Bangladesh).

Singapore

Computer Misuse Act (Cap 50A, 2007 Rev Ed, Singapore), as amended by the Computer Misuse (Amendment) Act 2017 (Act 9 of 2017).

Cybersecurity Act 2018 (Act 9 of 2018, Singapore).

Electronic Transactions Act 2010 (Act 16 of 2010, Singapore).

Evidence Act (Cap 97, 1997 Rev Ed, Singapore).

Penal Code 1871 (Cap 224, 2008 Rev Ed, Singapore).

Personal Data Protection Act 2012 (Act 26 of 2012, Singapore).

Protection from Online Falsehoods and Manipulation Act 2019 (Act 18 of 2019, Singapore).

United States

Computer Fraud and Abuse Act 1986 (US) (as amended), 18 USC § 1030.

Cybersecurity Information Sharing Act 2015 (US), Pub L 114-113.

DEFIANCE Act, Pub L No 118-121 (2024) (US).

Executive Order 14028 on Improving the Nation's Cybersecurity (US, 2021).

Executive Order 14110 on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence (The White House, 30 October 2023).

Federal Rules of Evidence, r 901 (US).

Gramm-Leach-Bliley Act 1999 (US).

Health Insurance Portability and Accountability Act 1996 (US) (HIPAA).

Identity Theft Enforcement and Restitution Act, 18 USC § 1028 (US).

NO FAKES Act (proposed; not enacted as of early 2026) (US).

Wire Fraud Act, 18 USC § 1343 (US).

SECONDARY SOURCES

C. International Instruments

Budapest Convention on Cybercrime (Council of Europe Treaty Series No. 185, 2001, entered into force 2004) <https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185> accessed 1 June 2026.

Organisation for Economic Co-operation and Development, Recommendation of the Council on Artificial Intelligence, OECD/LEGAL/0449 (2019, updated 2024).

Second Additional Protocol to the Convention on Cybercrime on Enhanced Co-operation and Disclosure of Electronic Evidence (Council of Europe Treaty Series No. 224, 2022).

D. Books and Book Chapters

Jabeen AZ, 'Camouflage of AI in Cyber Crimes Vis-a-Vis Legal Issues and Challenges' (unpublished manuscript, 2024).

Rao RA et al, 'Artificial Intelligence (AI) and Cybersecurity Law: Legal Issues in AI-Driven Cyber Defense and Offense' (Research Article, n.d.) 136.

E. Journal Articles

Jiow Hee Jhee, 'A Critical Analysis of Singapore's Cybercrime Legislation' (2023) 35 International Journal of Law and Information Technology 89 <https://doi.org/10.1093/ijlit/eaad002> accessed 1 June 2026.

Krishnamani T, 'Legal Challenges in Regulating AI-Powered Hacking, Phishing, and Identity Theft' (2025) 23(S4) Webology Journal <https://doi.org/10.1145/3680942> accessed 1 June 2026.

Rasyid, 'Cybercrime Threats and Responsibilities: The Utilization of Artificial Intelligence in Online Crime' (2024) Jurnal Ilmiah MIZANI.

Seetharaman S, 'Deepfakes and the Limits of Singapore's Criminal Law' (2024) 36 Singapore Academy of Law Journal 180.

Shetty S, 'AI-Driven Cybercrime: Global Trends and Legal Responses' (2024) 7(2) International Journal of Cybersecurity Intelligence & Cybercrime, Art. 3 <https://vc.bridgew.edu/ijcic/vol7/iss2/3/> accessed 15 April 2026.

F. Theses and Dissertations

Nabi Md Nur, 'Cyber Law Challenges: Bangladesh, India, UK' (LL.B. Thesis, Port City International University, 2022) <https://www.scribd.com/document/664313224/Md-Nur-Nabi-20th> accessed 5 March 2026.

Stephen G, 'AI-Driven Cybersecurity Threats and Defences' (Thesis, Theseus Repository, 2025) <https://www.theseus.fi/bitstream/handle/10024/891045/Stephen_Godwin.pdf> accessed 10 April 2026.

G. Reports and Policy Documents

ASEAN, 'Senior Officials Meeting on Transnational Crime (SOMTC)' <https://asean.org/our-communities/asean-political-security-community/crime/asean-senior-officials-meeting-on-transnational-crime-somtc/> accessed 1 June 2026.

Cyber Security Agency of Singapore, Singapore Cyber Landscape 2023 (CSA, 2024) <https://www.csa.gov.sg/our-programmes/research-and-development/singapore-cyber-landscape> accessed 1 June 2026.

Cyber Security Agency of Singapore, 'SingCERT: About Us' (CSA, 2024) <https://www.csa.gov.sg/singcert> accessed 1 June 2026.

Europol, Facing Reality? Law Enforcement and the Challenge of Deepfakes (Europol, 2022).

Haque MM, 'AI in the Crosshairs: An Assessment of AI-Based Cybersecurity Threats in Bangladesh' (Bangladesh Institute of International and Strategic Studies, 10 April 2025) <https://biiss.org> accessed 1 June 2026.

ICLG, 'Cybersecurity Laws and Regulations: Singapore' (2024) <https://iclg.com/practice-areas/cybersecurity-laws-and-regulations/singapore> accessed 1 June 2026.

Infocomm Media Development Authority (IMDA), 'Digital Economy Framework for Action' (IMDA, Singapore, 2018) <https://www.imda.gov.sg/how-we-can-help/digital-economy-framework> accessed 1 June 2026.

International Criminal Police Organization (INTERPOL) and United Nations Interregional Crime and Justice Research Institute (UNICRI), Malicious Uses and Abuses of Artificial Intelligence (2020).

International Telecommunication Union (ITU), Global Cybersecurity Index 2024 (ITU, 2024).

National Institute of Standards and Technology, AI Risk Management Framework (AI RMF 1.0) (US Department of Commerce, 2023) <https://www.nist.gov/artificial-intelligence> accessed 10 June 2026.

Personal Data Protection Commission (Singapore), Model AI Governance Framework (2nd edn, PDPC, 2020) <https://www.pdpc.gov.sg/help-and-resources/2020/01/model-ai-governance-framework> accessed 1 June 2026.

Personal Data Protection Commission, 'Summary of Key Enforcement Decisions' (PDPC, 2024) <https://www.pdpc.gov.sg/enforcement/decisions> accessed 1 June 2026.

Securities and Exchange Commission, 'Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure' (SEC, 2023).

Singapore Police Force, Annual Scams and Cybercrime Brief 2023 (SPF, 2024) <https://www.police.gov.sg/media-room/statistics> accessed 1 June 2026.

Singapore Police Force, 'Anti-Scam Command' (SPF, 2024) <https://www.police.gov.sg/about-us/organisational-structure/specialist-staff-departments/anti-scam-command> accessed 1 June 2026.

Trajano KKS and Ang B, 'Science, Technology and Security: AI and Crime' (RSIS Commentaries, 26 January 2026) <https://rsis.edu.sg/rsis-publication/rsis/science-technology-and-security-ai-and-crime-january-2026/> accessed 18 April 2026.

World Economic Forum, Global Cybersecurity Outlook 2026 (WEF, 12 January 2026) <https://www.weforum.org/publications/global-cybersecurity-outlook-2026> accessed 20 April 2026.

H. Websites and Online Resources

National Institutes of Health (NIH), PubMed Central Article on AI and Cybersecurity (PMC8862401) <https://pmc.ncbi.nlm.nih.gov/articles/PMC8862401/> accessed 8 April 2026.

Smart Nation Singapore, 'Smart Nation: The Way Forward' (Prime Minister's Office, 2018) <https://www.smartnation.gov.sg> accessed 1 June 2026.