NORTH CAROLINA JOURNAL of
LAW & TECHNOLOGY
Volume 27, Issue 1 2025

ARTICLE

Future Crime: A Theoretical Foundation for Designing Effective Cybercrime Laws in the Age of AI and Ransomware

Thi Ha Do[†] & Niloufer Selvadurai[‡]

The increasing frequency of artificial intelligence ("AI") facilitated cybercrime and ransomware attacks is challenging the effectiveness of current cybercrime laws. In this vexed legal and technological context, the objective of this Article is to develop a new theoretical model for evaluating and guiding the design of cybercrime legislation to address these new and emerging threats. While grounded in the four major criminal law theories: deterrence, retributive justice, restorative justice, and utilitarianism, this Article considers the unique characteristics of cybercrime and develops four normative criteria to assess the effectiveness of legal responses to cybercrime.

Those criteria are (a) clarity of legal definitions and scope of cybercrime and cybersecurity obligations; (b) proportional and consistent penalties; (c) restorative measures that support commercial resilience; and (d) mechanisms for balancing legal certainty with adaptability to technological change. Each criterion responds to a distinct feature of emerging cyber threats, including AI-generated offenses and global anonymity, and ransomware attacks. As the model

© 2025 Thi Ha Do & Niloufer Selvadurai.

[†] Ph.D. Candidate, Macquarie University, Sydney, Australia.

[‡] Professor of Technology Law at the Macquarie Law School, Director of Research and Innovation, Macquarie University, Sydney, Australia.

is theoretically grounded, it offers a practical framework for comparative analysis to guide law and policy makers around the world who are engaged in a critical challenge of our time-designing cybercrime laws that can remain effective and relevant in the face of constant technological change and cybercrime evolution.

Table of Contents

I. INTRODUCTION

As technological innovation transforms the nature and incidence of cybercrime, nations around the world are engaged in refining their cybercrime and cybersecurity laws to make them more effective and relevant. Cybercrime threats posed by artificial intelligence ("AI") such as AI-generated crime, ransomware, sophisticated phishing attacks, clickjacking, fake profiles, de-anonymization attacks, identity cloning, cyberstalking, and other emerging AI-enabled crimes are now common. At present, cybercrime laws do not typically address these new technologically-based cyber challenges. The problem is exacerbated by the rapid pace of technological development. By the time a new law is developed and put into effect, technologies often have already shifted, causing the law to be outdated.[1]

Existing cybercrime laws are often not technology-neutral, drafted in technology-specific language that undermines their longevity. Further, the interconnected nature of the internet has transformed cybercrime into a global problem requiring legislation that has built-in mechanisms for international cooperation. Such cooperation can relate to the proactive prevention of cybercrime such as through surveillance and the sharing of data, and the prosecution of cybercrime offenses through evidence gathering and enforcement.[2] Thus, substantive law reforms are needed to ensure that cybercrime laws effectively address the increasing spectrum of technological advancements and cyber threats.

However, before designing new cybercrime laws or amending existing ones, it is necessary to develop a principled foundation for reform. That is, a theoretical model should be developed to determine what constitutes "effective" law in today's evolving technological context. Such a model would provide objective criteria to evaluate the

1. DAVID GODDARD, MAKING LAWS THAT WORK: HOW LAWS FAIL AND HOW WE CAN DO BETTER 114 (2022).
2. Jonathan Clough, *Cybercrime*, 37 COMMW. L. BULL. 671, 679 (2011).

efficacy of existing laws, design refinements to such laws, and inform the creation of new laws. Such a model could define the scope and nature of effective cybercrime law and provide mechanisms for enforcement, thereby setting a principled and consistent foundation for cybercrime law. Moreover, such a model should effectively uphold cybersecurity,[3] enhance cooperation in combating sophisticated cybercrime,[4] and address the legal responsibilities of public and private sectors in maintaining cybersecurity,[5] while avoiding overly restrictive measures that could hinder digital economic growth.[6] In the absence of such a principled foundation, law reform risks becoming inconsistent and piecemeal.

Present theoretical models for criminal laws do not typically address the challenges raised by emerging cybercrimes such as AI-enabled crime and ransomware. While criminal law has been designed using well established theoretical models, principles, and criteria crafted to ensure justice, promote deterrence, and safeguard public safety,[7] these frameworks rarely address the various challenges

3. *Cf.* Adel Alqudhaibi et al., *Predicting Cybersecurity Threats in Critical Infrastructure for Industry 4.0: A Proactive Approach Based on Attacker Motivations*, 23 SENSORS 4539, 4539 (2023) (discussing models that predict cybersecurity attacks to aid in the prioritization of security countermeasures); *see also* Amanda N. Craig, Scott J. Shackelford & Janine S. Hiller, *Proactive Cybersecurity: A Comparative Industry and Regulatory Analysis*, 52 AM. BUS. L.J. 721, 752–53 (2015) (explaining how proactive cybersecurity measures are shifting the cost burden and becoming a best practice in the industry).
4. Susan W. Brenner & Bert-Jaap Koops, *Approaches to Cybercrime Jurisdiction*, 4 J. HIGH TECH. L. 1, 3–4 (2004).
5. JEFF KOSSEFF, CYBERSECURITY LAW 269 (2d ed. 2019); *see also* Tatiana Tropina & Cormac Callanan, SELF-AND CO-REGULATION IN CYBERCRIME, CYBERSECURITY AND NATIONAL SECURITY *passim* (2015) (discussing public-private collaboration in addressing cybercrime and cybersecurity issues); Kristen E. Eichensehr, *Public-Private Cybersecurity*, 95 TEX. L. REV. 467, 469 (2017).
6. VOXEU, *Commercial Policies and Regulations Now Fragment the Digital Economy*, CTR. FOR ECON. POL'Y RSCH. (June 27, 2022), https://cepr.org/voxeu/columns/commercial-policies-and-regulations-now-fragment-digital-economy [https://perma.cc/2Q3F-4U4T].
7. *See* JEREMY HORDER, ASHWORTH'S PRINCIPLES OF CRIMINAL LAW 16–17 (10th ed. 2022) (explaining that the fundamentatl justification for criminal law lies in deterring or preventing crime and reinforcing social conventions).

raised by cybercrime.[8] Furthermore, established criminal law models tend to focus on national frameworks, discounting the interconnected and global nature of cybercrime. A more effective theoretical model of cybercrime law is needed to address the wide range of both current and future technological advances.

In such a context, the aim of this Article is to develop a new theoretical model for determining what constitutes "effective" cybercrime law. This model will provide a foundation for designing new cybercrime laws and refining existing ones. This Article will begin by identifying the unique features of cybercrime activities that such a model must address. It will then consider the operation and limitations of existing criminal law theory. Building on this foundation, this Article will introduce criteria that are better suited to today's evolving Article landscape.

First, the conceptual model will address the distinct features of cybercrime including the anonymity, transnational reach, rapid evolution, large scale, and automation, all of which challenge the ability of law enforcement, businesses, and individuals to detect, prevent, and investigate offenses. Second, it will emphasize the importance of flexible and adaptable regulations that can evolve with technological changes.[9] Third, the model will bridge the gap between domestic and international legal approaches to cybercrime, promoting greater cross-border cooperation and aiming for a successful harmonization of international cybercrime law. Finally, it will highlight the need for laws that address the prosecution of cybercrimes and preventative measures, such as enhancing cybersecurity infrastructure, promoting e-commerce, and encouraging responsible internet usage. In doing so, this model, based on the concept of balancing "cybersecurity" and "internet commerce," is intended to be both comprehensive and effective. It can be used to identify strengths and weaknesses of existing cybercrime legislation and serve as a

---

8. Beatrice Brunhöber, *Criminal Law of Global Digitality: Characteristics and Critique of Cybercrime Law, in* THE LAW OF GLOBAL DIGITALITY 223, 229 (Matthias C. Kettemann, Alexander Peukert & Indra Spiecker gen. Döhmann eds., 2022).

9. Goddard, *supra* note 1, at 116.

reference point for revisiting cybercrime legislation within a reasonable time frame.

II. Unique Features of Cybercrime that Must be Addressed in a Theoretical Model

A. Emerging Cyber Offenses Enabled by Technology

Contemporary discourse in legal, economic, and information technology fields consistently acknowledges one undeniable reality: The current rate of technological advancement surpasses all historical precedents.[10] The exponential growth of AI, machine learning, and blockchain technologies has fundamentally transformed cybercrime, introducing sophisticated attack vectors that challenge traditional security paradigms.[11] As Treleaven et al. note, the awareness is the key factor in the ill preparation of (financial) regulators, law enforcement, and other institutions in tackling the "explosion" of cybercrime.[12] To establish a foundation for understanding the unique challenges posed by novel forms of cybercrime, it is useful to explore how emerging technologies are expanding the spectrum of cyber offenses. This Section will identify the key characteristics of these new cyber activities and examine how existing regulatory frameworks must co-evolve to address these rapidly developing threats more effectively.

---

10. *See* Alessandro Fedele & Cristian Roner, *Dangerous Games: A Literature Review on Cybersecurity Investments*, 36 J. Econ. Surv. 157, 158 (2022); Mazaher Kianpour & Shahid Raza, *More Than Malware: Unmasking the Hidden Risk of Cybersecurity Regulations*, 5 Int'l Cybersecurity L. Rev. 169, 169 (2024) (reiterating that technology is ever-evolving); Joëlle Webb, *Rethinking the Governance of Technology in the Digital Age*, *in* The Oxford Handbook of Cyber Security 688, 690 (Paul Cornish ed., 2021); Maskun et al., *Qualifying Cyber Crime as a Crime of Aggression in International Law*, 13 J. E. Asia & Int'l L. 397, 398 (2020); Marc Goodman, Future Crimes: Everything Is Connected, Everyone Is Vulnerable and What We Can Do About It 41 (2015).

11. Philip Treleaven et al., *The Future of Cybercrime: AI and Emerging Technologies Are Creating a Cybercrime Tsunami*, SSRN Elec. J. 1, 1 (2023), https://discovery.ucl.ac.uk/id/eprint/10173722/1/SSRN-id4507244.pdf [https://perma.cc/PG7C-APPE].

12. *Id.*

The notion of emerging technology refers to phenomena involving either: (a) the convergence of existing technologies; or (b) the creation of fundamentally novel technologies with the potential to radically reshape industrial landscapes and socioeconomic systems.[13] The greatest challenge of such technologies is balancing innovation and regulation.[14] Effective regulation must resolve the tension between present technological threats and probabilistic future misuse scenarios. Scholars have traditionally identified three generations of cybercrime:[15] (a) crimes committed using computers; (b) cybercrimes spanning global networks; and (c) cybercrimes meditated by technology, characterized by their distributed and automated nature.[16] The primary motives of cybercriminals include financial gain; espionage or spying (for governments, industries, or corporations); ideology (e.g., hacktivism, cyberterrorism, or cyberwarfare); and personal motives such as harassment, revenge, or fun.[17]

There are two common frameworks used by scholars and law enforcement to classify cybercrime. First, there are devices-as-targets[18] crimes which result in: (a) unauthorized access to computer systems; (b) malicious code (e.g., viruses, worms, trojan horses, software bombs); and (c) devices-as-tools crimes,[19] which include content violations and unauthorized alteration of data or software.[20] Second, a

---

13. Webb, *supra* note 10, at 690; *see also* HEDI NASHERI, EMERGING TECHNOLOGIES, NOVEL CRIMES, AND SECURITY: THE GOOD, THE BAD, AND THE UGLY 12 (2024) (describing how AI, robotics, quantum, 3D/biotech, 5G/6G, automation, and IoT are transforming the current world into a digital world and enabling entire industries and fields of science to be reshaped).

14. Treleaven et al., *supra* note 11, at 1.

15. DAVID WALL, CYBERCRIME: THE TRANSFORMATION OF CRIME IN THE INFORMATION AGE 44–47 (2007); *see* GOODMAN, *supra* note 10, at 37–43.

16. GOODMAN, *supra* note 10, at 41.

17. ALEX ALEXANDROU, CYBERCRIME AND INFORMATION TECHNOLOGY: THEORY AND PRACTICE—THE COMPUTER NETWORK INFRASTRUCTURE AND COMPUTER SECURITY, CYBERSECURITY LAWS, INTERNET OF THINGS (IOT), AND MOBILE DEVICES 54–55 (2021).

18. Brenner & Koops, *supra* note 4, at 40.

19. *See id.*

20. Maskun et al., *supra* note 10, at 401.

distinction is drawn between cyber-enabled crime[21] and cyber-dependent crime.[22] The relationship between these two cybercrime classification methods is illustrated in the following table:

Table 1. General Classification of Traditional Cybercrime

Cyber-enabled crime	Devices as tools	Example: Online fraud and scam, identity theft, online harassment and abuse, misinformation, unauthorized data acquisition
Cyber-dependent crime	Devices as targets	Example: Malware, ransomware, DDoS attacks, hacking

Prior to the emergence of criminal algorithms,[23] these crimes were known as traditional cybercrimes. Scholars have described a "perfect storm" of technologies[24] that has made certain cybercrimes

21. JACOPO BELLASIO ET AL., RAND EUR., THE FUTURE OF CYBERCRIME IN LIGHT OF TECHNOLOGY DEVELOPMENTS 2–3 (Dec. 2020), https://www.rand.org/pubs/research_reports/RRA137-1.html [https://perma.cc/XHG8-PQ4Z]. Cyber-enabled crime refers to crimes that existed before the internet, but technology has expanded in scale, such as online fraud. *Id.*

22. Cyber-dependent crime refers to crimes that cannot be committed without a computer system, such as malware, ransomware, distributed denial-of-service ("DDoS") attacks, and hacking. *Id.*

23. Treleaven et al., *supra* note 11, at 5; Carlo Piparo & Radovan Blazek, *Criminal Algorithms and Their Punishment in Modern Constitutionalism*, 8 BRATISLAVA L. REV. 199, 202 (2024) (Slovk.).

24. Treleaven et al., *supra* note 11, at 6.

unprecedentedly efficient.[25] For example, modern online scam strategies powered by technology are reported to be low-cost[26] and highly personalized, enabling perpetrators to target victims with exceptional precision.[27] To provide a broader understanding of novel cybercrime, Treleaven et al. offer a comprehensive analysis of its evolution alongside complex emerging technologies, including: (a) AI algorithms; (b) blockchain and decentralized systems; and (c) the Internet of Things ("IoT"), encompassing smart devices and critical infrastructure.[28]

First, regarding the use of generative AI in criminal activities, scalable social engineering is used in AI-generated text,[29] such as phishing emails[30] and romantic scams,[31] to create fraud scripts[32] or

---

25. Gregory Dickinson, *The Patterns of Digital Deception*, 65 B.C. L. REV. 2457, 2462 (2024).

26. P. Durgadevi et al., *Low-Cost High-Impact AI Tools vs Cybercrime, in* ARTIFICIAL INTELLIGENCE FOR CYBER DEFENSE AND SMART POLICING 110, 113 (Vijayalakshmi et al. eds. 2024).

27. Dickinson, *supra* note 25; Fiona Guy, *The Deepfake Crisis: How AI Is Reshaping Criminal Justice*, CRIME RSCH (Feb. 18, 2025), https://www.crimetraveller.org/2025/02/the-deepfake-crisis-ai-criminal-justice/ [https://perma.cc/KB2W-KEEQ].

28. Treleaven et al., *supra* note 11 *passim*.

29. FED. BUREAU OF INVESTIGATION, ALERT NO. I-120324-PSA, CRIMINALS USE GENERATIVE ARTIFICIAL INTELLIGENCE TO FACILITATE FINANCIAL FRAUD (Dec. 3, 2024), https://www.ic3.gov/PSA/2024/PSA241203 [https://perma.cc/6XWH-V386]. AI-powered phishing emails are understood as fraudulent emails created with generative AI that closely mimic legitimate communication by personalizing content and writing style, making them more difficult for users to detect. *See* Lenore Taylor, *AI Will Make Scam Emails Look Genuine, UK Cybersecurity Agency Warns*, GUARDIAN (Jan. 24, 2024), https://www.theguardian.com/technology/2024/jan/24/ai-scam-emails-uk-cybersecurity-agency-phishing [https://perma.cc/34XR-AV34].

30. AI-powered phishing emails are understood as fraudulent emails created with generative AI that closely mimic legitimate communication by personalizing content and writing style, making them more difficult for users to detect. *See* Taylor, *supra* note 29.

31. Cassandra Cross & Thomas J. Holt, *More than Money: Examining the Potential Exposure of Romance Fraud Victims to Identity Crime*, 24 GLOB. CRIME 107 *passim* (2023).

32. *See* Zeya Lwin Tun & Daniel Birks, *Supporting Crime Script Analyses of Scams with Natural Language Processing*, 12 CRIME SCI. 1, 2 (2023).

conversations in order to earn users' trust and steal money from their bank accounts in the form of gifts or high-yield investments.[33] AI-driven identity fraud, including the creation of fabricated profiles, deepfake imagery, and credential theft, now enables real-time impersonation with voice cloning and synthetic videos, eroding public trust in digital communications.[34] Scholars also note that cybercriminals may deliberately create jailbreak prompts to bypass AI safeguards, causing the system to generate harmful, illegal, or misleading content, even when the system is supposed to block such content,[35] or poison AI data for malicious purposes.[36] Moreover, sophisticated AI algorithms, androids, and avatars also present risks. Some "virus-like algorithms" are intentionally programmed to commit crimes, "feral algorithms" evolve in unintended ways, and "superintelligent AI" can potentially be used for criminal activities.[37]

Second, regarding blockchain and decentralized systems, the main issue lies in their anonymity. Smart contract exploits,[38] including reentrancy attacks and flash loans, are used to drain millions from

33. *See* Dickinson, *supra* note 25, at 2460.

34. For an explanation of how Generative AI and GPT enhance typical cyber scams like hacking, impersonation, malware, and reputational threats, see Treleaven et al., *supra* note 11, at 12,. This includes data mining to identify potential victims, 'pump-and-dump,' ransomware targeting dark web 'trap' sites, and romantic scams using fake online identities, chatbots, and avatars to capture victims' trust. *Id.*

35. *Id.* at 5. *See* Zhiyuan Yu et al., *Don't Listen to Me: Understanding and Exploring Jailbreak Prompts of Large Language Models* ARXIV (Sep. 30, 2024) https://doi.org/10.48550/arXiv.2403.17336 [https://perma.cc/S8G8-A4M6] (presenting one of the most well-known prompts is to ask an LLM to adopt a different persona and emulate 'Do Anything Now' behaviors to bypass safety constraints).

36. Junli Shen & Maocai Xia, *AI Data Poisoning Attack: Manipulating Game AI of Go*, ARXIV (July 30, 2020), https://arxiv.org/abs/2007.11820 [https://perma.cc/4NTN-3GCE].

37. Treleaven et al., *supra* note 11, at 4, 7.

38. *See e.g.*, U.N. OFF. ON DRUGS & CRIME, TRANSNATIONAL ORGANIZED CRIME AND THE CONVERGENCE OF CYBER-ENABLED FRAUD, UNDERGROUND BANKING AND TECHNOLOGICAL INNOVATION IN SOUTHEAST ASIA: A SHIFTING THREAT LANDSCAPE 104 (Oct. 2024).

decentralized finance ("DeFi") platforms.[39] Investors are exposed to increased risks and losses in the turbulent market due to the lack of regulation.[40] In addition, cryptocurrency-enabled crimes[41] now include traditional money laundering and investment fraud,[42] such as rug pulls,[43] non-fungible token ("NFT") fraud,[44] and anonymous ransomware payments that take advantage of regulatory grey areas.

Third, the growth of the IoT and decentralized infrastructures is facilitated by two core technological pillars: Web 3.0[45] and smart

---

39. *See* Arianna Trozze, Bennett Kleinberg & Toby Davies, *Detecting DeFi Securities Violations from Token Smart Contract Code*, 10 FIN. INNOVATION 78, 79 (2024). *See generally* Treleaven et al., *supra* note 11, at 14 (explaining bogus coin, non-fungible token giveaway, and fake crypto exchange cryptocurrency scams, and DeFi generally). Decentralized Finance ("DeFi") is a system of financial services, like lending, borrowing, or trading, that runs on blockchain without needing banks or middlemen.

40. Sean Kwon, *Regulation of DeFi Lending: Agency Supervision on Decentralization*, 24 COLUM. SCI. & TECH. L. REV. 379, 379 (2023).

41. Rhianna Hamilton & Christian Leuprecht, *The Crime-Crypto Nexus: Nuancing Risk Across Crypto-Crime Transactions, in* 115 FINANCIAL CRIME AND THE LAW: IDENTIFYING AND MITIGATING RISKS 15, 15 (Doron Goldbarsht & Louis de Koker eds., 2024).

42. Alana Maurushat & Dan Halpin, *Investigation of Cryptocurrency Enabled and Dependent Crimes*, *in* 47 FINANCIAL TECHNOLOGY AND THE LAW: COMBATING FINANCIAL CRIME 235 *passim* (Doron Goldbarsht & Louis De Koker eds., 2022).

43. *See* Ye Qiao et al., *Detecting Rug Pull Scams on Blockchain via Feature Fused Graph Classification*, *in* BLOCKCHAIN TECHNOLOGY AND APPLICATION 67, 68 (Jianming Zhu et al. eds., Springer 2024) (presented at the Int'l Conf. on Blockchain and Cybersecurity, 2023).

44. NFTs refer to digital assets that prove your unique digital item, like a piece of art, a collectible or other online content. *See* Nitin Upadhyay & Shalini Upadhyay, *The Dark Side of Non-Fungible Tokens: Understanding Risks in the NFT Marketplace from a Fraud Triangle Perspective*, 11 FIN. INNOVATION 62, 62–63 (2025).

45. Web 3.0 refers to the next generation of the internet, characterized by decentralization, semantic data integration, and user empowerment. Built upon decentralized technologies such as blockchain, peer-to-peer ("P2P") networks, and cryptographic protocols, Web 3.0 facilitates the development of decentralized applications ("Dapps") and services that operate without reliance on centralized servers. *See* Diptiben Ghelani, *Navigating the Complex Intersection of Cybersecurity, IoT, and Artificial Intelligence in the*

footnote continued on next page

devices.[46] The growing variety of interconnected digital technologies has expanded the potential entry points and attack surfaces that cybercriminals can exploit.[47] Botnet attacks, which are powered by compromised IoT devices, are frequently used to launch large-scale DDoS attacks on transportation networks, power grids, and hospitals.[48] More recently, AI-powered ransomware attacks[49] are increasingly targeting industrial control systems, posing threats to physical infrastructure.[50]

Era of Web 3.0, 71 INT'L J. COMPUT. TRENDS & TECH. 45, 45 (2023); *see also* Bandar Alotaibi, *Cybersecurity Attacks and Detection Methods in Web 3.0 Technology: A Review*, 25 SENSORS (BASEL) 342, 342 (2025) (arguing that Web 3.0 provides a new era of internet but has security concerns).

46. Smart devices include everyday electronic objects: Smartphones, smartwatches, or home appliances, that are equipped with sensors, internet connectivity, and the ability to collect and share data. *See* Hezam Akram Abdulghani, Anastasija Collen & Niels Alexander Nijdam, *Guidance Framework for Developing IoT-Enabled Systems' Cybersecurity*, 23 SENSORS 4174, 4174 (2023) (Switz.).

47. *See* Charles Harry, Ido Sivan-Sevilla & Mark McDermott, *Measuring the Size and Severity of the Integrated Cyber Attack Surface Across U.S. County Governments*, 11 J. CYBERSECURITY 1, 2–3 (2025) (providing an empirical assessment of attack surfaces in American municipalities); *see also* Uihyeon Song, Gimin Hur, Sangjin Lee & Jungheum Park, *Unraveling the Dynamics of the Cyber Threat Landscape: Major Shifts Examined Through the Recent Societal Events*, 103 SUSTAINABLE CITIES & SOC'Y 10, 10 (2024) (observing that technological adoption across industries has widened the attack surface, contributing to increasing cyberattacks at recent social events).

48. ALEXANDROU, *supra* note 17, at 302.

49. AI-powered ransomware attacks are a form of cyberattack where criminals use AI combined with ransomware to make their attacks smarter and harder to stop. It is explained that these attacks use machine learning algorithms to automatically find vulnerabilities in a victim's computer system, break in, and lock or encrypt important data. The attackers then demand money (a ransom) to restore access to the files or system. AI makes these attacks more dangerous because it allows the ransomware to adapt, avoid detection, and target victims more effectively. *See* Jannatul Ferdous et al., *AI-Based Ransomware Detection: A Comprehensive Review*, 12 IEEE ACCESS, 136666, 136666–67 (2024).

50. In March 2024, LockBit ransomware group targeted Crinetics Pharmaceuticals in the United States. The attackers used advanced ransomware that could adapt and encrypt large amounts of sensitive data. They demanded a $4

footnote continued on next page

1. Unique Features of Novel Cybercrimes Enabled by Emerging Technology

A notable feature of emerging cybercrime is the automation and scalability of attacks.[51] Cybercriminals now deploy AI-driven tools to autonomously identify network vulnerabilities, spread malware, and create convincing phishing campaigns at scale, making crimes faster and harder to investigate. The autonomous nature of AI systems introduces significant challenges for offender accountability. Unlike traditional tools, AI can operate without direct human intervention,[52] increasing the liability of businesses, creators, and users when AI-enabled crimes occur.[53] This shift from human-controlled crime to machine-mediated crime is likely to necessitate a reconsideration of

---

million ransom to release the stolen credentials and restore access to the compromised systems. *Id.* at 136667; *Understanding Ransomware Threat Actors: LockBit,* AUSTL. SIGNALS DIRECTORATE, AUSTL. CYBER SEC. CTR. (June 15, 2023), https://www.cyber.gov.au/about-us/advisories/understanding-ransomware-threat-actors-lockbit [https://perma.cc/57QX-34ZY]. EKANS ("Snake") Ransomware on Manufacturing & ICS: Attacks in June 2020 impacted Honda's global operations and systems at Enel Group, caused production lines to shut down, see Edgar Namoca, *Targeted Attacks on Industrial Control Systems*, UNIV. OF HAW. W. O'AHU CYBERSECURITY (Oct. 15, 2020), https://westoahu.hawaii.edu/cyber/ics-cybersecurity/ics-weekly-summaries/targeted-attacks-on-industrial-control-systems/ [https://perma.cc/X4F3-WXW3]. In August 2021, when the Hive ransomware group attacked Memorial Health System, a hospital network in Ohio, the ransomware shut down hospital IT systems, forcing the diversion of emergency patients and cancellation of surgeries and radiology exams. *See also* Anuja Vaidya, *Hive Is a New & Potentially Devastating Type of Ransomware. Here's What You Need to Know*, MEDCITY NEWS (Sep. 16, 2021, at 16:46 ET) medcitynews.com/2021/09/hive-is-a-new-potentially-devastating-type-of-ransomware-heres-what-you-need-to-know/ [https://perma.cc/5UQQ-S2Z5] (evolving threats in ransomware should make health systems cautious).

51. Joe Burton et al, *AI and Serious Online Crime*, in CETAS RESEARCH REPORT 11, 17, 19 (2025); Prithwish Ganguli, *The Rise of Cybercrime-as-a-Service: Implications and Countermeasures*, 6 INT'L J. MULTIDISCIPLINARY RSCH. 1, 1 (2024).

52. Francesca Lagioia & Giovanni Sartor, *AI Systems Under Criminal Law: A Legal Analysis and a Regulatory Perspective*, 33 PHIL. & TECH. 433, 434 (2020).

53. *See* Paulo Henrique Padovan, Clarice Marinho Martins & Chris Reed, *Black Is the New Orange: How to Determine AI Liability*, 31 A.I. & L. 133, 134 (2023).

traditional liability concepts, as AI systems may themselves be capable of committing offenses that are difficult to attribute to any single party.[54] In some cases, it has been argued that the damage caused by AI systems could warrant exploring new liability models, such as recognizing AI systems as legal entities or developing residual liability frameworks when no human actor can be identified.[55]

Another key characteristic is hyper-personalization,[56] where large-scale data mining[57] and machine learning allow criminals to craft highly tailored scams that exploit individual users' behaviors, preferences, and weaknesses.[58] This level of personalization increases the likelihood that the rate of fraudulent schemes will succeed, while simultaneously taking advantage of vulnerable populations without their knowledge or consent.[59] Furthermore, many of these offenses operate within a regulatory grey area.[60] Technologies used include

---

54. Andreas Nanos, *Criminal Liability of Artificial Intelligence*, 2023/III/3 (Prauge L. Working Paper Series 1, 3 (2023), https://ssrn.com/abstract=4623126 [https://perma.cc/QL6P-8WJF]; *see also* Beatrice Panattoni, *Generative AI and Criminal Law*, 1 CAMBREIDGE F. AI: L. & GOVERNANCE 1, 1 (2025) (discussing how AI content raises question about how criminal law should develop).

55. *See* Maarten Herbosch, *Liability for AI Agents*, 26 N.C. J.L. & TECH. 391, 405 (2025); Athina Sachoulidou, *AI Systems and Criminal Liability: A Call for Action*, 11 OSLO L. Rev. 1, 3 (2024).

56. Dickinson, *supra* note 25, at 2472.

57. ADEMOLA O. ADESINA ET AL., INVESTIGATING DATA MINING TREND in CYBERCRIME AMONG YOUTHS 725 (G. Ranganathan, R. Bestak & X. Fernando eds., Springer 2023).

58. Dickinson, *supra* note 25, at 2472.

59. Treleaven, *supra* note 11, at 12, 14; *see* Joanna Curtis & Gavin Oxburgh, *Understanding Cybercrime in 'Real World' Policing and Law Enforcement*, 96 POLICE J.: THEORY, PRAC. & PRINC. 573, 575 (2023); Alexandra Burton et al., *Exploring How, Why and What Contexts Older Adults Are at Risk of Financial Cybercrime Victimisation: A Realist Review*, 159 EXPERIMENTAL GERONTOLOGY 111678 *passim* (2022),

60. *See* Jacquelyn Sherman, *A Feast of Fraud: How International Hesitations to Regulate Deepfakes Are Creating a Buffet for Financial Criminals*, 56 GEO. WASH. INT'L L. REV. 91, 93 (2025); *see also* Yinuo Geng, *Comparing "Deepfake" Regulatory Regimes in the United States, the European Union, and China*, 7 GEO. L. TECH. REV. 157, 162 (2023) ("In the United States, no federal law on deepfakes (or on AI or on data privacy) has passed . . . [t]his has left a vacuum for states to fill.").

deepfakes,[61] criminal algorithms, and misleading digital interfaces, which may fall outside clear legal definitions of criminal intent[62] or damage.[63] Rooted in individual responsibility and retroactive enforcement, traditional criminal laws are currently not fit to handle autonomous, anonymized actors and algorithmic decision-making.[64]

---

61. Deepfakes generally refer to hyper-realistic media—most commonly videos, images, or audio—that falsely depict a person saying or doing something they never actually did. *See* Alena Birrer & Natascha Just, *What We Know and Don't Know About Deepfakes: An Investigation into the State of the Research and Regulatory Landscape*, NEW MEDIA & SOC'Y 5 (May 21, 2024), https://journals.sagepub.com/doi/10.1177/14614448241253138 [https://perma.cc/TN98-9MAU]. For deepfakes, the gray area lies in the fact that deepfakes intersect with many existing laws (privacy, consumer laws and advertising rules, online safety, digital services, intellectual property, defamation, criminal law), yet do not precisely fit any one category. Many of these regulations were not meant for AI-synthesized content, which leaves questions regarding intent, consent, liability, and implementation. While the United Kingdom, European Union, and Australia have begun to control some aspects of the issue (such as sexual deepfakes and platform responsibilities), there is no comprehensive or particular legal framework to handle the more general social, political, and ethical consequences of deepfakes. Roch Glowacki, *Digital, Commerce & Creative 101: Is This for Real? The Legal Reality Behind Deepfakes*, LEWIS SILKIN (Nov. 4, 2024), https://www.lewissilkin.com/insights/2024/11/04/is-this-for-real-the-legal-reality-behind-deepfakes [https://perma.cc/8ELJ-677M]; *see also* María-Paz Sandoval, Mariana de Almeida Vau, Julia Solaas & Lyria Rodrigues, *Threat of Deepfakes to the Criminal Justice System: A Systematic Review*, 13 *Crime Sci.* art. no. 41, at 5 (2024) (discussing issues with attribution and building a legal case with deepfakes).

62. Technologies like deepfakes blur the line between intentional deception and automated manipulation, making it difficult for the law to adequately capture the full range of harms and to establish clear intent in such cases. *See* Andrew W. Eichner, *Artificial Intelligence and Weaponized Illusions: Methodologies for Federal Fraud Prosecutions Involving Deepfakes*, 73 AM. U. L. REV. 1319, 1339 (2024).

63. Dickinson, *supra* note 25, at 2495 ("These catch-all provisions mean the laws provide little certainty to regulated entities, who can see no guaranteed path of compliance. And the laws are unnecessary because the conduct they target is already barred by general consumer protection laws prohibiting unfair or deceptive practices of any sort.").

64. *Id.* at 2499 ("Precedent-based decision-making sacrifices ex ante certainty for ex post flexibility and provides less certainty to regulated parties . . . [t]he approach shines, however, in contexts where ex ante rules are impossible or

footnote continued on next page

Recent legal discourse on the EU AI Act and U.S. cybersecurity reforms note that current legal frameworks remain overly focused on static data protection (particularly the confidentiality of information) while neglecting the integrity (e.g., website defacement) and availability (e.g., ransomware attacks) of data and systems, leading them fail to anticipate the dynamic, real-time manipulation capabilities of emerging cybercrimes.[65] The inadequacy of the law in addressing these unique features exposes individuals and organizations to harm that is difficult to detect, attribute, or prosecute.

2. Regulatory Responses to Cybercrime Involving Emerging Technology

In response to these complex regulatory challenges, some scholars suggest that lawmakers should adopt a co-adaptive[66] and

---

undesirable, and thus, there is little loss of certainty to regulated parties by delaying classification of behaviour as lawful or unlawful until after all facts are in hand. Online deception is such a context."). Indeed, cybercrime presents a challenge that law enforcement is ill equipped to regulate:

> More importantly, law enforcement and regulators traditionally operate a) retrospectively, b) with identifiable individuals and organizations, and c) in national jurisdictions. Cybercrime is changing all of this. Firstly, the dynamic nature of emerging technologies requires near real-time intervention using authentication and anomaly detection. Examples being misinformation or deepfake impersonation. Secondly, participants are increasingly anonymous: humans, algorithms, avatars, and organizations. Thirdly, innovations and abuses frequently occur in cyberspace domains unfamiliar to regulators and law enforcement. An example being young TikTok influencers offering financial advice to young naïve fans.

Treleaven et al., *supra* note 11, at 1.

65. *See* Jeff Kosseff, *Upgrading Cybersecurity Law*, 61 HOUS. L. REV. 51, 56–57 (2023); *see also* Simona Ramos & Joshua Ellul, *Blockchain for Artificial Intelligence (AI): Enhancing Compliance with the EU AI Act Through Distributed Ledger Technology. A Cybersecurity Perspective*, 5 INT'L CYBERSECURITY L. REV. 1, 10 (2024) (implementing blockchain technology can provide secure storage for data addressing current concerns).

66. Marco Dell'Erba, *The Underlying Complexities Within the Line of Disruption, in* TECHNOLOGY IN FINANCIAL MARKETS: COMPLEX CHANGE AND DISRUPTION 1, 7 (2024).

forward-looking legal framework[67] capable of addressing emerging activities of cybercrime. It is recommended that legislation proactively define the misuse of synthetic content, such as deepfakes, within cybercrime statutes and mandate technical measures like AI "watermarking" to verify authenticity.[68] Establishing civil liability or criminal frameworks for offenses committed by or through AI systems,[69] while balancing robust enforcement with the need to promote innovation,[70] is also crucial. Because private enforcement has proven insufficient and fragmented,[71] emerging cyber harms should be explicitly recognized and prosecuted under criminal law frameworks. Furthermore, it has been proposed that international cooperation should be strengthened by harmonizing cryptocurrency regulations to mitigate jurisdictional arbitrage, and by expanding the capacity of global law enforcement agencies, such as INTERPOL's cybercrime units, to facilitate cross-border investigations.[72] Strengthening public-private partnerships to address vulnerabilities in decentralized infrastructures is a critical solution emphasized by scholars.[73]

---

67. Kosseff, *supra* note 65, at 56.

68. Eichner, *supra* note 62, at 1331–32.

69. Lagioia & Sartor, *supra* note 52, at 457–59 (Section 8.1 and 8.2 outline civil and criminal liability responses to AI crimes).

70. *See* Treleaven et al., *supra* note 11, at 20 ("[I]ncreasingly LawTech is used for all aspects of (DeepTech) technologies for delivering law enforcement services.").

71. *See* Dickinson, *supra* note 25, at 2499.

72. Kosseff, *supra* note 65, at 69–70; Treleaven et al., *supra* note 11, at 25; *see also* Dickinson, *supra* note 25, at 2500 (discussing how it can be difficult for victims to have their claim heard when it comes to cross-border issues); Nancy Michail & Niloufer Selvadurai, *Towards an Effective Regulatory and Governance Framework for Central Bank Digital Currencies*, 6 STAN. J. BLOCKCHAIN L. & POL'Y 189, 190 (2023).

73. Kosseff, *supra* note 65, at 66; *see also* Raphael Bossong & Ben Wagner, *A Typology of Cybersecurity and Public- Private Partnerships in the Context of the EU*, 67 CRIME L. & SOC. CHANGE 265, 265 (2017) ("[T]o provide cybersecurity[,] public[,] and private actors clearly need to engage with each other.").

This includes the introduction of mandatory security certification standards for IoT devices,[74] akin to existing safety standards in other industries, and the allocation of resources to develop AI-driven threat detection tools accessible to law enforcement agencies. It is also suggested that future legal reforms should prioritize the development of victim-centric protections to enhance victim participation, and improve overall justice outcomes.[75] Suggested measures include the streamlining of cybercrime reporting through centralized platforms, and the implementation of public awareness campaigns to educate users about the risks of AI-enabled fraud and manipulation.[76] Table 2 classifies emerging cybercrimes and regulatory challenges linked to new technologies:

---

74. Internet of Things Cybersecurity Improvement Act of 2020, Pub. L. No. 116-207, 134 Stat. 1189 (2020); *see also* Kosseff, *supra* note 65, at 79–80 (discussing Cybersecurity Improvement Act's requirements for the development of security guidelines for IoT device's).

75. Paul Michael Gilmour, *Exploring the Barriers to Policing Financial Crime in England and Wales*, 15 POLICING: J. POL'Y & PRAC. 1507, 1519 (2021) ("Victims of fraud and other financial crimes need the full support of the police … [t]raining materials should be cascaded throughout the police workforce to support investigators facing increasing policing demands and to enhance support for victims."); Danielle Keats Citron, *Sexual Privacy*, 128 YALE L.J. 1870, 1877 (2019) (suggesting a path for reform that would fill gaps in the existing protections that have enabled a culture of impunity); Clare McGlynn & Erika Rackley, *Image-Based Sexual Abuse*, 37 OXFORD J. LEGAL STUD. 534, 561 (2017) ("We recommend harnessing the expressive and coercive power of civil and criminal law in new ways to provide redress for victim-survivors and to encourage cultural change . . . .").

76. OFFICE FOR STATISTICS REGULATION, *Systemic Review Programme: Review of Fraud and Computer Misuse Statistics for England and Wales* 4 (Apr. 2025) (presenting the central recording of fraud and computer misuse crimes, managed by the City of London Police); *see also* Sherman, *supra* note 60, at 116–17 ("[I]ndividuals will also be on the frontlines in preventing attacks and must develop the skills and tools necessary to avoid harm.").

Table 2: Classification of Emerging Cybercrime Threats, Regulatory Challenges, and Proposed Legal Responses[77]

Emerging Technology	Novel Cybercrime Threats	Regulatory Challenges	Proposed Legal Responses
Generative AI and Deepfakes	Non-consensual deepfakes, AI-generated impersonation scams	Legal uncertainty about synthetic content misuse	Clearly define misuse of synthetic content in cybercrime statutes, Mandate digital watermarking of AI-generated media
Blockchain and DeFi	Smart contract exploits (reentrancy attacks, flash loans), Cryptocurrency-enabled crimes (rug pulls, NFT fraud, ransomware payments)	Anonymity complicating prosecution, Jurisdictional arbitrage	Harmonize cryptocurrency regulations, Expand INTERPOL's cybercrime units
IoT	Botnet-driven DDoS attacks on critical infrastructure, AI-driven ransomware targeting industrial control systems	Fragmented security standards across manufacturers	Require IoT security certification standards

77. *See generally* Treleaven et al., *supra* note 11 (offering a chart that summarizes threats of and regulatory responses to emerging technologies).

Decentralized Infrastructures	Ice phishing attacks, Data manipulation in DApps and Web 3.0 platforms	Regulatory lag behind emerging technologies	Develop real-time regulatory frameworks, Promote the coevolution of AI-powered threat detection tools for law enforcement
Critical Infrastructure Dependence on Private Vendors	Blurred accountability in infrastructure attacks	Public-private divide in cybersecurity governance	Promote public-private collaboration, Clarify liability frameworks

B. The Human Factor: Psychological Vulnerabilities and Cybercrime Laws

Traditional criminal laws often fall short in addressing emerging harms—particularly psychological distress[78]—that arise in cyber-related contexts.[79] Some argue that human factors have traditionally been explored primarily through criminological theories of offending and victimization, while receiving comparatively little attention in legal or consumer protection frameworks.[80] Legal discourse on cybercrime tends to focus on eye-catching technological

78. Paul McGorrery, *Causing Psychological Harm: A Criminal Offense?*, 46 CRIM. L.J. 125, 131 (2022).

79. Isabella Voce & Anthony Morgan, *Developing a Harm Index for Individual Victims of Cybercrime*, 706 TRENDS & ISSUES CRIME & CRIM. JUST. 1, 2 (2025) (Austl.).

80. Afrah Almansoori, Mostafa Al-Emran & Khaled Shaalan, *Exploring the Frontiers of Cybersecurity Behavior: A Systematic Review of Studies and Theories*, 13 APPL. SCI. 5700, 5703 (2023); Slim Masmoudi, *Unveiling the Human Factor in Cybercrime and Cybersecurity: Motivations, Behaviors, Vulnerabilities, Mitigation Strategies, and Research Methods*, *in* CYBERCRIME UNVEILED: TECHNOLOGIES FOR ANALYSING LEGAL COMPLEXITY 41, 41 (Mohamed Chawki & Ajith Abraham eds., 2025); Gift Onwuadiamu, *Cybercrime in Criminology: A Systematic Review of Criminological Theories, Methods, and Concepts*, 8 J. ECON. CRIMINOLOGY 100136, 100137 (2025).

exploits, such as cyberattacks, hacking or sophisticated malware.[81] Yet, an equally potent, perhaps even more pervasive, threat appears to be the human factor: attackers relying on tactics of persuasion or emotional manipulation, a risk that remains insufficiently addressed.[82] Psychological vulnerabilities, including trust, fear, greed, or even simple inattention, likely open the door for attackers to manipulate unsuspecting individuals.[83] Phishing emails, social-engineering phone calls, and malicious links frequently rely more on human trust than on advanced technical skill, suggesting that effective cybercrime mitigation requires the transition towards human-centered approaches, covering cognition and behaviors.[84] Historically, cybercrime laws in some jurisdictions have focused on concrete outcomes or tangible harms, and as a result, have sought to criminalize specific tools and methods (e.g., malware or DDoS attacks),[85] while overlooking the psychological distress inflicted on victims.[86] Current research consistently indicates that cybercriminals capitalize on predictable mental shortcuts, such as urgency, authority, or social proof.[87] For example, an attacker might impersonate a familiar institution and urge immediate action ("Your account will be closed if . . . "), hijacking our ingrained fear of negative consequences or

---

81. Matthew C. Waxman, *Cyber-Attacks and the Use of Force: Back to the Future of Article 2(4)*, 36 YALE J. INT'L L. 421, 422 (2011); *see also* Neel Guha, Peter Henderson & Diego A. Zambrano, *Vulnerabilities in Discovery Tech*, 35 HARV. J.L. & TECH. 609 (2022) (focusing on hacking exploits and malware vulnerabilities in legal technology systems); Marcelo Triana, *Is Selling Malware a Federal Crime?*, 93 N.Y.U. L. REV. 1311, 1313 (2018) (discussing malware sales that complicate the implementation of Computer Fraud and Abuse Act).

82. Gareth Norris, Alexandra Brookes & David Dowell, *The Psychology of Internet Fraud Victimisation: A Systematic Review*, 34 J. POLICE & CRIM. PSYCHOL. 231, 237 (2019).

83. Masmoudi, *supra* note 80, at 42.

84. Tianhao Xu & Prashanth Rajivan, *Determining Psycholinguistic Features of Deception in Phishing Messages*, 31 INFO. & COMPUT. SEC. 199, 200 (2023).

85. *See* Jonathan Lusthaus, *Reconsidering Crime and Technology: What Is This Thing We Call Cybercrime?*, 20 ANN. REV. L. & SOC. SCI. 369, 380 (2024).

86. Jildau Borwell, Jurjen Jansen & Wouter Stol, *The Psychological Impact of Cybercrime Victimization: The Importance of Personal and Circumstantial Factors*, 22 EUR. J. CRIMINOLOGY 1 *passim* (2025).

87. Norris, Brookes & Dowell, *supra* note 82, at 234–35.

respect for authority.[88] Even individuals with significant technical expertise can be snared by these cognitive biases,[89] implying that human beings remain the "weakest link"[90] if psychological factors go unaddressed.

The use of emerging technology to deceive individuals has proliferated in both volume and sophistication.[91] With social engineering now widely used to manipulate individuals into divulging confidential information for fraudulent purposes, certain demographics are especially vulnerable.[92] This challenge requires strong cybersecurity legislation alongside ongoing public education and awareness campaigns to help people recognize and avoid common threats. Because many crimes occur at this intersection of technology and human vulnerability, criminal law, consumer protection laws, and frameworks are central to reducing risk and harm.[93] While traditional anti-fraud statutes offer a crucial legal foundation, they may need to be updated or reinterpreted to encompass digital-age crimes.[94] Furthermore, legal frameworks must ensure that victims have access

---

88. Xu & Rajivan, *supra* note 84, at 212.

89. *See* Craig Grimestad, *The Psychology of Cybercrime: Do Not Trust Until Verified*, RIMPA Q. NOV. 2019, at 17, 17 (Austl.).

90. Eur. Union Agency for L. Enf't Coop., *Internet Organised Crime Threat Assessment (IOCTA) 2023,* at 7, PUBL'S OFF. OF THE EUR. UNION (July 2023) https://www.europol.europa.eu/publication-events/main-reports/internet-organised-crime-threat-assessment-iocta-2023 [https://perma.cc/EES5-BN5R] (Lux.).

91. *See supra* Part II.A.

92. *See generally* Eur. Union Agency for L. Enf't Coop., *supra* note 90 (discussing social engineering in the employment context). *See also* Button, Mark, Vasileios Karagiannopoulos, Julak Lee, Joon Bae Suh & Jeyong Jung, *Preventing Fraud Victimisation Against Older Adults: Towards a Holistic Model for Protection*, 77 INT'L J. L., CRIME & JUST. 1, 2 (2024) (reviewing evidence and narratives around vulnerability of older adults to fraud); Havers, Benjamin, Kanika Tripathi, Amy Burton, Sally McManus & Claudia Cooper, *Cybercrime Victimisation Among Older Adults: A Probability Sample Survey in England and Wales*, 19 PLOS ONE art. no. e0314380, at 2 (2024) (defining 'social-engineering' as tricking someone into disclosing information needed to acess a variety of apps and web-services).

93. *See* Susilowati Suparto et al., *Consumer Protection of Girls from Cybercrime in a Gender Perspective*, 5 J.L. & LEGAL REFORM 2045, 2051–56 (2024).

94. *See* Lusthaus, *Reconsidering Crime and Technology*, *supra* note 85, at 380.

to appropriate remedies, including compensation for financial losses and psychological harm.[95] This is especially urgent given the increasing frequency of online scams, identity theft, and fraud,[96] all of which demand laws that are responsive to the evolving nature of cybercrime, in order to ensure greater safety in online commerce.

C. Anonymity and Complexity in Attribution and Detection

The legal framework for cybersecurity must address the intricate challenges of attribution and detection in cyberspace. The anonymity provided by the Internet is an important feature that distinguishes cybercrime from traditional forms of criminal activity.[97] Anonymity allows cybercriminal's illegal efforts to thrive.[98] It is argued that the

---

95. The argument learns insights from other areas of law that have developed victim-centered approaches, such as legal frameworks addressing human trafficking and domestic violence. These areas emphasize the importance of not only prosecuting offenders but also ensuring that victims receive adequate protection, compensation, and psychological support. Similar principles could inform how we design remedies for victims of cybercrime. *See* Julio Montanez & Amy Donley, *Against the Clock: Crime Victim Compensation Law and Temporality Across the 50 United States*, CRIME & DELINQ., at 2 (Feb. 5, 2024) ("Crime Victim Compensation . . . has a connection with public policy, social control, and the body . . . uses physical and psychological injury and disability, indicators of body and mind, to, in part, ground claims for compensation."); *see also* Fakhrul Islam, *Human Trafficking Law Enforcement Over the Victims and Offenders: The Perspective of Anti-Trafficking Stakeholders*, 19 VICTIMS & OFFENDERS 1512, 1512 (2024) (examining the effects of compensation and rehabilitation in legal frameworks).

96. Milind Tiwari, You Zhou, Paul Gilmour & Ausma Bernot, *Confronting Metacrime: Complexities, Enforcement Challenges, and Regulatory Pathways*, 17 LAW, INNOV. & TECH. 159, 162 (2025) (documenting escalating "sophistication, diversity, and frequency" of threats in immersive online environments and detailing fraud vectors that signal an evolving cybercrime landscape); Cassandra Cross & Thomas J. Holt, *Beyond Fraud and Identity Theft: Assessing the Impact of Data Breaches on Individual Victims*, J. CRIME & JUST. at 19 (July 17, 2025) (describing rising incident volumes and growing cyber attack cadence, noting that "data breaches . . . are increasing globally as are the number of victims affected").

97. JONATHAN LUSTHAUS, INDUSTRY OF ANONYMITY: INSIDE THE BUSINESS OF CYBERCRIME 5 (2018).

98. ALEXANDROU, *supra* note 17, at 89.

ability to conceal one's identity online permits cybercriminals to collaborate with others while remaining anonymous.[99]

This anonymity affects trust and accountability, both in general and within cybercriminal networks.[100] There is a dilemma faced by cybercriminals: They must strike a balance between staying anonymous and creating an online persona that allows them to collaborate, all the while avoiding detection by law enforcement.[101] Anonymity has not prevented cybercriminals from forming sophisticated and organized networks.[102] After takedowns, they migrate to new forums, increasing complexity of their operations and presenting challenges for law enforcement to investigate.[103]

Regarding the tactics used to hide identities, recent studies indicate that cybercriminals continue to employ conventional techniques, including virtual private networks ("VPNs"), encrypted messaging, and the dark web, but with enhanced sophistication due to technological advancements.[104] Jain et al. note that while VPNs and Tor

---

99. *See* LUSTHAUS, *supra* note 97, at 69.

100. *Id.* at 114–15.

101. *See id.* at 96, 105–06.

102. *Id.* at 197.

103. *Id.*

104. Pieter Hartel & Rolf van Wegberg, *Going Dark? Analyzing the Impact of End-to-End Encryption on the Outcome of Dutch Criminal Court Cases*, 12 CRIME SCI. art. no. 5, 2023, at 2–3 (detailing how cybercriminals leverage E2EE tools and platform vulnerabilities such as Phantom Secure, Ennetcom, EncroChat, Sky ECC, while law enforcement adapts with exploits, infiltration, server seizures, and device-level tactics, illustrating technology-driven escalation on both sides.); *see also* Vikas Kumar Jain et al., *Unmasking the True Identity: Unveiling the Secrets of Virtual Private Networks and Proxies*, 16 INFO. 126, 126 (2025) (Switz.) (showing contemporary deception tooling like VPNs/proxies); Danish Nisarahmed Tamboli & Shaliesh Pramod Bendale, *Crowdfunded Assassinations and Propaganda by Dark Web Cyber Criminals*, *in* DARK WEB PATTERN RECOGNITION AND CRIME ANALYSIS USING MACHINE INTELLIGENCE 74, 79–80 (Romil Rawat et al. eds., 2022) (explaining that propaganda long predates the internet, which now accelerates falsehoods via insecure, novel channels, social platforms, hacked databases, and news sites, constituting cyber propaganda); Keshav Kaushik, *Dark Web: A Playground for Cyber Criminals*, 2 COMPUTOLOGY: J. APPLIED COMPUT. SCI. & INTELLIGENT TECHS. 44, 45–46 (2022) (India) (describing the Dark Web as a haven for international criminals and details how technologies such as the Tor network facilitate anonymity through layered encryption).

browsers[105] enhance user privacy, they are also "exploited by cybercriminals to obscure their identities,"[106] and shield the acts of "those distributing child abuse content, selling or buying illicit drugs, or sharing malware online,"[107] making it difficult to trace the real IP addresses behind the anonymization. This creates significant challenges for traditional detection methods, which often cannot penetrate these layers of disguise,[108] leaving law enforcement with limited means to track offenders.[109]

Secure messaging apps (e.g., Telegram, Signal, and WhatsApp) with end-to-end encryption ("E2EE") enable criminals to communicate covertly.[110] Law enforcement agencies warn that widespread encryption hampers their ability to attribute communications to suspects, a challenge often dubbed the "going dark" problem.[111] Hartel and van Wegberg observe that E2EE "hampers attribution and prosecution of criminals who rely on encrypted communication," complicating investigations of offenses ranging from drug trafficking to child exploitation.[112] In some cases, even when police have the authority to intercept data, strong encryption prevents

---

105. Tor (The Onion Router) is a free, open-source network that enables anonymous communication by routing internet traffic through multiple encrypted relays to protect users' privacy and bypass censorship. *See* Eric Jardine, Andrew M. Lindner & Gareth Owenson, *The Potential Harms of the Tor Anonymity Network Cluster Disproportionately in Free Countries*, 117 PNAS 31716, 31716 (2020).

106. Jain et al., *supra* note 104, at 126.

107. Jardine, Lindner & Owenson, *supra* note 105, at 31716.

108. *See id.*

109. *See* VINNY TROIA, HUNTING CYBER CRIMINALS: INVESTIGATIONS AND THREAT ACTORS 19 (Rhia Dancel ed., Wiley 2020).

110. Ahmad Shehabat, Teodor Mitew & Yahia Alzoubi, *Encrypted Jihad: Investigating the Role of Telegram App in Lone Wolf Attacks in the West*, 10 J. STRATEGIC SEC. 27, 27 (2017).

111. Hartel & van Wegberg, *supra* note 104, at 1.

112. *Id.* at 6. Hartel & van Wegberg note that:

> Offenders and the police are engaged in an ongoing battle. As soon as one wins, the other tries to nullify that lead. E2EE gives the offender a head start, and the question is to what extent the special powers of the police can cope.

Id.

them from accessing the content of a suspect's messages.[113] Scholars also discuss law enforcement's options to tackle encryption, which include: obtaining the passcode directly from the suspect (though not under duress),[114] using biometric identification,[115] and employing specialized tools to bypass the passcode.[116]

Adding to the complexity of the anonymity challenge, the dark web marketplaces allow "hidden customers" to buy from "hidden sellers" with relative confidence, using cryptocurrencies to further obscure identities which "often keeps law enforcement at bay."[117] While anonymity networks may pose more risks than benefits overall,[118] scholars caution that a complete takedown of the dark web or Tor browsers could lead to unintended consequences. These include

---

113. In this case, lawful interception may be legally permitted, but technically ineffective due to encryption. *See id.* at 1.

114. Catherine O'Rourke, *Is This the End for 'Encro' Phones?*, 2020 COMPUT. FRAUD & SEC. 8, 8 (2020).

115. SECOND REPORT OF THE OBSERVATORY FUNCTION ON ENCRYPTION, EUROPOL. & EUROJUST. 12–15, https://www.europol.europa.eu/publications-documents/second-report-of-observatory-function-encryption [https://perma.cc/43RK-LRWU] (last updated Dec. 7, 2021).

116. For instance, in the San Bernardino iPhone 5C case, where the FBI paid over $1 million for access, and installed key logger malware under a magistrate's permission to capture the passcode. *See* NAT'L ACADS., DECRYPTING THE ENCRYPTION DEBATE: A FRAMEWORK FOR DECISION MAKERS 51 (NAT'L ACADS. PRESS 2018); Steven David Brown, *Hacking for Evidence: The Risks and Rewards of Deploying Malware in Pursuit of Justice*, 20 ERA F. 423, 423–24 (2020).

117. *Taking on the Dark Web: Law Enforcement Experts ID Investigative Needs*, NAT'L INST. OF JUST. (June 15, 2020), https://nij.ojp.gov/topics/articles/taking-dark-web-law-enforcement-experts-id-investigative-needs[https://perma.cc/9MXN-AQH2].

118. Jardine, Lindner & Owenson, *supra* note 101, at 31716; *see also* Gemma Davies, *Shining a Light on Policing of the Dark Web: An Analysis of UK Investigatory Powers*, 84 J. CRIM. L. 407, 408 (2020) (highlighting the most common type of content requested via Tor: child pornography and black marketplaces). In the above report by the U.S. Department of Justice, there is a section explaining the rapid growth of dark web tools used for illicit transactions: The criminal side of the dark web relies on anonymizing technology and cryptocurrency to hide its trade in an assortment of contraband such as opioids and other drugs, bomb parts, weapons large and small, child pornography, social security numbers, body parts—even criminal acts for hire. *See id*

reduced trust in the internet's neutrality, which can negatively affect online transactions;[119] undermining privacy when there is a need to protect sensitive communications of security researchers or companies;[120] and disrupting innovation,[121] such as by preventing the development of blockchain-based services that underpin the future of fintech and e-commerce. As a result, certain cyber threats may be harder to detect and monitor if they spill over into mainstream online marketplaces, which in turn increases security costs for legitimate businesses.[122]

In responding to the complexity in attribution and detection of anonymous cybercriminals, scholars and policymakers advocate for a multi-modal regulatory approach that integrates legal, technological, market, and community-driven responses.[123] In Australia, for example, the introduction of the Assistance and Access Act 2018[124] prompted concerns over the tightening of enforcement measures against encrypted communication.[125] The concept of the "disruption calculus"

---

119. *See* Kristina Radivojevic et al., *Dark Web and Internet Freedom: Navigating the Duality to Facilitate Digital Democracy*, 9 J. CYBER POL'Y 300, 300 (2024) (U.K.).

120. Chandrika Nath & Thomas Kriechbaumer, *The Darknet and Online Anonymity,* PARL. OFF. SCI. & TECH. (Mar. 2015), https://researchbriefings.files.parliament.uk/documents/POST-PN-488.pdf[https://perma.cc/EKD4-EQB2 (staff-uploaded)].

121. *See* Brendan Walker-Munro, *A Shot in the Dark: Australia's Proposed Encryption Laws and the "Disruption Calculus*," 40 ADEL. L. REV. 783, 792–94 (2019) (Austl.).

122. *See* Yvon Dandurand, *Law Enforcement Strategies to Disrupt Illicit Markets*, GLOB. INITIATIVE AGAINST TRANSNAT'L ORGANIZED CRIME 9 (Aug. 27, 2023), https://globalinitiative.net/wp-content/uploads/2024/02/Yvon-Dandurand-Law-enforcement-strategies-to-disrupt-illicit-markets-GI-TOC-August-2023.pdf [https://perma.cc/75LA-FDYH].

123. Walker-Munro, *supra* note 121, at 804.

124. *Assistance and Access Act 2018* (Cth.) (Austl.).

125. Keiran Hardy, *Australia's Encryption Laws: Practical Need or Political Strategy?*, 9 INTERNET POL'Y REV. 1, 2–4 (2020) (Eur.); *see* Peter Alexander Earls Davis, *Decrypting Australia's 'Anti-Encryption' Legislation: The Meaning and Effect of the 'Systemic Weakness' Limitation*, 44 COMPUT. L. & SEC. REV. 105659, 105659 (2022); *see also* Rick Sarre, *Revisiting Metadata Retention in Light of the Government's Push for New Powers*, DAILY BULLETIN (June 8, 2018), https://www.dailybulletin.com.au/the-conversation/38301-revisiting-metadata-retention-in-light-of-the-government [https://

footnote continued on next page

was proposed to highlight the need for a more comprehensive strategy that allows for the combination of regulatory interventions with technology companies.[126] This increased cooperation has the potential to promote more effective legal access methods while ensuring the privacy of businesses conducting business. One best-practice example is Israel, which incentivizes compliance through licensing benefits and market access.[127]

A recurring issue is the need for a clear legal framework when using intervention tools, such as malware, to de-anonymize identities or individuals involved in government criminal investigations.[128] In the U.S., the lesson of "encryption workaround" in many criminal investigations has been documented by Kerr and Schneier.[129] These authors suggest that the legal measures for addressing online anonymity and encryption focus on clarifying the scope of authority to compel individuals and third-party companies to assist with decryption or encryption bypass.[130] They emphasize that legal frameworks for these actions remain underdeveloped, and ongoing debates about balancing privacy and law enforcement needs do not add clarity to the issue.[131] Use of such tools[132] requires a well-defined legal framework and an effective advocacy strategy to raise public awareness about the transparency of these activities. Bercovitz and

---

perma.cc/ZR5Y-YDPG] (revisiting the history of Australia's government mandated collection of metadate).

126. Walker-Munro, *supra* note 121, at 784.

127. *See id.* at 811.

128. Orin S. Kerr & Sean D. Murphy, *Government Hacking to Light the Dark Web: What Risks to International Relations and International Law?*, 70 STAN. L. REV. ONLINE 58, 60 (2017); *see also* Ahmed Ghappour, *Searching Places Unknown: Law Enforcement Jurisdiction on the Dark Web*, 69 STAN. L. REV. 1075, 1075 (2017) (advocating for a novel regulatory framework that shifts decision-making from rank-and-file officials to institutional actors who are better prepared to balance the competing interests of foreign policy and law enforcement).

129. Orin S. Kerr & Bruce Schneier, *Encryption Workarounds*, 106 GEO. L.J. 989, 989 (2018).

130. *See id.* at 1000, 1012.

131. *Id.* at 1019.

132. Examples of these tools are the Network Investigative Techniques ("NITs") in the U.S and Equipment Interference specified in the Investigatory Powers Act 2016 in the UK. *See* Davies, *supra* note 113, at 418.

Mayer, for example, both emphasize that the deployment of malware by police should be subject to strict conditions, including notice requirements, duration limits, and oversight to protect privacy.[133]

The collaboration between governments, states, and technology corporations alone is no longer sufficient to tackle the growing complexity of anonymity in cybercrime.[134] To improve law enforcement effectiveness, stronger collaboration is needed, including mutual legal assistance agreements and reinforced cross-border legal frameworks.[135] Mayer highlights the growing desire to integrate privacy-protecting technology into law enforcement efforts.[136] In order to avoid overly broad measures that may undermine trust in the digital ecosystem, governments should focus more on fostering innovation in privacy technologies while maintaining lawful access pathways.[137] Finally, technical solutions, such as honeypots[138] and Canarytokens,[139] provide non-intrusive means of unmasking anonymized users, allowing law enforcement to identify offenders without violating privacy and while remaining in compliance with legal norms.[140]

---

133. Rachel Bercovitz, *Law Enforcement Hacking: Defining Jurisdiction*, 121 COLUM. L. REV. 1251, 1285 (2021); *see also* Jonathan Mayer, *Government Hacking*, 127 YALE L.J. 570, 581 (2018) (arguing for stricter procedures and oversight of government hacking).

134. Hartel & van Wegberg, *supra* note 104, at 8 (observe that despite improved information access through online and offline surveillance, law enforcement still faces significant challenges in investigating crimes involving end-to-end encryption (E2EE). Their study on Dutch court cases concludes that while courts can effectively prosecute offenders without breaking encryption, law enforcement outcomes remain inconclusive).

135. *See* LUSTHAUS, *supra* note 97, at 179 (discussing a few examples on how transnational anonymous cybercriminals exploit jurisdictional complexity and dispersed servers).

136. *See* Mayer, *supra* note 133, at 641–43.

137. *See id.* at 659.

138. A honeypot is a deceptive computer system designed to attract cybercriminals, allowing organizations to gather information about potential threats without directly addressing specific security issues. *See* Jain et al., *supra* note 104, at 6.

139. Canarytokens are concealed triggers embedded in digital assets that alert the creator with details like the attacker's IP address and timestamp when activated, helping to detect unauthorized access. *See id.*

140. *Id.*

Collectively, these legal and technical solutions offer a more comprehensive, balanced response to the complex issue of online anonymity.

D. The Global and Borderless Nature of Cybercrime

One of the most defining characteristics of cybercrime is its ability to transcend geographical boundaries.[141] As various studies highlight, cybercrime has become a global phenomenon, with cybercriminals in one country frequently targeting victims in others.[142] For instance, United States citizens lost an estimated $3.5 billion to scams in 2023 alone, with many scams traced to operations based in Cambodia and Myanmar.[143] More significantly, criminal organizations from China are able to operate internationally by using front companies, advanced technology,[144] and fake identities to run illegal gambling sites that

---

141. *See* MAJID YAR & KEVIN F. STEINMETZ, CYBERCRIME AND SOCIETY 14 (3rd ed. 2019); *see also* PETER N. GRABOSKY & RUSSELL G. SMITH, CRIME IN THE DIGITAL AGE: CONTROLLING TELECOMMUNICATIONS AND CYBERSPACE ILLEGALITIES 9 (1998) (analyzing the criminal opportunities which accompany technological changes including illegal interception of telecommunications); DAVID WALL, CYBERCRIME: THE TRANSFORMATION OF CRIME IN THE INFORMATION AGE 38 (2007) (describing how the internet has transformed criminal behavior, as well as the differences between cybercrime and traditional criminal activities).

142. *See* Peter Grabosky & Roderic Broadhurst, *Computer-Related Crime in Asia: Emergent Issues, in* CYBER CRIME: THE CHALLENGE IN ASIA 1 (Roderic Broadhurst & Peter Grabosky eds., 2005); *see also* NIGEL PHAIR, CYBERCRIME: THE REALITY OF THE THREAT 153 (2007) (explaining the dangers cyber-crimes pose); SUSAN W. BRENNER, CYBERCRIME: CRIMINAL THREATS FROM CYBERSPACE 135 (2010) (discussing the same).

143. *See* Press Release, *Treasury Sanctions Burma Warlord and Militia Tied to Cyber Scams, Human Trafficking, and Cross-Border Smuggling*, U.S. DEP'T TREASURY (2025), https://home.treasury.gov/news/press-releases/sb0129 . *See also* Julia Dickson & Lauren Burke Preputnik, *Cyber Scamming Goes Global: Unveiling Southeast Asia's High-Tech Fraud Factories*, CTR. FOR STRATEGIC & INT'L STUD. (Dec. 12, 2024), https://www.csis.org/analysis/cyber-scamming-goes-global-unveiling-southeast-asias-high-tech-fraud-factories [https://perma.cc/5CER-QAQT].

144. There has been ongoing analysis on how digital technology, especially AI-driven systems playing as dealers, are used to enhance the effectiveness of gaming while causing local laws and regulations to constrain. *See* IpKin

footnote continued on next page

attract victims worldwide.[145] The cross-border nature of cybercrime poses a huge issue for law enforcement agencies, as they normally work within their own country's boundaries.[146] Because there is currently no centralized or global police agency dedicated to cybercrime, criminals can exploit national borders to avoid prosecution and continue their unlawful activities.[147] Law enforcement's jurisdictional constraints lead to gaps in enforcement and regulation,[148] leaving victims vulnerable across borders.

The growing interconnectedness of global markets and commercial activities adds another layer of complexity to the legal landscape. Safe and open internet platforms are critical for effective online financial, e-commerce and customer interactions.[149] However,

---

Anthony Wong, Keng Fong Chau & Heng U. Chan, *An Empirical Study on Customers' Gambling Intention in AI-Supported Casinos*, 14 J. HOSP. & TOURISM TECH. 121, 122 (2023) (arguing that AI has altered the way consumers approach gambling); *see also* Matthew Tingchi Liu, Shiying Dong & Mingxia Zhu, *The Application of Digital Technology in Gambling Industry*, 33 ASIA PAC. J. MKTG. & LOGISTICS 1685, 1700 (2021) (explaining how AI has major implications for the gambling industry); Julia Hörnle et al., *Regulating Online Advertising for Gambling – Once the Genie Is Out of the Bottle*, 28 INFO. & COMMC'N TECH. L. 311, 312 (2019).

145. U.N. OFF. ON DRUGS & CRIME, Casinos, Money Laundering, Underground Banking, and Transnational Organized Crime in East and Southeast Asia: A Hidden and Accelerating Threat 5 (2024), https://www.unodc.org/roseap/uploads/documents/Publications/2024/Casino_Underground_Banking_Report_2024.pdf [https://perma.cc/555T-4P6M].

146. Brenner & Koops, *supra* note 4, at 135–36.

147. For example, in the most recent on-going case involving an online scam center, Vietnamese police lacked the legal authority to arrest the scammers in Cambodia due to the absence of a legal assistance agreement between the two countries. As a result, the authorities had to wait until the criminals returned to Vietnam to apprehend them. *Female Mastermind Behind US$40 Million Fraud in Vietnam Arrested*, ASIA NEWS NETWORK (Jan. 28, 2025), https://asianews.network/female-mastermind-behind-us40-million-fraud-in-vietnam-arrested/ [https://perma.cc/EF6Z-6KXR].

148. Andrew Teng**,** Jurisdictional Barriers: Cybercrime Prosecution Challenges 47 (2017) (Capstone paper, Utica College) (on file with Utica College).

149. Anahiby Becerril, *Cybersecurity and E-Commerce in Free Trade Agreements*, 13 MEX. L. REV. 3, 6–8 (2020); *see* Aaron Lerman, *Remnants of Net Neutrality: Policing Unlawful Content Through Broadband,* 12 BROOK. J. CORP. FIN. &

footnote continued on next page

the free flow of online commerce can be limited by overly rigid cybersecurity regulations or inconsistent cybersecurity regulations across countries. For example, access to specific platforms can be restricted by strict national cybersecurity policies while international commercial operations can be restricted by laws requiring data storage within national boundaries.[150] The EU's General Data Protection Regulation ("GDPR") has been criticized for its stringent requirements, which can impede cross-border trading.[151]

Data localization requirements across different nations can create barriers that limit how companies operate in international markets.[152] Pioneering scholars on the relationship between cybersecurity and e-commerce emphasize that while cybersecurity regulations are necessary to ensure security and legal certainty, they must not create barriers that limit economic growth and electronic commerce.[153] Cybersecurity laws must be carefully designed, because overly restrictive policies or measures can become possible trade barrier, preventing the openness of the internet which directly affects global e-commerce. While the openness of the internet is crucial for innovation and global trade, this can be undermined by overly strict

---

COM. L. 363, 366–67 (2018); David Stein, *Data Insecurity Law*, 39 SANTA CLARA HIGH TECH. L.J. 445, 450 (2023); *see also* Lina M. Khan, *The Separation of Platforms and Commerce*, 119 COLUM. L. REV. 973, 1081–82 (2019) (observing how businesses rely on dominant platforms as central markets to reach consumers and conduct transactions); Kosseff, *supra* note 65, at 53.

150. Becerril, *supra* note 149, at 9.

151. Iskander Sanchez-Rola et al., *Can I Opt Out Yet? GDPR and the Global Illusion of Cookie Control*, *in* 14th ACM Asia Conference on Computer & Communications Securirty (AsiaCCS '19), July 7–12, 2019, Auckland, New Zealand 340; *see also* Connor Luckett et al., *Odlaw: A Tool for Retroactive GDPR Compliance*, in 2021 IEEE 37TH INT'L CONF. ON DATA ENG. passim (ICDE) (2021) (discussing an argument that the best way to comply with the GDPR is to work retroactively with 3rd party tools).

152. *See* Michael R. Kenwick, Beth A. Simmons & Richard J. McAlexander, *Infrastructure and Authority at the State's Edge: The Border Crossings of the World Dataset*, 61 J. PEACE RSCH. 500, 508 (2024) (discussing how states increasingly invest in filtering mechanisms to control cross-border transactions, signaling a trend toward regulatory fortification that impacts trade and data flows).

153. Becerril, *supra* note 149, at 29.

or inconsistent regulations.[154] However, existing research is limited to analyzing the cybersecurity policies and strategies of selected trade-oriented countries, highlighting the diverse approaches to the concept of cybersecurity. The criteria for assessing the effectiveness of cybercrime and cybersecurity legislation have received insufficient attention in efforts to strike a balance between promoting trade and protecting against cyber threats.

Perhaps clearer legal criteria are needed, along with greater coordination between technological, economic, and legal experts, to address the global nature of cybercrime. The central question, then, is how to create a legal framework that enhances cybersecurity without risking the commercial need for an open and accessible internet. Achieving this requires not only international cooperation but also thoughtful regulation that does not unduly constrain legitimate commercial activities.

III. Established Criminal Law Theories and Their Limitations when Applied to Cybercrime

A. Overview

To develop criteria for what constitutes effective cybercrime law, it is useful to begin by considering existing legal scholarship on criminal theory and its application to cybercrime and cybersecurity. The ultimate functions of criminal law are both retributive and preventive.[155] To explore these functions in the context of cybercrime, this Section examines well-established criminal theories to identify key criteria for addressing such offenses. Criminal law theory focuses on the justification and purpose of criminal legislation, namely how society should define, prosecute, and punish illegal behaviors.[156] At the

---

154. *See id.*

155. *See* Guyora Binder & Robert Weisberg, *What Is Criminal Law About?*, 114 Mich. L. Rev. 1173, 1175 (2016).

156. *See* Mark Dsouza, Alon Harel & Re'em Segev, *Criminal Law Theory: Introduction*, 18 Crim. L. & Phil. 493, 493–94 (2024); *see also* Nina Persak, *Criminal Law, the Victim and Community: The Shades of 'We' and the Conceptual Involvement of Community in Contemporary Criminal Law Theory*, 8 Crim. L. & Phil. 205, 206 (2014) (explaining the importance of including community as an actor in criminal law).

heart of this field is the debate between retributivism, which emphasizes punishment as a moral response to wrongdoing,[157] and consequentialism, which justifies punishment based on its social utility, such as deterrence or rehabilitation.[158]

Modern criminal law theory frequently reflects a blend of these views, attempting to balance moral culpability with broader societal aims such as crime prevention.[159] These foundations of criminal law theory are crucial, as they offer a framework for understanding, preventing, and prosecuting crimes in the rapidly evolving technological landscape. For the purposes of doctrinal analysis, revisiting the most dominant criminal law theories—deterrence theory, retributive justice, restorative justice, and utilitarianism—will aid in redefining and categorizing new forms of illegal behaviors that existing criminal law struggles to address,[160] and ensure that any recommendation for law reform is firmly grounded in sound legal principles.

B. Deterrence Theory in Cybercrime Prevention

Deterrence theory is a fundamental concept in criminal law, rooted in the principle of rational choice[161] which influences the offender's decision-making process. This principle suggests that individuals make decisions based on a calculated cost-benefit analysis.[162] The theory posits that crime can be mitigated when

---

157. Darryl K. Brown, *Criminal Law Theory and Criminal Justice Practice*, 49 AM. CRIM. L. REV. 73, 77–78 (2012).

158. *Id.* at 74; *see* EMMANUEL MELISSARIS, THEORIES OF CRIME AND PUNISHMENT, THE OXFORD HANDBOOK OF CRIMINAL LAW 355, 374 (Markus D. Dubber & Tatjana Hörnle eds., 2014).

159. Brown, *supra* note 157, at 86; Malcolm Thorburn, *Introduction: Criminal Law Theory*, 70 U. TORO L.J. 1, 2 (2020).

160. Dominic Wood et al., *Cybercrime and Digital Policing, in* BLACKSTONE'S HANDBOOK FOR POLICING STUDENTS 522, 522 (19th ed. 2025).

161. David Décary-Hétu et al., *"Like Aspirin for Arthritis:" A Qualitative Study of Conditional Cyber-Deterrence Associated with Police Crackdowns on the Dark Web*, 22 CRIMINOLOGY & PUB. POL'Y 639, 640–41 (2023).

162. Marcus Felson, *Linking Criminal Choices, Routine Activities, Informal Control, and Criminal Outcomes*, *in* THE REASONING CRIMINAL: RATIONAL CHOICE PERSPECTIVES ON OFFENDING 119–20 (Derek B. Cornish & R.V.G. Clarke eds., 1986).

punishment is certain, severe, and with celerity.[163] Some scholars have observed that this theory forms the foundation of most Western criminal justice systems, and informs modern punitive approaches toward offenders.[164] By emphasizing the deterrence of undesirable behaviors through the threat of negative consequences,[165] deterrence theory assumes that rational individuals will avoid actions they perceive as having greater costs than benefits.[166] Although often criticized for relying on subjective perception rather than objective reality,[167] deterrence theory remains one of the most significant frameworks for understanding criminal behaviors.[168] Originating from Cold War nuclear strategy, it was initially intended to prevent warfare by leveraging threats of severe retaliation or producing fear of attack,[169] particularly in the context of nuclear conflict.[170]

Deterrence application in criminal law involves both general deterrence, which aims to prevent the general population from engaging in crime by instilling fear of legal consequences, and specific deterrence, which focuses on discouraging individuals who have

163. John M. Eassey & John H. Boman IV, *Deterrence Theory, in* THE ENCYCLOPEDIA OF CRIME AND PUNISHMENT 483–89 (Wesley G. Jennings ed., 2015); *see also* Jack P. Gibbs, *Crime, Punishment, And Deterrence*, S.W. SOC. SCI. Q. 515, 523 (1975) (explaining the theory of deterrence in criminal law).

164. THOMAS J. HOLT & ADAM M. BOSSLER, CYBERCRIME IN PROGRESS: THEORY AND PREVENTION OF TECHNOLOGY-ENABLED OFFENSES 75 (2016).

165. Raymond Paternoster, *How Much Do We Really Know About Criminal Deterrence*, 100 J. CRIM. L. & CRIMINOLOGY 765, 766 (2010); Joseph S. Nye, Jr., *Deterrence and Dissuasion in Cyberspace*, 41 INT'L SEC. 44, 52 (2017).

166. *See* Paternoster, *supra* note 165, at 782 ("Deterrence theory is a theory of crime that presumes that human beings are rational enough to consider the consequences of their actions and to be influenced by those consequences.").

167. Karl Sörenson, *Prospects of Deterrence: Deterrence Theory, Representation and Evidence*, 35 DEF. & PEACE ECON. 145, 145 (2024).

168. Eassey & Boman IV, *supra* note 163, at 488.

169. ERIK GARTZKE & JON R. LINDSAY, ELEMENTS OF DETERRENCE: STRATEGY, TECHNOLOGY, AND COMPLEXITY IN GLOBAL POLITICS 2 (2024).

170. *Id.* at 17, 18; *see* Nye, Jr., *supra* note 165, at 45.

previously committed crimes from reoffending.[171] In the context of cyber-criminal behavior, deterrence theory can be interpreted as seeking to prevent malicious cyber activities by discouraging adversaries through conditions where the costs of cyber-attacks outweigh their benefits.

As a cornerstone of criminal law, how can deterrence theory strengthen contemporary cybercrime legislation? Deterrence principles have been recognized as a powerful tool in combating cybercrime, offering a framework to effectively discourage malicious cyber activities from individual actors and groups,[172] by imposing multifaceted costs on attackers,[173] enhancing legal measures,[174] and communicating credible retaliation strategies.[175] According to Fischer, effective deterrence in cyberspace requires integrating denial measures, such as building robust defenses and resilient systems, alongside lawful responses to cyber-attacks[176] that are tailored to discourage adversaries by affecting their cost-benefit analysis. Deterrence can be effective when law enforcement or governments make concerted efforts to demonstrate their capabilities to deter cyberattacks by leveraging different strategies, including punishment and cross-domain deterrence.[177] Publicized arrests or indictments of cybercriminals may have a deterrent effect,[178] particularly on those less

---

171. *See* Paternoster, *supra* note 165, at 775; Mark C. Stafford, *Deterrence Theory: Crime*, *in* INTERNATIONAL ENCYCLOPEDIA OF THE SOCIAL & BEHAVIORAL SCIENCES 255, 255 (James D. Wright ed., 2015).

172. Sean D. Carberry, *Why There's No Silver Bullet for Cyber Deterrence*, NEXTGOV (June 6, 2017) https://www.nextgov.com/cybersecurity/2017/06/software-vulnerability-researcher-finds-ways/144087/ [https://perma.cc/2KRQ-Q7W6] ("Unlike nuclear deterrence, which deals with relatively few actors and variables, cyber deterrence requires addressing a wide range of threats, actors, unknown capabilities and escalation potentials, said James Miller, former undersecretary of defense for policy.").

173. Manuel Fischer, *The Concept of Deterrence and Its Applicability in the Cyber Domain*, 18 CONNECTIONS: Q. J. 69, 74 (2019) (Eng.).

174. *See id.* at 73 (Explaining how changing the calculus by increasing the probability that an adversary would lose value can be a powerful defensive mechanism).

175. *Id.*

176. *Id.* at 84–85.

177. Erica Lonergan & Mark Montgomery, *What Is the Future of Cyber Deterrence?*, 41 SAIS REV. INT'L AFFS. 61, 65 (2021).

178. *Id.* at 67.

motivated to avoid detection.[179] Nevertheless, numerous scholars argue that deterrence in cyberspace is less about preventing attacks entirely and more about limiting their scope and severity.[180]

In developing a theoretical model for an effective cybercrime law, deterrence theory offers principles that can enhance legal frameworks by shaping provisions that discourage cybercriminal behavior. These principles are: (a) certainty of consequences; (b) severity of penalties; and (c) celerity of enforcement. Applying these principles to cyber defense strategies emphasizes the need for sanctions that are certain, severe, and swift enough[181] to outweigh the perceived benefits of crime. Deterrence by denial conveys certainty and credibility of retaliation to cyber attackers, while demonstrating a willingness to impose significant costs on attackers can dissuade malicious activities.[182] For instance, signaling a nation's cyber capabilities, even with imperfect attribution, can create a perceived risk for potential attackers, thereby reducing their willingness to act.[183] An effective deterrence strategy often involves making it difficult for cybercriminals to achieve their objectives while also maintaining the threat of punishment for acts

---

179. David Maimon, C. Jordan Howell & George W. Burruss, *Restrictive Deterrence and the Scope of Hackers' Reoffending: Findings from Two Randomized Field Trials*, 125 COMPUTS. HUM. BEHAV. art. no. 106943, at 4 (2021) (finding that low-skilled hackers reduced their misconduct after being warned by law enforcement).

180. *See* Lonergan & Montgomery, *supra* note 171, at 69; *see also* Michael P. Fischerkeller & Richard J. Harknett, *Deterrence Is Not a Credible Strategy for Cyberspace*, 61 ORBIS 381, 391 (2017) (arguing that counter subversion as a defense in cyberspace is about mitigation); Eugenio Lilli, *Redefining Deterrence in Cyberspace: Private Sector Contribution to National Strategies of Cyber Deterrence*, 42 CONTEMP. SEC. POL'Y 163, 166 (2021).

181. Mariarosaria Taddeo, *The Limits of Deterrence Theory in Cyberspace*, 31 PHIL. & TECH. 339, 345 (2018).

182. Jonathan Welburn, Justin Grana & Karen Schwindt, *Cyber Deterrence with Imperfect Attribution and Unverifiable Signaling*, 306 EUR. J. OPERATIONAL RSCH. 1399, 1400 (2023).

183. *Id.* at 1403; *see* Maria Keinonen & Kimmo Halunen**,** *Options for Signalling Cyber Deterrence Using Cyber Capabilities*, *in* PROCS. OF THE 19TH INT'L CONF. ON CYBER WARFARE & SEC. (ICCWS 2024) 463, 464 (2024).

that occur.[184] This dual approach is seen as complementary rather than mutually exclusive. Establishing international norms and stigmatizing cybercrimes can serve as a deterrent by increasing the reputational risks and penalties for state and non-state actors engaged in cyberattacks.[185]

Utilizing private sector contributions can also strengthen the deterrence framework by augmenting cyber defenses, enabling attribution, and increasing the consequences of harmful actions.[186] This is crucial since a significant portion of the cyber infrastructure is privately owned and managed.[187] Finally, recent discussions of deterrence theory in cyberspace indicate that integration of AI in strategic stability,[188] shared threat intelligence, cooperative law enforcement, and harmonized policies among nations may strengthen deterrence by increasing the likelihood of identifying and prosecuting cybercriminals across borders.[189]

However, deterrence theory is not suited to engage with the unique features of cybercrime, notably its seamless global nature, technical complexity, psychological underpinnings, and anonymity.[190] Researchers have long questioned how well deterrence works. For example, as discussed in Part II. the online environment presents a variety of unique challenges the application of criminal laws is

---

184. Annegret Bendiek & Tobias Metzger, *Deterrence Theory in the Cyber-Century: Lessons from a State-of-the-Art Literature Review*, STIFTUNG WISSENSCHAFT UND POLITIK [GER. INST. FOR INT'L & SEC. AFFS.] RSCH DIV. EU/EUR., at 6 (2025) https://www.swp-berlin.org/publications/products/arbeitspapiere/Bendiek-Metzger_WP-Cyberdeterrence.pdf [https://perma.cc/4MG4-E48U].

185. Lilli, *supra* note 180, at 175.

186. *Id.*

187. *Id.* at 170.

188. James Johnson, *Deterrence in the Age of Artificial Intelligence & Autonomy: A Paradigm Shift in Nuclear Deterrence Theory and Practice?*, 36 DEF. & SEC. ANALYSIS 422, 427–28 (2020).

189. Kai-Lung Hui, Seung Hyun Kim & Qiu-Hong Wang, *Cybercrime Deterrence and International Legislation: Evidence from Distributed Denial of Service Attacks*, 41 MIS Q. 497, 498, 519–20 (2017) (finding that enforcement of the Conventional on Cybercrime (Budapest Convention) reduces DDoS attacks by at least 11.8% in enforcing countries, and such deterrence effectiveness relies on international cooperation among nations).

190. *See* supra Part II.A.1.

substantially more complex, making deterrence less reliable in practice.[191] While in conventional settings, deterrence works by threatening punishments, in cyberspace, the deterrent effect is diluted by jurisdictional fragmentation, the anonymity of perpetrators, the absence of precise attribution,[192] and the potential rapid pace of cyberattacks.[193]

Criminals can mask their identity or operate across borders, making it harder for law enforcement agencies to track and punish them.[194] If attackers believe they can avoid detection or blame, deterrence strategies lose their efficacy.[195] This decreases the perceived likelihood of punishment, thus weakening the effectiveness of deterrence in the cyber realm.[196] There has been ongoing discussion suggesting that certain types of cybercrime may be challenging to deter using traditional criminal justice mechanisms.[197] Cyberattacks using AI are increasing in pace and complexity. Exploitative vulnerabilities are emerging more rapidly than defender's legal and

191. Lonergan & Montgomery, *supra* note 177, at 66.

192. Nye, Jr., *supra* note 165, at 49–52; Taddeo, *supra* note 181, at 343–44 (noting that "identifying the malware, the network of infected machines, or even the country of origin of the attack is not sufficient for attribution, as it is well known that attackers can design and route their operations through third-party machines and countries with the goal of obscuring or misdirecting attribution"); *see* Jim Chen, *Cyber Deterrence by Engagement and Surprise*, 7 PRISM 100, 102 (2017).

193. Chen, *supra* note 192, at 110.

194. A pertinent example is the 2024 ransomware attack on several London hospitals by the Russian-speaking cybercrime group Qilin, which led to cancelled surgeries, delayed test results, and leaked patient data. However, no members of the ransomware group have been publicly reported as arrested or prosecuted in connection with the cyberattack on Synnovis, see Jessica Lyons, *UK and US Cops Band Together to Tackle Qilin's Ransomware Shakedowns*, REGISTER (June 25, 2024, 12:01 UTC), https://www.theregister.com/2024/06/25/nca_fbi_qilin_ransomware/ [https://perma.cc/DQT4-WQGM].

195. Taddeo, *supra* note 181, at 340.

196. Nye, Jr., *supra* note 165, at 55.

197. HOLT & BOSSLER, *supra* note 164, at 76.

institutional responses adapt, making it difficult for deterrence by punishment to keep pace with emerging threats.[198]

C. Retributive Justice Theory and Cybercrime Punishment

Retributive justice, rooted in moral and legal philosophy,[199] appeared to be the oldest justification of punishment and can be found in the theories offered by Kant and Hegel.[200] It is described as a system of justice that emphasizes punishment as a response to crime or misconduct.[201] The theory addresses the question of how individuals who have deliberately engaged in recognized immoral actions that inflict direct or indirect suffering on others should be punished for their offenses.[202] Kant's view on retributivism underscores proportionality and justice, asserting that punishment should be based on the severity of the offense rather than justified by potential advantages like deterrence or rehabilitation.[203]

Retributive justice may offer a useful lens for tackling cybercrime as it emphasizes accountability and reinforcing societal order through proportional penalties. By establishing proportionality as the

---

198. *See* Suhail Adel Alansary & Mahmoud M. Saafan, *Emerging AI Threats in Cybercrime: A Review of Zero-Day Attacks via Machine, Deep & Federated Learning*, KNOWLEDGE & INFO. SYS. (2025) https://doi.org/10.1007/s10115-025-02556-6 ; See also Fabian M. Teichmann & Sonia R. Boticiu, *Adequate Responses to Cyber-Attacks*, 5 INT'L CYBERSECURITY L. REV. 337, 338–39 (2024); Lonergan & Montgomery, *supra* note 171, at 62 (explaining that attribution problems make deterrence by punishment difficult to sustain in cyberspace).

199. Don E. Scheid, *Kant's Retributivism*, 93 ETHICS 262, 264 (1983).

200. Thom Brooks, *Corlett on Kant, Hegel, and Retribution*, 76 PHIL. 561, 564 (2001).

201. *See* Michael Wenzel, Tyler G. Okimoto, & Michael J. Platow, *Retributive and Restorative Justice*, 32 L. & HUM. BEHAV. 375, 375 (2008); *see* Michael Wenzel & Tyler G. Okimoto, *Retributive Justice*, HANDBOOK OF SOC. JUST. THEORY AND RSCH. 237 (Clara Sabbagh & Manfred Schmitt eds., 2016); Robin Antony Duff, *Responsibility, Restoration, and Retribution*, *in* RETRIBUTIVISM HAS PAST: HAS IT FUTURE? 63 (Michael Tonry ed., 2011).

202. Kevin M. Carlsmith & John M. Darley, *Psych. Aspects of Retributive Justice*, 40 ADVANCES EXPERIMENTAL SOC. PSYCH. 193, 194 (2008).

203. Scheid, *supra* note 199, at 281; *see also* Neil Vidmar, *Retribution and Revenge*, *in* HANDBOOK OF JUST. RSRCH. LAW 31, 31–46 (Joseph Sanders & V. Lee Hamilton eds., 2002).

foundation for the prosecution and punishment of cyber offenses, it becomes a critical component of a more comprehensive legal response. For example, by emphasizing moral guilt, the idea conveys a definitive message that cybercrimes, including hacking, identity theft, and ransomware attacks, are unacceptable and will have legal consequences, thereby reinforcing the rule of law in cyberspace.[204] This perspective aligns with the broader moral foundations of criminal law, as contemporary legal philosophers like Hart,[205] Dworkin,[206] and Devlin[207] acknowledge the role of moral principles in shaping legal frameworks.[208] It is argued that moral principles—the harm principle,[209] the offense principle,[210] legal paternalism[211] and legal

204. H. Brian Holland, *The Failure of the Rule of Law in Cyberspace? Reorienting the Normative Debate on Borders and Territorial Sovereignty*, 24 J. MARSHALL J. COMPUT. & INFO. L. 1 (2005); Newman U. Richards & Felix E. Eboibi, *African Governments and the Influence of Corruption on the Proliferation of Cybercrime in Africa: Wherein Lies the Rule of Law?*, 35 INT'L REV. L. COMPUTERS & TECH. 131, 132–35 (2021); Cheng Chen & Bin Dong, *Digit. Forensics Analysis Based on Cybercrime and the Study of the Rule of Law in Space Governance*, 13 OPEN COMPUT. SCI. 1, 1 (2023).

205. *See* H.L.A. HART & LESLIE GREEN, THE CONCEPT OF LAW *passim* (2012).

206. *See* ROBERT S. SUMMERS, ESSAYS IN LEGAL PHILOSOPHY *passim* (1968).

207. *See* PATRICK BARON DEVLIN, THE ENFORCEMENT OF MORALS *passim* (1965).

208. Litska Strikwerda, *Should Virtual Cybercrime Be Regulated by Means of Criminal Law? A Philosophical, Legal-Economic, Pragmatic and Constitutional Dimension*, 23 INFO. & COMMC'N TECH. L. 31, 32 (2014).

209. *See* JOEL FEINBERG, 1 THE MORAL LIMITS OF THE CRIMINAL LAW: HARM TO OTHERS 32–35 (1987) (explaining the concept of harm involves three senses: direct harm on a person's self-interest; indirect effect from an initial wrong; and the sense in which the setback is morally indefensible or wrongful).

210. *See* JOEL FEINBERG, 2 THE MORAL LIMITS OF THE CRIMINAL LAW: OFFENSE TO OTHERS 49 (1988) (explaining that offense involves "evils" which are inherently offensive conduct; acts causing reasonable resentment or disgust; and profound, non-trivial impacts that are morally unjustifiable).

211. *See* JOEL FEINBERG, 3 THE MORAL LIMITS OF THE CRIMINAL LAW: HARM TO SELF 8–9 (1986) (justifying state coercion through criminal law to protect individuals from self-inflicted harm or misguided choices, overriding personal autonomy when the actor's welfare is at stake, as in laws prohibiting risky behaviors).

moralism[212]—provide a sound basis for penal provisions,[213] offering the justification for the criminalization of conduct.[214] In this context, the core principles of retributive theory can help to clarify the moral ground for criminalizing cyber offenses, focusing on the blameworthiness and the idea that individuals deserve punishment for wrongdoings.

However, the value of retributive justice theory in cyberspace is being questioned due to the conceptual and practical limitations. These challenges result primarily from the automation, scalability, and anonymity that characterize many cybercrimes. Retributivism, based on moral guilt and proportional punishment, presupposes identifiable offenders, clear causal links, and harms that can be measured.[215] However, cyber harms, particularly sequences of ransomware attacks,[216] are difficult to quantify and accommodate,[217] which makes proportionality in punishment challenging to determine. Retributivist assumptions about punishment as morally deserved retribution become strained when offenders range[218] from teenage hackers with limited understanding of legal consequences to highly trained state-sponsored threat actors with strategic motives. It is noted that retributivism hinges on the idea that punishment is

212. *See* JOEL FEINBERG, 4 THE MORAL LIMITS OF THE CRIMINAL LAW: HARMLESS WRONGDOING 3–5 (1988) (explaining legal moralism as the doctrine that justifies state coercion through criminal law to enforce prevailing moral standards and prohibit conduct deemed inherently immoral or degrading to public morality, even absent harm to others).

213. Strikwerda, *supra* note 208, at 40.

214. *See* 3 FEINBERG, *supra* note 211, at 323.

215. Dan Markel, *Retributive Damages: A Theory of Punitive Damages as Intermediate Sanction*, 94 CORNELL L. REV. 239, 278 (2009); *see* J. Angelo Corlett, *Making Sense of Retributivism*, 76 PHIL. 77, 83 (2001).

216. For example, the Akira ransomware group, active since March 2023, has impacted over 250 organizations worldwide, attributing responsibility and imposing proportionate punishment remain elusive. *See* CYBERSECURITY & INFRASTRUCTURE SEC. AGENCY, *#StopRansomware: Akira Ransomware*, (Apr. 18, 2024), https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-109a [https://perma.cc/E4A6-DTN7].

217. *See* N. Pattnaik et al., *It's More Than Just Money: The Real-World Harms from Ransomware Attacks*, *in* HUMAN ASPECTS OF INFORMATION SECURITY AND ASSURANCE 261, 270 (N. Clarke & S. Furnell eds., 2023).

218. Duff, *supra* note 201, at 64; *see also* Markel, *supra* note 215, at 260.

justified only if the offender had "the capacity and a fair opportunity or chance to adjust his behaviors to the law" and nonetheless chose to act wrongfully.[219]

Scholars have also questioned retributivism's capacity to respond to offenses mediated by avatars or autonomous agents, noting that punishment traditionally targets "flesh-and-blood" moral agents.[220] The use of avatars challenges certainty over proper subjects of punishment, as the user-avatar relationship blurs distinctions between actual and virtual harm.[221] This ambiguity decreases the moral power of retributive punishment.[222] Furthermore, this theory is frequently criticized for its failure to clarify why punishment should be applied for specific moral wrongs and not for others,[223] which creates uncertainty in defining the criteria for and implementation of retributive justice. Retributivism has been criticized for its failure to provide a thorough and pragmatic framework for penal justice, especially regarding the issues of accountability and proportionality in criminal conduct.[224]

To counter this challenge, scholars discuss hybrid models of assessing harms, and the possible paths of justice in incorporating

---

219. Hugo Adam Bedau, *Retribution and the Theory of Punishment,* 75 J. PHIL. 601, 606 (1978).

220. Marcus Johansson, *Why Unreal Punishments in Response to Unreal Crimes Might Actually Be a Really Good Thing*, 11 ETHICS & INFO. TECH. 71, 71 (2009).

221. *See id.* at 78.

222. *See* Wenzel, Okimoto & Platow, *supra* note 201, at 381 (arguing that ambiguity about how a transgression implicates shared values and status/power undermines retributive censure's capacity to reaffirm communal norms or to restore the disrupted status/power equilibrium, thereby diminishing its justificatory force); Dan Markel & Chad Flanders, *Bentham on Stilts: The Bare Relevance of Subjectivity to Retributive Justice*, 98 CALIF. L. REV. 907, 934 (2010).

223. Russ Shafer-Landau, *The Failure of Retributivism*, 82 PHIL. STUD. 289, 299 (1996); Leora Dahan Katz, *Response Retributivism: Defending the Duty to Punish*, 40 LAW & PHIL. 585, 585–86 (2021), ("This claim is commonly regarded by critics as remaining shrouded in mystery and thus the ability of retributivism to justify punishment regarded as suspect . . . [the benefits and burdens approach] has long since been regarded as suffering from serious flaws, leaving a justificatory vacuum in its wake.").

224. *See id.*

restorative and preventive measures, particularly in cases involving digital abuse, privacy breaches, or psychological harm.[225] Though retributivism holds enduring ethical sway, its shortcomings in the digital realm demand a nuanced framework attuned to the shifting landscape of cyber harms.

D. Restorative Justice and Victim Compensation in Cybercrime Cases

Criminal theory leans heavily on retributive justice, but this focus frequently overlooks alternatives such as restorative justice, which could combat cybercrime more effectively.[226] Restoration focuses on repairing harm and reconciling relationships rather than solely

---

225. The process of implementing methods of restorative justice may not be solely about punishment:

> In recent decades, a restorative justice movement has emerged in the criminal justice domain that challenges the assumption underlying the existing belief that punishment of the offender is sufficient, or even necessary, to restore justice after an offense . . . [c]rucial for proper restorative justice is a process of deliberation that places emphasis on healing rather than punishing: [H]ealing the victim and undoing their hurt, healing the offender and rebuilding their moral and social selves, and healing the group as a whole while mending social relationships.

See Tyler G. Okimoto, Michael Wenzel & N. T. Feather, *Beyond Retribution: Conceptualizing Restorative Justice and Exploring Its Determinants*, 22 SOC. JUST. RES. 156, 157–58 (2009). *See supra* section II.A.2; Allan Asher, *The Evolution of Harms in the Digital Age: Blurring Lines Between Online and Offline Harms*, AUSTRALIAN RISK POLICY INSTITUTE (ARPI) RESEARCH PAPER 1 (Dec. 2024) https://arpi.org.au/wp-content/uploads/2024/12/The-Evolution-of-Harms-in-the-Digital-Age-10122024.pdf [https://perma.cc/A4JX-95S7]; Tyrone Kirchengast, *The Limits of Criminal Law and Justice: 'Revenge Porn' Criminalisation, Hybrid Responses, and the Ideal Victim*, 2 UNISA STUDENT L. REV. 96, 97 (2016).

226. *See* Anne-Marie McAlinden, *"Transforming Justice": Challenges for Restorative Justice in an Era of Punishment-Based Corrections*, 14 CONTEMP. JUST. REV. 383 *passim* (2011).

punishing the offender.[227] This mechanism[228] or process,[229] emphasizes the needs of the victim,[230] accountability of the offender,[231] and the involvement of the community.[232] Restorative justice operates within a legal context, often involving legal practitioners, mediators, and sometimes even the state—albeit in a more rehabilitative or compensatory role[233]—in the healing process.[234]

In the context of cybercrime, where victims[235] may face not only financial losses[236] but also emotional distress at different levels of

---

227. JOHN BRAITHWAITE, RESTORATIVE JUSTICE & RESPONSIVE REGULATION 11 (2001); *see also* Tatjana Hörnle, *A Framework Theory of Punishment* 25–26 (MAX PLANCK INST. FOR THE STUDY OF CRIME, SEC. & LAW, Working Paper No. 2021/01, 2021), http://dx.doi.org/10.2139/ssrn.3783314 [https://perma.cc/ME6Y-2WTP]; Okimoto, Wenzel & Feather, *supra* note 225, at 157.

228. *See generally* Kathleen Daly, *What Is Restorative Justice? Fresh Answers to a Vexed Question*, 11 VICTIMS & OFFENDERS 9 (2016).

229. Wenzel, Okimoto & Platow, *supra* note 201, at 376.

230. Teresa Lancry A. S. Robalo & Razwana Begum Bt Abdul Rahim, *Cyber Victimisation, Restorative Justice and Victim-Offender Panels*, 18 ASIAN J. CRIMINOLOGY 61, 64 (2023); *see* Lara Bazelon & Bruce A. Green, *Victims' Rights from a Restorative Perspective*, 17 OHIO ST. J. CRIM. L. 293, 295 (2020).

231. Bazelon & Green, *supra* note 230, at 299; *see also* GERRY JOHNSTONE & DANIEL W. VAN NESS, HANDBOOK OF RESTORATIVE JUSTICE 35 (2007) (discussing empathy and accountability for an offender).

232. Persak, in her discussion of idea that was put forward by Lernestedt, argues that the community plays a central role in criminal law, not merely as passive beneficiaries of legal outcomes but as active participants whose norms and values guide legal frameworks. She discussed the desirability of constructing a model of criminal law that would include community as an important actor that shares responsibility and collective ownership of justice processes. This view aligns with restorative justice which aims to reinforce societal values while fostering offender rehabilitation. *See* Persak, *supra* note 156.

233. *See* HOWARD ZEHR, THE LITTLE BOOK OF RESTORATIVE JUSTICE: REVISED AND UPDATED app. I § 1.2 (2015).

234. JOHNSTONE & VAN NESS, *supra* note 231, at 15.

235. Victim, commonly encountered in the field of criminological research and justice system, is understood as "a natural person who has suffered harm, including physical, mental or emotional harm or economic loss which was directly caused by a criminal offense." ELENA MARTELLOZZO & EMMA A. JANE, CYBERCRIME AND ITS VICTIMS 15 (2017).

236. Jildau Borwell, Jurjen Jansen & Wouter Stol, *The Psychological and Financial Impact of Cybercrime Victimization: A Novel Application of the Shattered*

footnote continued on next page

severity.[237] In many cases, "[T]he victims may have no idea how they were victimized."[238] Restorative justice may offer a victim-centered, flexible framework that could fill in some of the gaps left by a strictly punitive legal system.[239] Current criminal law, argued by Vincent,[240] faces significant hurdles when applied to cybercrimes, particularly due to the anonymous nature of online offenders,[241] jurisdictional challenges,[242] and the complexity of proving mens rea[243] and causation.[244] In the criminal law system, victims and their harms are not the central concern.[245] Victims are marginalized while the prominent features are the offenders, the state, and offenses against it.[246]

The current system of criminal law is not helpful in recognizing and responding to the complex nature of cybercrime, which suggests that there must be an alternative or complementary mechanism designed to adequately address the justice gap. In cyberbullying, cyber-sexual offenses, and cyber-fraud cases, victims often require

---

Assumptions Theory, 40 SOC. SCI. COMPUT. REV. 933, 933 (2022); HOLT & BOSSLER, *supra* note 164, at 13.

237. HOLT & BOSSLER, *supra* note 164, at 12–13; Robalo & Abdul Rahim, *supra* note 230, at 64; Bazelon & Green, *supra* note 230, at 297.

238. Mark Button et al., *Online Fraud Victims in England and Wales: Victims' Views on Sentencing and the Opportunity for Restorative Justice?*, 54 HOWARD J. CRIM. JUST. 193, 206 (2015).

239. *See* Natalie Hadar, Ronen Shehman & Tali Gal, *When a Boy Hurts a Girl in Cyberspace: Facilitators' Views on Potential Benefits and Challenges in Restorative Justice,* 51 CRIM. JUST. & BEHAV. 1378, 1383 (2024).

240. Nicole A. Vincent, *Victims of Cybercrime: Definitions and Challenges*, *in* CYBERCRIME AND ITS VICTIMS 27 (Elena Martellozzo & Emma A. Jane eds., 2017).

241. *Id.* at 34–35.

242. *Id.* at 36.

243. "Mens rea" or "guilty mind" means intent of wrongdoing; it is a common creed between criminal lawyers to believe that crime is constituted from a concurrence of an evil-meaning mind (mens rea) and an evil-doing hand (actus reus). *See* STEPHEN P. GARVEY, GUILTY ACTS, GUILTY MINDS 7 (2020).

244. Vincent, *supra* note 240, at 37.

245. *Id.* at 28.

246. *Id.* at 30.

acknowledgment of harm, emotional validation, and mechanisms to prevent future harm.[247]

Restorative justice processes, such as family conferencing in South Australia[248] and victim-fraudsters mediation[249] in the United Kingdom, offer formally regulated platforms for victims to voice their grievances, receive apologies, and seek reparations.[250] Integrating restorative justice into the legal framework for addressing cybercrime requires targeted refinements to existing laws and policies. For example, in cases like cyberbullying, a technology-neutral approach offers a more adaptable and comprehensive legal response, ensuring relevance amidst rapid technological advancements,[251] rendering the

---

247. *See* Chee-kit Chan, Xin Wang & Xue Yang, *Prevalence and Relationships of Dating Application Usage, Cyber-Fraud and Mental Health Among Emerging Adults in Hong Kong*, 4 PSYCHIATRY RES. COMMC'NS 100197, 100197 (2024); Gregor Urbas, *Legal Perspectives on Cybercrime*, *in* RESEARCH HANDBOOK ON TRANSNATIONAL CRIME 316 (Valsamis Mitsilegas, Saskia Hufnagel & Anton Moiseienko eds., 2019); Gregor Urbas, *Protecting Children from Online Predators: The Use of Covert Investigation Techniques by Law Enforcement*, 26 J. CONTEMP. CRIM. JUST. 410, 410-12 (2010); Gregor Urbas, *Substantive and Procedural Legislation in Australia to Combat Webcam-Related Child Sexual Abuse*, in SWEETIE 2.0: USING ARTIFICIAL INTELLIGENCE TO FIGHT WEBCAM CHILD SEX TOURISM 135 (Simone van der Hof et al. eds., 2019); Des Butler, Sally Kift & Marilyn Campbell, *Cyber Bullying in Schools and the Law: Is There an Effective Means of Addressing the Power Imbalance?*, 16 E. LAW: MURDOCH U. ELEC. J.L. 84, 88 (2009). *See generally* Hadar, Shehman & Gal, *supra* note 239, at 1382 (explaining the importance of acknowledgment, validation, and the role of a victims family and greater society to address a harm done to them).

248. By facilitating dialogue between the victim, the offender, and their families, the family conferencing process seeks to repair relationships and restore trust, while also preventing further criminalization of youth. *See* Colette Langos & Rick Sarre, *Responding to Cyberbullying: The Case for Family Conferencing*, 20 DEAKIN L. REV. 299, 310–13 (2015) (Austl.).

249. Button et al., *supra* note 238, at 208.

250. A.M. Nascimento, J. Andrade & A. de Castro Rodrigues, *The Psychological Impact of Restorative Justice Practices on Victims of Crimes—a Systematic Review*, 24 TRAUAMA VIOLENCE ABUSE 1929, 1938 (2023) (reporting a systematic review of restorative justice victim outcomes).

251. *See* Niloufer Selvadurai, *The Relevance of Technology Neutrality to the Design of Laws to Criminalise Cyberbullying*, 1 INT'L J.L. & PUB. ADMIN. 14, 15 (2018).

creation of a new cyberbullying-specific law or dedicated offense unnecessary.[252]

In the context of necessary amendments to criminal law to better address cybercrime, restorative justice is considered a valuable approach to support the establishment of provisions aimed at enhancing victim protection.[253] It is supposed to help make existing legal regulations less fragmented and more consistent when approaching the concept of justice[254] throughout the processes of investigation, trial, and sentencing in cybercrime cases. Moreover, several significant challenges appear to arise when applying restorative justice in cybercrime cases, such as the complexity of addressing digital harm,[255] cross-border legal complications,[256] and, perhaps most importantly, the possibility that victims might hesitate to participate in these processes.[257] To address these issues, it could be beneficial for legislators to explore incorporating more adaptable, behavior-focused

---

252. Donna Pennell et al., *Should Australia Have a Law Against Cyberbullying? Problematising the Murky Legal Environment of Cyberbullying from Perspectives Within Schools*, 49 AUSTL.. EDUC. RESH. 827, 840–41 (2022).

253. Robalo & Abdul Rahim, *supra* note 230, at 63.

254. *See generally* Julia Davis, *Legal Responses to Cyberbullying by Children: Old Law or New?*, 1 UNIV. S. AUSTL. L. REV. 52 (2015) (proposing that creative legislative initiatives bridge gaps in fragmented tort and criminal regimes; offering a more cohesive response to technology-enabled wrongs like cyberbullying to ensure equitable and effective justice).

255. Sijia Xiao, Coye Cheshire & Niloufar Salehi, *Sensemaking, Support, Safety, Retribution, Transformation: A Restorative Justice Approach to Understanding Adolescents' Needs for Addressing Online Harm*, *in* PROC. OF THE 2022 CHI CONF. ON HUM. FACTORS IN COMPUT. SYS. (2022).

256. *See* Thomas J. Holt, *Regulating Cybercrime Through Law Enforcement and Industry Mechanisms*, 679 ANNALS AM. ACAD. POL. & SOC. SCI. 140, 151–52 (2018); Benoit Dupont, *Bots, Cops, and Corporations: On the Limits of Enforcement and the Promise of Polycentric Regulation as a Way to Control Large-Scale Cybercrime*, 67 CRIME L. & SOC. CHANGE 97, 102 (2017); Cassandra Cross, *'Oh We Can't Actually Do Anything About That': The Problematic Nature of Jurisdiction for Online Fraud Victims*, 20 CRIMINOLOGY & CRIM. JUST. 358, 362 (2020).

257. Gerry Johnstone, *Restorative Justice for Victims: Inherent Limits?*, 5 RESTORATIVE JUST. 382 (2017); *see also* William R. Wood & Masahiro Suzuki, *Four Challenges in the Future of Restorative Justice*, 11 VICTIMS & OFFENDERS 149, 154–55 (2016); Button et al., *supra* note 238, at 207.

legal frameworks[258] that work alongside restorative justice principles. This approach might help improve accountability and support victims, even in the face of these difficulties.

E. Utilitarianism and Cybercrime Law: Balancing Competing Interests

Building on the insights from the above analysis of deterrence, retributive, and restorative justice theories that may apply to cybercrime, there are principles from such theories that can provide critical perspectives on the enforcement and moral implications of cybercrime law. Meanwhile, utilitarian principles may offer a promising comprehensive societal viewpoint to develop an effective legal framework for cybercrime and cybersecurity based on cost-benefit analysis.

Utilitarianism has traditionally informed criminal law by emphasizing the optimization of societal welfare through cost-benefit analyses.[259] In the utilitarian view, punishment should be proportional to the crime—with deterrence as its central aim—discouraging potential offenses and promoting public security.[260] In the discussion on the motives of utilitarianism applied to punishment, it is highlighted that it stems from the inefficacy of excessive punishments that failed to reduce crime rates in Great Britain during the 1980s and 1990s.[261] The author also points out that a major challenge in the utilitarian approach to punishment lies in the criticism directed at

---

258. The focus is on the actions or offenses (cyberbullying, fraud, harassment) rather than the tools or platforms used to commit them (specific social media platforms, messaging apps, or devices).

259. *See* Guyora Binder & Nick Smith, *Framed: Utilitarianism and Punishment of the Innocent*, 32 RUTGERS L.J. 115, 116 (2000); ADAM J. KOLBER, PUNISHMENT FOR THE GREATER GOOD 25 (2024).

260. *See* James T. McHugh, *Utilitarianism, Punishment, and Ideal Proportionality in Penal Law: Punishment as an Intrinsic Evil*, 10 J. BENTHAM STUD. 1, 2, 8, 10 (2008).

261. *See id.* at 2.

rule utilitarianism,[262] rather than act utilitarianism,[263] which focuses on the state's subjective cost-benefit calculations rather than a general evaluation based on the rational choices of individuals in a "reasonable" and "well-informed" condition.[264]

The discussion on the application of utilitarianism to cybercrime law appears to be relatively limited in current literature. Legal discourse in this area often focuses on ethical dilemmas surrounding the regulation of emerging technologies[265] and the delicate balance between privacy and security.[266] However, these specific issues, while

262. A rule utilitarian is guided by a system of rules based on considerations of utility and adheres to these rules, even in situations where breaking the rule might yield better outcomes. *See* J. J. C. Smart, *Utilitarianism and Punishment*, 25 ISR. L. REV. 360, 371 (1991).

263. Act utilitarians, often referred to as "real utilitarians," maintain tactful interactions with social institutions and customs that embody non-utilitarian modes of thinking as Bentham explicitly outlines the principle of utility, focusing on the immediate consequences of actions to determine their morality. *See id.*; JEREMY BENTHAM, AN INTRODUCTION TO THE PRINCIPLES OF MORALS AND LEGISLATION 2 (1823).

264. *See id.* at 3.

265. *See* Lubna Luxmi Dhirani et al., *Ethical Dilemmas and Privacy Issues in Emerging Technologies: A Review*, 23 SENSORS 1151, 1151 (2023) (reviewing ethical concerns in AI, big data, and cybersecurity); Tareq Na'el Al-Tawil, *Ethical Implications for Teaching Students to Hack to Combat Cybercrime and Money Laundering*, 27 J. MONEY LAUNDERING CONTROL 21 (2024) (analyzing moral concerns in ethical hacking education, including potential misuse for privacy violations, while proposing protections to connect pedagogical advantages with anti-crime goals without undermining trust in regulatory enforcement); Ken Owen & Milena Head, *Motivation and Demotivation of Hackers in Selecting a Hacking Task*, 63 J. COMPUT. INFO. SYS. 522 *passim* (2023) (using deterrence theory to investigate hacker motivations, exposing how privacy-sensitive objectives influence task selection and emphasizing the necessity for ethical regulations to prohibit misuse while sustaining innovation). *See generally* Winfred Yaokumah, *Predicting and Explaining Cyber Ethics with Ethical Theories*, 10 INT'L J. CYBER WARFARE & TERRORISM 46 (2020) (finding consequentialism most predictive of privacy and integrity issues in digital contexts, highlighting regulatory gaps in balancing ethical norms with technological innovation).

266. *See generally* Derek E. Bambauer, *Privacy Versus Security*, 103 J. CRIM. L. & CRIMINOLOGY 667 (2013) (explaining that security and privacy should be decoupled in legal analysis, with security flaws warranting stricter penalties

footnote continued on next page

important, are beyond the scope of this Article. Instead, this Article focuses on exploring how utilitarian principles can provide a theoretical foundation for addressing challenges posed by cybercrime.

Applied to cybercrime law, the theory seeks to maximize collective security while minimizing harm to individuals and organizations by balancing the potential benefits of deterring and punishing cybercriminals against the costs and potential negative consequences of enforcement.[267] Some proponents of a utilitarian theory, argue that a utilitarian framework may provide some flexibility in combating cybercrime, particularly by calling for regulations that establish more stringent cybersecurity protocols, including measures that could protect businesses and critical infrastructure from cyber harms and large-scale attacks.[268] Some experts believe that measures like predictive policing,[269] increased surveillance,[270] and certainty of

---

than privacy breaches since they universally worsen outcomes and advocating a cost-benefit framework to evaluate enforcement measures that deter threats while avoiding over-penalization of informational harms); Alan D. Smith, *E-Security Issues and Policy Development in an Information-Sharing and Networked Environment*, 56 ASLIB PROC. 272, 273 (2004) (applying utilitarianism to concerns in information-sharing and global e-commerce).

267. Michael Edmund O'Neill, *Old Crimes in New Bottles: Sanctioning Cybercrime*, 9 GEO. MASON L. REV. 237, 281 (2000); Taiwo Oriola, *Bugs for Sale: Legal and Ethical Proprieties of the Market in Software Vulnerabilities*, 28 J. MARSHALL J. COMPUT. & INFO. L. 451, 520–21 (2011); Jonathan Lusthaus, *How Organised is Organised Cybercrime?*, 14 GLOB. CRIME 1 *passim* (2013); Paul Hunton, *The Growing Phenomenon of Crime and the Internet: A Cybercrime Execution and Analysis Model*, 25 COMPUT. L. & SEC. REV. 528, 528–31 (2009).

268. An Jungkook & Kim Hee-Woong, *A Data Analytics Approach to the Cybercrime Underground Economy*, 6 IEEE ACCESS 26636, 26637 (2018).

269. Elena Falletti, *Surfing Reality, Hype, and Propaganda: An Empirical Comparative Analysis on Predictive Software in Criminal Justice*, 4 A.I. & ETHICS 819 (2024); *see also* David H. McElreath, Sherri DioGuardi & Daniel Adrian Doss, *Pre-Crime Prediction: Does It Have Value? Is It Inherently Racist?*, 13 INT'L J. SERV. SCI., MGMT., ENGINEERING & TECH. 1 *passim* (2022); John Motsamai Modise, *Balancing Safety and Justice, the Ethics of Predictive Policing*, INT'L J. INNOVATIVE SCI. & RES. TECH. 3455, 3455–60 (2024).

270. Terry Palfrey, *Surveillance as a Response to Crime in Cyberspace*, 9 INFO. & COMMC'NS TECH. L. 173 *passim* (2000).

punishments[271] can help dissuade potential offenders while also protecting essential infrastructure from serious harm.[272] This approach appears to be consistent with rule utilitarianism,[273] which may prioritize regulatory systems designed to benefit long-term societal well-being by prohibiting harmful online behaviors.[274]

However, the unprecedented features of cyber threats may complicate these utilitarian goals. Some scholars insist that applying utilitarianism to address cyber threats is far from straightforward.[275] The most frequently mentioned obstacle is the balancing the interests involved.[276] Cybercrime causes many types of damage, including proprietary harm, mental harm, physical harm, and emotional harm,[277] making it difficult to measure the harmful consequences or calculate the benefits of prevention. Furthermore, the

---

271. David Maimon, *Deterrence in Cyberspace: An Interdisciplinary Review of the Empirical Literature*, *in* THE PALGRAVE HANDBOOK OF INTERNATIONAL CYBERCRIME AND CYBERDEVIANCE 449 (Thomas J. Holt & Adam M. Bossler eds., 2020); NAT'L INST. OF JUST., *Five Things About Deterrence,* U.S. DEP'T OF JUST. (June 5, 2016), https://nij.ojp.gov/topics/articles/five-things-about-deterrence [https://perma.cc/AM2P-RFPK].

272. Fotios Spyropoulos, *Artificial Intelligence and Crime: Navigating a Hybrid Criminal Landscape Through Technoethics*, 27 J. LEGAL, ETHICAL & REGUL. 1, 2 (2024).

273. Smart, *supra* note 262, at 371.

274. Martha Finnemore & Duncan B. Hollis, *Constructing Norms for Global Cybersecurity*, 110 AM. J. INT'L L. 425, 440 (2016); Nicola Dalla Guarda, *Governing the Ungovernable: International Relations, Transnational Cybercrime Law, and the Post-Westphalian Regulatory State*, 6 TRANSNAT'L LEGAL THEORY 211, 248 (2015).

275. Tom Harrison, *Virtuous Reality: Moral Theory and Research into Cyber-Bullying*, 17 ETHICS & INFO. TECH. 275, 279 (2015); *see* Roger Brownsword, *Law, Authority, and Respect: Three Waves of Technological Disruption*, 14 L. INNOVATION & TECH. 5, 18 (2022).

276. Serge-Christophe Kolm, *The Impossibility of Utilitarianism*, *in* THE GOOD AND THE ECONOMICAL 30, 30 (P. Koslowski & Y. Shionoya eds., 1993).

277. *See also* Ioannis Agrafiotis et al., *A Taxonomy of Cyber-Harms: Defining the Impacts of Cyber-Attacks and Understanding How They Propagate,* 4 J. CYBERSECURITY 1, 2–4 (2018) (developing a hierarchical taxonomy of cyber-harms). *See generally* Benoît Dupont, Francis Fortin & Rutger Leukfeldt, *Broadening Our Understanding of Cybercrime and Its Evolution*, 47 J. CRIME & JUST. 435 (2024) (surveying the evolution of cybercrime through a special issue lens, identifying diverse damage forms).

intangible and usually cross-border nature of cyber damage complicate the analyses of interests, as measures implemented in one region can inadvertently impact interests in another. For example, data that is evidence in a case under investigation can be routed through or stored remotely in many countries with different legal regimes, creating obstacles in law enforcement.[278]

There are even cases where individuals are implicated because the evidence data passes through that region.[279] Additionally, it is argued that the concept of "clustering" in cybercrime regulations, described in the United Nation Offices on Drugs and Crime cybercrime report of 2013,[280] points to many limitations in inter-regional cooperation that exacerbate jurisdictional conflicts.[281] These obstacles continue to pose significant challenges.[282] In order to tackle such complexities, scholars suggest integrating utilitarian principles with emerging techno-ethical paradigms. Spyropoulos advocates for balancing technological innovation with ethical safeguards to address AI-enabled crimes.[283] Supporting this approach, transnational cooperation is emphasized to harmonize legal norms and overcome jurisdictional fragmentation.[284]

The literature on utilitarianism and cybercrime law is primarily concerned with the tension between effectiveness in deterrence and maintaining fairness and proportionality. In the context of this Article's analysis, utilitarianism, together with other examined criminal theories, emphasize the importance of balanced regulations that address the complexities of cybercrime. It protects cybersecurity by deterring and punishing cybercriminals, while promoting internet

---

278. Guarda, *supra* note 274, at 237.

279. *Id.*

280. U.N. Off. on Drugs & Crime, *Comprehensive Study of the Problem of Cybercrime and Responses to it by Member States, the International Community and the Private Sector* at 11, U.N. Doc. CCPCJ/EG.4/2013/2 (Feb. 2013).

281. Guarda, *supra* note 274, at 237.

282. *See* M. Shahidullah Shahid et al., Global Cybercrime and Cybersecurity Laws and Regulations: Issues and Challenges in the 21st Century 22 (2022).

283. *Id.* at 8.

284. Guarda, *supra* note 274, at 249.

commerce by fostering trust and minimizing overregulation. To achieve this balance, effective cybercrime and cybersecurity laws must be founded on clear and consistent criteria. These criteria are intended to provide a foundation for assessing the effectiveness of laws based on contemporary legal theories while ensuring they remain grounded and do not deviate in their relationship with technology.

Table 3 presents an overview of the interrelationships among key criminal theories analyzed above, highlighting their respective key points, theoretical interactions, and specific roles within the context of cybercrime law:

Table 3. Criminal theories and their roles in cybercrime law

Theory	Focus	Interaction	Role
Deterrence	Preventing crime	Utilitarianism, Retribution	Enforces boundaries
Retributive Justice	Moral accountability	Deterrence, Restorative Justice	Fair punishment
Restorative Justice	Victim-centered	Retributive Justice, Utilitarianism	Compensation and repair
Utilitarianism	Greatest good	All of the above	Law as social utility

Having examined how the fundamental criminal law theories of deterrence, retributive justice, restorative justice, and utilitarianism inform the foundational principles of cybercrime regulation, this Article will now develope a refined theoretical model. The following Part proposes a set of evaluative criteria specifically designed to assess the effectiveness of cybercrime legislation. This model aims to advance criminal law scholarship by combining traditional jurisprudential approaches with the novel complexities raised by emerging

cybercrimes. It is designed to improve the effectiveness of cybercrime law and to lay the groundwork for future reforms to tackle challenges of AI-driven automation and industrialized ransomware.

IV. A New Theoretical Model: Criteria for Determining Effective Cybercrime Law in the Age of AI and Ransomware

A. Overview

This section aims to explore and develop a new theoretical model for understanding what constitutes effectiveness in cybercrime legislation. While many scholars have developed models based on deterrence, retribution, and prevention theories, there is still a need for an integrated framework tailored precisely to the unique nature of cybercrime in the age of AI and ransomware. This analysis of existing legal scholarship identifies major contributions and gaps, laying the foundation for the proposed model advanced in this Article. As mentioned, the effectiveness of legislation generally refers to its ability to achieve intended outcomes and drive positive social change.[285] In the context of this research, it is suggested that cybercrime law is effective when it is functional[286]—in both addressing emerging cybercrime and incorporating economic considerations as a key factor influencing the legislation's objectives. Table 4 below outlines a theoretical model that integrates foundational criminal law theories with specific criteria for effective cybercrime legislation, grounded in the unique features of cybercrime:

285. *See* John Dickinson, *Legislation and the Effectiveness of Law*, 17 A.B.A. J. 645, 694 (1931); Goddard, *supra* note 1, at 16.

286. Maria Mousmouti, Designing Effective Legislation 56 (2019).

Table 4: Conceptual framework for evaluating cybercrime law

Criminal Theories	Criteria for Effective Cybercrime Law	Cybercrime Features
Deterrence theory in crime prevention	Clear legal definitions and scope that balances security and commercial freedom	Global and borderless Anonymous
Retributive justice and cybercrime punishment	Proportional and consistent penalties that account for economic impact	Automation and scalability; Anonymity
Restorative justice and victim compensation	Restorative measures emphasizing recovery and resilience in commerce	Hyper-personalization
Utilitarianism in shaping cybercrime law	Legal certainty andflexibility in the context of emerging technologies	Psychological vulnerabilities

B. The Need for Clear Legal Definitions and Scope that Balances Security and Commercial Freedom

An effective cybercrime law requires clear legal definitions and scope to address the complexities of digital misconduct. Legal clarity is critical because it ensures stability in society, guiding behaviors through well-defined rules.[287] It refers to the attribute of being clear

287. Ryan J. Owens & Justin P. Wedeking, *Justices and Legal Clarity: Analyzing the Complexity of U.S. Supreme Court Opinions*, 45 L. & SOC'Y REV. 1027, 1029 (2011).

and easy to understand.[288] Drawing insights[289] from the concept of legal clarity, we can apply this notion to the domain of cybercrime, where legal clarity refers to the extent to which the meaning of the legal text is determined without ambiguity of legal frameworks designed to address cyber-related offenses.[290] Textual clarity ensures that laws are understandable and predictable, enabling both compliance by citizens and enforcement by authorities,[291] as well as promoting trust for efficient internet commerce.[292]

The lack of agreement on what constitutes cybercrime has a significant impact on society, legal structures, and academic study.[293] For example, in Australia, the ambiguity and inconsistency in definitions of cybercrime were seen as significant obstacles to successfully addressing offenses uniformly nationwide,[294] and it is desired for greater leadership and better understanding across all

---

288. *See Clarity*, DICTIONARY.CAMBRIDGE.ORG, https://dictionary.cambridge.org/dictionary/english/clarity [https://perma.cc/JKR2-9JKA] (last visited June 8, 2025); Jonathan H. Choi, *Measuring Clarity in Legal Text*, 91 U. CHI. L. REV. 1, 1–4 (2024) (presenting a theoretical and empirical measure of how clear, precise and self-sufficient the legal text is in guiding interpretation).

289. *See* Edward B. Whitney, Doctrine of Stare Decisis, 3 MICH. L. REV. 89, 91 (1904) (underscoring the interconnectivity between judicial decisions and the doctrine of stare decisis in the context of common law systems); Owens & Wedeking, supra note 287; *cf.* Gillian K. Hadfield, *The Quality of Law: Judicial Incentives, Legal Human Capital and the Evolution of Law* 3–4 (U. S. Cal. L. & Econ. Org. Rsch. Paper No. C07-3) (Feb. 2007), http://dx.doi.org/10.2139/ssrn.967494 [https://perma.cc/5N7Y-XKT2]) (relying on written statutes and codes, legal clarity in civil law systems comes from the precision and comprehensibility of the legal texts themselves, rather than judicial decisions).

290. *See* Choi, *supra* note 288, at 4.

291. *See* Owens & Wedeking, *supra* note 287.

292. Oriola Sallavaci**,** *Combating Cyber Dependent Crimes: The Legal Framework in the UK*, *in* 630 COMMUNICATIONS IN COMPUTER AND INFORMATION SCIENCE, GLOBALSECURITY, SAFTEY AND SUSTAINABILITY–SECURIRTY OF THE CONNECTED WORLD 53, 53 (Arshad Jamal et al. eds., 2017).

293. Kirsty Phillips et al., *Conceptualizing Cybercrime: Definitions, Typologies and Taxonomies*, 2 FORENSIC SCI. 379, 379–80 (2022).

294. CASSANDRA CROSS ET AL., CRIMINOLOGY RSCH. ADVISORY COUNCIL, CRG 23/16–17, RESPONDING TO CYBERCRIME: PERCEPTIONS AND NEED OF AUSTRALIAN POLICE AND THE GENERAL COMMUNITY, at 60 (2021), https://www.aic.gov.au/sites/default/files/2021-08/CRG_Responding%20to%20cybercrime_0.pdf [https://perma.cc/T8S2-5EH3] (Austl.).

agencies.[295] In the United States, vague criminal law provisions may provide prosecutors and judges extensive interpretive discretion, which risks arbitrary implementation and exacerbates systemic inequalities.[296] In Hungary, the principle of "clarity of norms" emphasizes the need for precision in criminal law to maintain the rule of law.[297] Confusing terms like "apparently anti-social" in the Hungarian Criminal Code result in uncertainty in understanding and may create inconsistent judicial verdicts, referring to the need for linguistic precision and contextual comprehension.[298]

The rapid evolution of technology and digital behaviors increasingly complicate the definition of cybercrime. Cybercrime encompasses a broad range of behaviors, from hacking and identity theft to cyberterrorism, making it difficult to define complete legal standards.[299] Variability in terminology, such as "computer crime," "electronic crime," "high-tech crime," and "technology-enabled crime" adds to differences among jurisdictions.[300] In Turkey, the obstacles within the legal framework prevent the successful prosecution of cybercrime.[301] The ambiguity in legislation includes issues such as vague definitions, excessively broad terminology, and outdated provisions. This presents considerable obstacles in ensuring the effective implementation of cybercrime law.[302]

---

295. *See id.* at 61.

296. *See* Shon Hopwood, *Clarity in Criminal Law*, 54 AM. CRIM. L. REV. 695, 696–99 (2017); Jeremy Waldron, *Void for Vagueness: Vagueness in Law and Language: Some Philosophical Issues*, 82 CALIF. L. REV. 509, 509–12 (1994).

297. Krisztina Ficsor, *Certainty and Uncertainty in Criminal Law and the 'Clarity of Norms' Doctrine*, 59 HUNG. J. LEGAL STUD. 271 *passim* (2018).

298. *See id.* at 272.

299. Laura Bartoli, *Cybersecurity and the Fight Against Cybercrime: Partners or Competitors?*, 16 EUR. J. RISK REGUL. 498, 512 (2025); *see* James Hawdon et al., *Cybercrime: Victimization, Perpetration, and Techniques*, 46 AM. J. CRIM. JUST. 837, 837–38 (2021) (discussing the broad range of conduct encompassed by cybercrime, from fraud and identity theft to threats and intimidation).

300. Phillips et al., *supra* note 293, at 380.

301. Elvin Shukurov & Uzeyir Jafarov, *Legal Professionals' Perspectives on the Challenges of Cybercrime Legislation Enforcement*, 2 INTERDISC. STUD. SOC'Y L. & POL. 25, 27 (2023).

302. *See id.* at 29.

Examples of unclear legal terms in cybercrime law can be seen in the United States and the United Kingdom In the United States, criticism has been raised over the terms of "access" and "authorization"[303] which have long been sources of ambiguity and controversy.[304] Courts have struggled to define "access" and "authorization" because the internet provides competing standards, and technological advancements resulting in new platforms that have complicated the hunt for a clear and uniform interpretation.[305] In *Van Buren v. United States*,[306] the legal clarity issue stemmed from the ambiguous definition of "exceeds authorized access" under the Computer Fraud and Abuse Act ("CFAA").[307]

The CFAA resulted in inconsistent interpretations of whether misuse of legitimate access constitutes a cybercrime. In the United Kingdom, the application of unauthorized access offenses under the Computer Misuse Act of 1990[308] has underscored critical ambiguities.[309] Inconsistent judicial interpretations continue to undermine the Act's effectiveness.[310] Nevertheless, these examples merely highlight issues related to hacking into closed computer systems, where "authorization" is determined by an entity's terms of service or internal

---

303. 18 U.S.C. § 1030 (1986).

304. Orin S. Kerr, *Cybercrime's Scope: Interpreting "Access" and "Authorization" in Computer Misuse Statutes*, 78 N.Y.U. L. REV. 1596, 1599 (2003).

305. *See id.*

306. 593 U.S. 374 (2021).

307. *Id.* at 379; Kerr, supra note 304, at 1598–99; *see also* Orin S. Kerr, *Norms of Computer Trespass*, 116 COLUM. L. REV. 1143, 1163 (2016) (arguing that the ambiguity in the CFAA "exceeds authorized access" provision comes from unsettled trespass norms in the digital age, where courts must distinguish between technical authentication barriers and mere policy violations to prevent overcriminalization, and proposing an authentication principle where access is unauthorized only if it bypasses required credentials, to clarify and narrow the statute's scope pending norm development).

308. Computer Misuse Act 1990, c. 18 (U.K.).

309. *See* Sallavaci, *supra* note 292, at 55–56.

310. *See id.*

policies,[311] which might not be designed with criminal law in mind.[312] Today, cybersecurity challenges have become far more complex, including web scraping,[313] API usage,[314] security research,[315] and AI-driven automation,[316] none of which are adequately addressed in the legislation.

In common law jurisdictions, a "clear-statement rule" would compel legislatures to provide precise definitions, reducing the reliance on judicial discretion.[317] A definition of cybercrime has been proposed that encompasses the role of computers, techniques of

311. Alden Anderson, *The Computer Fraud and Abuse Act: Hacking into the Authorization Debate*, 53 JURIMETRICS 447, 451 (2013).

312. Stein Schjolberg, *The History of Global Harmonization on Cybercrime Legislation - The Road to Geneva,* CYBERCRIME LAW (Dec. 2008), https://cybercrimelaw.net/documents/cybercrime_history.pdf [https://perma.cc/7ZQL-TMCE].

313. *See* Tess Macapinlac, *The Legality of Web Scraping: A Proposal*, 71 FED. COMMC'NS L.J. 399, 401 (2019) (referring to the gathering of data from a website's output and saving it to a file or database).

314. *See* Zubaidi Alaa Abdul Al Muhsen Hussain Al & Florentin Ipate, *Application Programming Interface (API) Security: Cybersecurity Vulnerabilities Due to the Growing Use of APIs in Digital Communications*, 6 INT'L RES. J. INNOVATIONS ENGINEERING & TECH. 108, 112 (2022) ("API vulnerabilities emerge…when the underlying application's security architecture is poor.").

315. Rebecca Slayton, *What Is the Cyber Offense-Defense Balance? Conceptions, Causes, and Assessment*, 41 INT'L SEC. 72, 73–74 (2017); *see generally* Robert Jervis, *Cooperation Under the Security Dilemma*, 30 WORLD POL. 167 (1978) (introducing the security dilemma as a structural condition, where actions taken by one state to enhance its own security may inevitably threaten the security of others); Toby Shevlane & Allan Dafoe, *The Offense-Defense Balance of Scientific Knowledge: Does Publishing AI Research Reduce Misuse?, in* PROC. AAAI/ACM CONF. AI, ETHICS & SOC'Y 173, 173 (2020) (suggesting that policymakers and the AI community must adapt and develop tailored legal and policy frameworks to effectively manage the risks of misuse while enabling defensive advancements).

316. *See* Lucia Stanham, *AI-Powered Cyberattacks*, CROWDSTRIKE (Jan. 16, 2025), https://www.crowdstrike.com/en-us/cybersecurity-101/cyberattacks/ai-powered-cyberattacks/ [https://perma.cc/7SJV-Y7AW].

317. Hopwood, *supra* note 296, at 737.

attack, and perspectives of both attackers and defenders.[318] This approach is beneficial for legislators because it improves their understanding of cybercrime mechanisms, appreciating the importance of technology-based knowledge systems, and indicates that legal strategies should attempt to keep pace with the rapid evolution of cyber threats. In general, definitions and terms associated with cybercrime can be examined from social, political, and criminological viewpoints.[319] Nonetheless, when required, they must be incorporated into legal documents, ensuring the requisite consistency to promote fair and effective law enforcement.[320]

In addition, a well-defined scope is crucial to delineate the boundaries of cybercrime laws. Broadhurst et al. explained that the Australian Cybercrime Online Reporting Network ("ACORN") illustrates how a focused scope can enhance the effectiveness of enforcement.[321] ACORN highlights the need for specificity in prevention of cybercrime by categorizing incidents like fraud and identity theft. In doing so, the system brings into focus the demographics most at risk—particularly those between the ages of twenty and forty—and stresses the centrality of social networking platforms as primary channels through which these crimes are carried out.[322] Among the recent legislative efforts[323] to clarify cybercrime law, Australia's Cyber Security Legislative Package 2024 stands out. It revises the legal framework to account for emerging cyber threats and

318. Charlette Donalds & Kweku-Muata Osei-Bryson, *Toward a Cybercrime Classification Ontology: A Knowledge-Based Approach*, 92 COMPUT. IN HUM. BEHAV. 403, 407–09 (2019).

319. *See id.* at 404.

320. Gargi Sarkar & Sandeep K. Shukla, *Behavioral Analysis of Cybercrime: Paving the Way for Effective Policing Strategies*, 2 J. ECON. CRIMINOLOGY art. no. 100034, at *passim* (2023).

321. Roderic Broadhurst, *Cybercrime in Australia*, *in* THE AUSTRALIAN & NEW ZEALAND HANDBOOK OF CRIMINOLOGY, CRIME & JUSTICE 221, 222 (Antje Deckert & Richard Sarre eds., 2017).

322. *See id.*

323. *See* Grégoire Webber, *Legislative Measures and Legislators' Motives*, 2 COMP. CONST. STUD. 150, 150 (2024).

supports the broader national objective of positioning Australia as a global cybersecurity leader by 2030.[324]

C. The Need for Proportional and Consistent Penalties that Account for Economic Impact

Effective cybercrime and cybersecurity laws require penalties that are proportional and consistent. These penalties should reflect the offender's moral blameworthiness. They must also take account for the broader economic losses and systemic harms caused by digital offenses. Retributive punishment traditionally depends on the principle of proportionality between crime and penalty, yet this principal risks becoming conceptually unstable when there is no clear standard for measuring the gravity of wrongdoing or the suffering inflicted.[325] In the context of emerging cybercrime, the difficulty of assessing harm is magnified. Impacts are often wide-ranging, indirect, and complex, manifesting in severe business interruption, financial and reputational harm, psychological trauma among employees, and long-term degradation of organizational trust and resilience.[326]

An effective approach to cybercrime sentencing must integrate proportionality with a careful assessment of the economic disruption caused by cyber offenses. Specifically, such an approach should, first ensure that punishment conveys moral condemnation for cyber harms. Second, it should address the tangible impacts on digital infrastructure, commercial ecosystems, and public trust. Third, it should reinforce societal resilience by promoting accountability that resonates with both victims and broader economic interests. In summary, balancing moral gravity with economic realities is essential to maintaining justice and protecting the stability of the digital economy.

It is useful to examine how leading jurisdictions respond to AI-enabled cybercrime and ransomware, as this reveals both divergent and

---

324. DEP'T OF HOMELAND AFFS., 2023–2030 AUSTRALIAN CYBER SECURITY STRATEGY 4 (2023), https://www.homeaffairs.gov.au/cyber-security-subsite/files/2023-cyber-security-strategy.pdf [https://perma.cc/M4BU- DGF6] (Austl.).

325. Bedau, *supra* note 219, at 604.

326. *See* Gareth Mott et al., *'There Was a Bit of PTSD Every Time I Walked Through the Office Door': Ransomware Harms and the Factors That Influence the Victim Organization's Experience*, 10 J. CYBERSECURITY 1, 11 (2024).

converging approaches to proportional and consistent penalties. In the United States, cybercrimes—including AI-facilitated fraud—are prosecuted under general laws like the CFAA. 18 U.S.C. § 1030, for example, carries up to ten years' imprisonment, and twenty years for repeat violation.[327] Notably, subsection (c)(2)(B) prescribes that offenses under subsection (a)(2), such as committing unauthorized access to protected computers, are punishable by a fine and/or imprisonment of up to five years, particularly when the act is committed for commercial advantage or private financial gain, in furtherance of another criminal or tortious act, or "when the value of the information obtained exceeds $5,000."[328] These aggravating factors reflect an effort to scale punishment in proportion to economic harm or malicious intent.

Recent procecusions show ransomware conspirators facing cumulative penalties of twenty-five to forty-five years under wire fraud and money laundering counts, with the actual sentence set by the court after calculating the advisory U.S. Sentencing Guidelines and considering other statutory factors.[329] In contrast to the United States' reliance on broad federal statutes and cumulative sentencing, the European Union adopts a harmonized minimum standards approach, emphasizing proportionality and consistency through Directive 2013/40/EU on attacks against information systems[330]: basic illegal access or data interference must carry at least two years' maximum,[331] rising to three or five years if large botnets, serious damage or critical infrastructure are involved.[332] EU member states enact these minima and mandate "effective, proportionate and dissuasive" sanctions.[333] Regarding AI misuse, Article 99 of the proposed EU AI Act provides for administrative fines of up to €35 million

---

327. 18 U.S.C. § 1030.

328. *Id.*

329. Press Release, U.S. Dep't of Just., Two Foreign Nationals Plead Guilty to Participating in LockBit Ransomware Group (July 18, 2024) ("[W]ill determine any sentence after considering the U.S. Sentencing Guidelines and other statutory factors.").

330. Directive 2013/40 of the European Parliament and of the Council of 12 Aug. 013 on Attacks Against Information Systems and Replacing Council Framework Decision 2005/222/JHA, 2013 O.J. (L 218/8).

331. *Id.*

332. *Id.* art. 9(4).

333. *Id.* art. 11.

or, in the case of undertakings, up to 7% of their total worldwide annual turnover.[334] Similarly, the GDPR enforces data security through administrative penalties on firms (up to 4% of annual turnover),[335] not individual criminal liability.[336] This reflects the EU's dual-track approach[337]: penalizing corporate non-compliance civilly while reserving criminal law for targeted, defined cyber offenses.

In Australia, the Criminal Code criminalizes hacking—including unauthorized access or data modification—punishable by imprisonment for a term of up to five years.[338] Ransomware Action Plan 2022 recommended increasing penalties and expanding offenses,[339] however, the Criminal Code already prescribed strong maximum penalties (ten years or more) for core cyber offenses prior to the Plan.[340] In sum, proportional and consistent penalties—especially in terms of economic impact—provide a practical and measurable basis for assessing legislative effectiveness across jurisdictions.

---

334. *See* Regulation 2024/1689 of the European Parliament and of the Council of 13 June 2024 Laying Down Harmonised Rules on Artificial Intelligence, 2004 O.J. (L 168/1) art. 99(3) (hereinafter *Artificial Intelligence Act*).

335. *See* Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data (*General Data Protection Regulation*), [2016] O.J. (L 119/1) art. 83(5).

336. *See Facebook Owner Hit with 251 Million Euros in Fines for 2018 Data Breach*, AP NEWS (Dec. 17, 2024, at 07:47 ET), https://apnews.com/article/meta-facebook-privacy-european-union [https://perma.cc/8D2A-N7BW]; Andrew J. Hawkins, *Uber Hit with $324 Million EU Fine for Improper Data Transfer*, THE VERGE (Aug. 26, 2024, at 09:30 ET), https://www.theverge.com/2024/8/26/24228589 [https://perma.cc/NQ6M-ZN69].

337. *See* Giulia Gentile & Orla Lynskey, *Deficient by Design? The Transnational Enforcement of the GDPR*, 71 INT'L & COMP. L.Q. 799, 824 (2022).

338. *Criminal Code Act 1995* (Cth) ss 477.1, 478.1 (Austl.).

339. Cybercrime Legislation Amendment (Ransomware Action Plan) Bill 2022, Bills Digest No. 62 of 2021–22 (Apr. 1, 2022), sch 1 items 3, 4, 6, 10, https://www.aph.gov.au/Parliamentary_Business/Bills_Legislation/bd/bd2122a/22bd062 [https://perma.cc/R5XF-5EY7] (Austl.).

340. *Criminal Code Act 1995* (Cth) ss 477.1 (unauthorized access or modification, maximum 10 years' imprisonment); ss 477.2–477.3 (causing or risking serious harm to data or systems, maximum 10 years); s 478.1 (possession of data with intent to commit a computer offense, maximum 3 years) (Austl.).

D. The Need for Restorative Measures Emphasizing Recovery and Resilience

A functional feature of effective cybercrime legislation is its capacity to address not only the criminal act, but also the broader social and economic harms resulting from cyber offenses. In the case of AI-enabled frauds and ransomware, where the scalability and hyper-personalization of attacks accentuate both the immediacy and complexity of victimizing, this becomes clearer. Advanced AI enables offenders to craft highly personalized fraudulent communications and ransomware attacks, exploiting individual behavioral data to maximize coercion and deception.[341] These incidents contribute to new forms of victimization that go beyond traditional categories, imposing on not only individuals but also on businesses, and entire economies. Responding to these challenges, the need for restorative measures that prioritize recovery and commercial resilience becomes obvious.

Retributive penalties alone are insufficient to repair the multilayered harms caused by hyper-personalized cybercrimes. The empirical study of online fraud victims by Button et al. reveals that many victims seek restitution and opportunities to engage in justice processes that acknowledge their losses and promote healing, rather than solely punitive outcomes.[342] This is consistent with restorative

---

341. *See* Button et al., *supra* note 238; Cross and Holt, *supra* note 31; *Cyber Signals Issue 9: AI-Powered Deception—Emerging Fraud Threats and Countermeasures,* MICROSOFT (Apr. 16, 2025), https://www.microsoft.com/en-us/security/blog/2025/04/16/cyber-signals-issue-9-ai-powered-deception-emerging-fraud-threats-and-countermeasures/ [https://perma.cc/Q2D4-FWNG].

342. Indeed, restorative justice in the cybercrime context may prove useful:

> What was most interesting, however, was the interest shown by the victims and stakeholders in the potential for restorative justice. Clearly the anonymous nature of many online frauds made it very attractive to victims to find out who did it and why they were selected. However, there was also a more sophisticated realization that online fraudsters can escape the impact of their crimes through the anonymity of the Internet. They do not see the harm they do. As such there was a view amongst the victims and the stakeholders that providing an opportunity for the victims to meet the fraudsters and articulate the damage it had

footnote continued on next page

justice theory, which provides that justice should seek to empower victims, heal harm, and encourage responsibility that supports both personal and institutional resilience.[343]

The relevance of this criterion can be seen in real-world ransomware incidents. Post-attack recovery often exposes a host of legal challenges. These include incident response protocols, breach notification statutes, and compensation mechanisms.[344] Together they show how recovery efforts may align with or diverge from restorative justice principles such as restitution, harm repair, and resilience-building. A clear example arose in the United States in 2019 when the City of Baltimore suffered a major ransomware attack. Critical municipal systems were disabled. The city refused to pay the ransom and instead undertook a prolonged and costly recovery process. Although the recovery costs far exceeded the ransom demand,[345] Baltimore's refusal to pay aligned with restorative justice principles, as it avoided enriching offenders. However, the burden of recovery fell entirely on the city and its residents, underscoring the lack of government compensation mechanisms and revealing significant gaps in victim support framework.

In the wake of the Baltimore incident, the United States government reinforced policies discouraging ransom payments[346] and

---

> done would be beneficial to both the victims and the offender.
>
> Button et al, *supra* note 238, at 208.

343. *See* BRAITHWAITE, *supra* note 227, at 10; JOHNSTONE & NESS, *supra* note 231.

344. Melanie K. Worsley, Joseph Kendall-Morwick & Kate A. Houston, *Change Waits for No One: An Examination of the Legal Response to Ransomware Attacks*, CRIM. JUST. POL'Y REV. (forthcoming 2025) (manuscript at 4).

345. Following a ransomware attack and the decision to reject an $80,000 ransom demand, Baltimore incurred approximately $18 million in recovery costs. *See* Clare O'Gara, Ransomware Aftermath: Baltimore Buys $20 Million in Cyber Insurance, SECUREWORLD (Oct. 21, 2019, at 08:00 PT), https://www.secureworld.io/industry-news/the-aftermath-of-ransomware-baltimore-invests-20-million-into-cyber-insurance[https://perma.cc/4VJU-WAFJ]; Jonathan Greig, *Thousands of Baltimore Students, Teachers Affected by Data Breach Following February Ransomware Attack*, RECORD (Apr. 23, 2025), https://therecord.media/baltimore-public-schools-data-breach-ransomware [https://perma.cc/Z5QM-A9YX].

346. U.S. DEP'T OF THE TREASURY, OFFICE OF FOREIGN ASSETS CONTROL, UPDATED ADVISORY ON POTENTIAL SANCTIONS RISKS FOR FACILITATING

footnote continued on next page

later enacted the Cyber Incident Reporting for Critical Infrastructure Act of 2021, which requires timely reporting of major cyberattacks in order to strengthen national response and resilience efforts.[347] The Baltimore case emphasized the necessity for more accessible recovery aid programs—financial or technological[348]—to effectively realize restorative justice goals. On a positive note, the case did lead to greater investment in cyber resilience, including upgrading systems, buying insurance, and training staff[349]—which is a form of systemic restitution where the city learned from the attack and took steps to protect its citizens from future harm.[350]

In Australia, two major ransomware attacks against Toll Group in 2020 severely disrupted logistics operations,[351] but demonstrated the legal emphasis on resilience and harm repair. Crucially, Toll Group refused to pay any ransom demands. Instead, the company undertook a painstaking recovery process: It isolated infected systems, wiped and restored servers from clean backups, and gradually brought core operations back online.[352] This reflects restorative values in that Toll

---

RANSOMWARE PAYMENTS *passim* (2021), https://ofac.treasury.gov/media/912981/download? [https://perma.cc/3SZQ-JCJQ].

347. 6 U.S.C. § 681b(a)(1)(A) (proposing the Cyber Incident Reporting for Critical Infrastructure Act of 2021, HR 5440, 117th Cong., § 2220A(d)(5).

348. *See* Jake DeBacher, *Ransomware*, 6 GEO. L. TECH. REV. 300, 307 (2022).

349. Edward A. Morse & Ian Ramsey, *Navigating the Perils of Ransomware*, 72 BUS. LAW. 287, 293 (2016).

350. *Id.* at 294.

351. Toll Group, a large Australian transportation and logistics company, suffered two ransomware attacks in quick succession, one attack in January 2020 by the "Mailto" strain and a second in May 2020 by the Nefilim group. These attacks forced Toll to shut down parts of its IT systems, disrupting package deliveries and supply chain services across Australia and beyond. *See* Jamie Humphrey, *Toll Attack Shows Ransomware Is the New Normal*, AUSTRL. CYBER SEC. MAG. (May 22, 2020), https://australiancybersecuritymagazine.com.au/toll-attack-shows-ransomware-is-the-new-normal/ [https://perma.cc/NF5U-F3W9]; *When Giants Fall: What We Can Learn from the Cyberattack on Toll Group* (May 3, 2024, at 13:01 ET), CYBER HELPER, https://cyberhelper.com.au/cyber-crime/when-giants-fall-what-we-can-learn-from-the-cyberattack-on-toll-group/ [https://perma.cc/G5Z6-FUZU].

352. Ry Crozier, *Toll Group's Corporate Data Stolen by Attackers*, ITNEWS (May 12, 2020, at 16:39 ET), https://www.itnews.com.au/news/toll-groups-corporate-data-stolen-by-attackers-548033 [https://perma.cc/AL4E-4DEY].

prioritized rebuilding and securing its infrastructure over capitulating to criminals, even though this meant short-term pain for the business and customers. Under the Privacy Act 1988 and Notifiable Data Breaches scheme,[353] Toll notified the affected individuals and regulators, thus ensuring transparency and victim protection.[354] The recovery involved close collaboration with the Australian Cyber Security Centre and Federal Police, reflecting a policy environment focused on collective resilience and restorative justice at the community level.[355] From a legal standpoint, the Toll Group case highlighted gaps and prompted changes. The absence of a ransom payment meant there was no immediate financial transaction to trace or recover, but it also meant law enforcement's role focused on the investigation and creating deterrence. At the time, there was no specific Australian law criminalizing the act of paying a ransom, but the government has since considered mandatory reporting of ransom demands and even criminalization of ransom payments to deter attackers.[356]

These cases show that recovery from ransomware is a multidimensional challenge that burdens not only an organization's technical defenses and crisis management but also the strength of legal and policy frameworks in place. The United States and Australian case studies show that although victims can recover operations over time,

---

353. *See Notifiable Data Breaches*, OFF. AUSTL. INFO. COMM'R https://www.oaic.gov.au/privacy/notifiable-data-breaches [https://perma.cc/XD52-3T99] (last visited June 11, 2025).

354. Casey Tonkin, *Toll Group Data Dumped on Dark Web*, INFORMATION AGE (May 21, 2020, at 11:23 ET) https://ia.acs.org.au/article/2020/toll-group-data-dumped-on-dark-web.html [https://perma.cc/6NCH-F3N] (" 'As a result, we are now focused on assessing and verifying the specific nature of the stolen data that has been published … [a]s this assessment progresses, we will notify any impacted parties as a matter of priority and offer appropriate support.' ").

355. Australian Cyber Sec. Ctr., *Annual Cyber Threat Report: 1 July 2020 to 30 June 2021,* 34 (2021), https://www.cyber.gov.au/sites/default/files/2023-03/ACSC%20Annual%20Cyber%20Threat%20Report%20-%202020-2021.pdf [https://perma.cc/F56X-3ZGB].

356. DEP'T OF HOME AFFS., *Ransomware Action Plan* 8 (2021) https://www.homeaffairs.gov.au/cyber-security-subsite/files/ransomware-action-plan.pdf [https://perma.cc/86QU-BVMD]; *Cyber Security Act 2024* (Cth) pt III divs 1–2 ss 25–27 (Austl.).

through rebuilding systems, restoring data, and receiving support from law enforcement, the process can be still financially and psychologically grueling. Restorative justice values are evident in the recovery process. First, restitution involves reclaiming losses, including through insurance payouts for damage. Second, repair focuses on rebuilding systems and assisting those harmed. Third, building resilience means drawing lessons from an incident to empower defenses and prevent future incidents.

However, these recovery efforts also expose persistent gaps: Legal regimes have only recently begun catching up to the cyber-attacks scourge. Victims have few formal routes to seek recompense from perpetrators, especially if attackers live in states that do not extradite cybercriminals.[357] As AI-enabled crime and ransomware become more hyper-personalized, restorative tactics emphasizing recovery and resilience are not only theoretically justified, but also practically pivotal.[358] Their proven applicability and measurability make them essential components of an effective and forward-thinking cybercrime legal model. There is a need for legislation and policy to evolve in tandem with the growing threats like ransomware, such as improving international law enforcement collaboration and requiring mandatory

---

357. There have been no publicly reported arrests or prosecutions directly linked to the 2019 Baltimore City ransomware attack and the 2020 Toll Group ransomware incidents. The Toll Group attacks attributed to the MailTo (Netwalker) and Nefilim ransomware variants. *See Toll Group Ransomware Attack*, CYBER SEC. INCIDENT DATABASE (May 5, 2020), https://www.csidb.net/csidb/incidents/5c4a2852-b83f-4314-be79-6297a8728b35/ [https://perma.cc/P3HA-PTB6]; *Baltimore City Government Ransomware Attack,* CYBER SECURITY INCIDENT DATABASE https://www.csidb.net/csidb/incidents/f705dd05-6e95-416c-81af-02bc8960dcf7/ [https://perma.cc/Y553-ZAQ9]. In another case, two Russian nationals operated a cybercrime group deploying Phobos ransomware, which victimized over 1,000 public and private entities worldwide and extorted more than $16 million in ransom payments. Before their arrests by U.S. authorities, the group had operated transnationally for years, frequently evading prosecution due to jurisdictional challenges and the absence of extradition cooperation from certain states. *See* Press Release, U.S. DEP'T OF JUST., Phobos Ransomware Affiliates Arrested in Coordinated International Disruption (Feb. 10, 2025), https://www.justice.gov/opa/pr/phobos-ransomware-affiliates-arrested-coordinated-international-disruption [https://perma.cc/5L6T-KU3P].

358. *See* ROGER A. GRIMES, RANSOMWARE PROTECTION PLAYBOOK 133–154 (2021).

reporting of ransom payments to help authorities trace and combat the threat.

E. The Need for Legal Certainty and Flexibility

The need to balance legal certainty with adequate flexibility to respond to changing technology and criminal dynamics is an important prerequisite for effective cybercrime legislation. These twin objectives safeguard both the rule of law and the capacity to respond to evolving cyber threats.[359]

Utilitarianism provides a robust foundation for this criterion. Bentham argued, laws should maximize social utility by reducing harm and avoiding unnecessary punitive excess.[360] Legal certainty deters crime by making the consequences of unlawful conduct clear to potential offenders. Flexibility, by contrast, allows the law to adapt to emerging threats, such as AI-enabled fraud and industrialized ransomware. Proportionality is a utilitarian ideal, requiring that punishments and regulations align with both deterrence and social benefit.[361] At the same time, cybercrime—being borderless, often anonymous, technologically complex—requires laws that are both stable and adaptable.[362] Stability ensures clear, predictable rules that foster public trust, and facilitate international cooperation.[363] Adaptability is critical because cyber threats evolve quickly through innovations like malware-for-hire services, AI-generated attack tools, and increasingly sophisticated techniques that exploit new vulnerabilities.[364]

---

359. Nicholas Tsagourias, *The Rule of Law in Cyberspace: A Hybrid and Networked Concept?,* 80 ZEITSCHRIFT FÜR AUSLÄNDISCHES ÖFFENTLICHES RECHT UND VÖLKERRECHT [J. Foreign Pub. L. & Int'l L.] 433, 445–46 (2020) (Ger.).

360. McHugh, *supra* note 260, at 10.

361. *Id.* at 2.

362. Patricia Scotland, *Foreword* to N. IFEANYI-AJUFO, COMMONWEALTH COUNTRIES' CYBERCRIME LAWS: AN OVERVIEW vii (2024) https://eprints.leedsbeckett.ac.uk/id/eprint/11552/ [https://perma.cc/F9BZ-RAZ5] (U.K.).

363. *See* Owens & Wedeking, *supra* note 287.

364. Scotland, *supra* note 362, at 97.

Flexible laws should not only respond to technological changes but also promote innovation and economic growth.[365] Criminal law must be clear and predictable to uphold rational legality, but it must also adapt to social, technological, and transnational challenges.[366] Flexibility is a *structural* feature, that keeps the law relevant in dealing with complicated and growing crimes, such as cybercrime. This blend of stability and adaptability is critical for effective cybercrime legislation, and closely linked to Bentham's utilitarianism and the modern codification movement.[367] Clarity and predictability promote deterrence and fairness. Flexibility guarantees that the law can respond to new and unforeseen developments,[368] creating an essential balance between stability and responsiveness.

V. CONCLUSION

As technological innovations constantly redefine the world of cybercrime, a robust theoretical model for developing effective cybercrime legislation becomes increasingly important. This Article develops a structured model using grounded principles drawing from leading criminal law theories, setting out the core criteria for effective cybercrime legislation.

The first criterion is legal clarity guided by deterrence theory. Legal clarity is believed to be vital for balancing security with commercial freedom and for combating the global, borderless, and anonymous character of cybercrime. Effective legislation must clearly define criminal behaviors while respecting legitimate commercial activities, facilitating international cooperation, and improving prevention.

Second, proportional and consistent penalties drawn from retributive justice theory are critical to address the automation and scalability of

---

365. *See id.*

366. Simon Bronitt, *Towards a Universal Theory of Criminal Law: Rethinking the Comparative and International Project*, 27 CRIM. JUST. ETHICS 53, 56 (2008).

367. *See id.* at 57–58.

368. *Id.* at 56 ("The truth is, that the law is always approaching, and never reaching, consistency. It is forever adopting new principles from life at one end, and it always retains old ones from history at the other, which have not yet been absorbed or sloughed off. It will become entirely consistent only when it ceases to grow.") (quoting OLIVER WENDELL HOLMES, THE COMMON LAW 36 (1923)).

cybercrime. Recent legislative frameworks, such as the United States' Cyber Incident Reporting for Critical Infrastructure Act of 2021 and Australia's Cyber Security Act 2024, promote the importance of economically informed sanctions in deterring large-scale automated cyber offenses like AI-enabled ransomware.

Third, restorative justice underscores the need for recovery and resilience measures in commerce, addressing the hyper-personalization that marks emerging forms of cybercrime. Incidents such as the 2019 ransomware attack on Baltimore and the 2020 attack on Australia's Toll Group, discussed above, show how restorative practices can aid victim recovery as well as strengthen the resilience of cyber systems.

Fourth, legislation must strike a balance between legal certainty and flexibility, a principle grounded in utilitarian thought. Such adaptability is not just beneficial but essential to ensure a law to be fair, relevant, and effective in confronting rapidly evolving cyber threats.[369] Recent studies indicate that cybercriminals tend to adopt new technologies quickly, choosing tools that offer high rewards with relatively low risk.[370] This pace requires the need for legal frameworks that are forward-looking yet stable; anticipating disruptive applications of AI without quickly becoming outdated.

This model rests on four normative criteria: legal clarity, proportional penalties, restorative resilience, and adaptive certainty. Together, these principles provide a framework that is both evaluative and prescriptive. They allow for a sharper assessment of existing cybercrime legislation while pointing the way toward doctrinal refinement and policy innovation. Each criterion reflects a distinct theoretical foundation while responding to observable traits in current cyber offending: (a) automation and large-scale attack capabilities; (b) hyper-personalization of targets; (c) exploitation of psychological vulnerabilities; (d) anonymity and complexity in

369. Bronitt, *supra* note 366, at 56–57.

370. Vincenzo Ciancaglini & David Sancho, *Back to the Hype: An Update on How Cybercriminals Are Using GenAI*, TREND MICRO (May 8, 2024), https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/back-to-the-hype-an-update-on-how-cybercriminals-are-using-genai [https://perma.cc/44SN-5EYW].

detection; and (e) inherently global operational reach. The model's prognosis that AI-driven threats will dominate twenty-first century criminal law discourse, is undoubtedly correct, and its structured approach may well guide legislative responses to ransomware, adversarial AI, and other emergent cyber pathologies.

While this model advances cybercrime legislation, its limitations must be acknowledged. First, theoretical assumptions often falter in systems with diverse traditions, as seen in Australia's federated enforcement model[371] or the EU's harmonized regulatory paradigm,[372] where centralized doctrines clash with decentralized operational realities.[373] Second, in many developing countries, limited resources and fragmented cyber systems,[374] make it difficult to implement criteria of proportionality and adaptive certainty. Third, an emphasis on restorative resilience presents difficulty in the possibility of overlooking areas where localized adaptations are essential, such as Indigenous data governance in Australia.[375] Furthermore, while this model offers an integrated and structured foundation for assessing effective cybercrime legislation, it is not presented as a definitive blueprint. As Dubber suggests, criminal law theorists are not passive observers but part of an interpretive tradition that shapes legal evolution through critique, comparison, and engagement.[376]

---

371. Peter Hanks, *'Inconsistent' Commonwealth and State Laws: Centralizing Government Power in the Australian Federation*, 16 FED. L. REV. 107, 108 (1986) (Austl.).

372. Philipp Eckhardt & Anastasia Kotovskaia, *The EU's Cybersecurity Framework: The Interplay Between the Cyber Resilience Act and the NIS 2 Directive*, 4 INT'L CYBERSECURITY L. REV. 147, 147–49 (2023).

373. Mark Raymond, *Managing Decentralized Cyber Governance: The Responsibility to Troubleshoot*, 10 STRATEGIC 123, 125–26 (2016).

374. *Enhancing Cyber Resilience in Developing Countries*, WORLD BANK (Jan. 29, 2025), https://www.worldbank.org/en/results/2025/01/29/-enhancing-cyber-resilience-in-developing-countries [https://perma.cc/NTR4-VJHY].

375. James Rose, Marcia Langton, Kristen Smith & Darren Clinch, *Indigenous Data Governance in Australia: Towards a National Framework*, 14 INT'L INDIGENOUS POL'Y J. 1, 8 (2023) (Austl.).

376. Markus D. Dubber, *Comparative Criminal Law, in* THE OXFORD HANDBOOK OF COMPARATIVE LAW 1278 (Mathias Reimann & Reinhard Zimmermann eds., 2019) ("All comparative law carries critical, even subversive, potential by exposing the relativity of apparently ironclad rules. The mere existence of

footnote continued on next page

In constructing a theoretical model for cybercrime law, the scholar takes part in this interpretive tradition: shaping the evolution of legal norms through scholarship, litigation, and reform. Moreover, in the digital age, this role becomes even more critical, as what is needed is not a single grammar of cybercrime law,[377] but a polyphonic dialogue between global standards and situated justice.[378] It is said that the path forward requires both intellectual boldness and contextual sensitivity in iterative collaboration: refining this model through comparative case studies, such as Association of Southeast Asian Nations ("ASEANs") cybercrime harmonization efforts, while embedding safeguards against 'one-size-fits-all' imperialism.[379] Only through such calibrated balance can global cybercrime law achieve its dual mandate: empowering law enforcement and preserving the pluralism inherent to legal systems.[380]

alternative rules suggests that alternatives are possible; and if alternatives are possible, it is only a small step to the suggestion that they might be preferable.")

377. *See* Miriam Gur-Arye, *The Nature of Crime: A Synthesis, Following the Three Perspectives Offered in The Grammar of Criminal Law*, 27 CRIM. JUST. ETHICS 91, 91 (2008); George P. Fletcher, *Responses to the Critiques of The Grammar of Criminal Law*, 27 CRIM. JUST. ETHICS 99, 103 (2008).

378. *See* Xin Wang, *Global (Re-)Framing of Cybercrime: An Emerging Common Interest in Flux of Competing Normative Powers?*, 38 LEIDEN J. INT'L L. 235, 237 (2024) (Neth.).

379. Dubber, *supra* note 376, at 1296.

380. *See* PAUL SCHIFF BERMAN, THE OXFORD HANDBOOK OF GLOBAL LEGAL PLURALISM 30 (2020).