Investigating Cybercrime: The Key Jurisdictional and Technical Challenges Faced by Law Enforcement and Ways to Address Them

Hayden Coupland

Abstract

The rapid expansion of cyberspace has created significant opportunities but also introduced new threats in the form of cybercrimes. Law enforcement agencies are increasingly challenged in investigating these crimes due to the complex, transnational nature of the internet. This paper examines the key jurisdictional and technical obstacles that hinder effective cybercrime investigations and explores strategies to overcome these challenges. Jurisdictional challenges primarily arise from the global nature of cybercrimes. Disparate legal frameworks, conflicting international laws, and limited cooperation between countries further complicate the ability of agencies to investigate and prosecute offenders. On the technical front, cybercrimes often exploit sophisticated technologies that evolve faster than the capabilities of law enforcement agencies. Encryption, anonymisation tools, and the use of dark web platforms make it increasingly difficult for investigators to track cybercriminals, especially given the limitations of their forensic tools and training. Having established the challenges, the article discusses some approaches to reform and suggests a multifaceted approach to improving cybercrime investigations combining investing in advanced training, better resource allocation, and public–private partnerships to enhance investigative capabilities, while also supporting the existing calls for legal harmonisation.

1 Introduction

The rapid advancement of technology has profoundly transformed the landscape of crime, with cybercrime appearing as a significant threat to global security. Law enforcement agencies worldwide are grappling with the dual challenges of jurisdictional and technical complexities in their efforts to investigate and combat cybercrimes. These crimes, which encompass a wide range of illegal activities including hacking, identity theft, online fraud, and cyber espionage, often transcend national borders, creating intricate legal dilemmas regarding jurisdiction.[1] Moreover, the sophisticated technical means employed by cybercriminals, such as encryption, anonymisation tools, and the dark web, further complicate the investigative process.[2]

The primary aim of this article is to dissect these challenges and propose practical strategies to enhance the efficacy of cybercrime investigations. The paper thus does three things: first, it delineates the scope and nature of the jurisdictional and technical challenges of investigating cybercrime; second, it analyses the current relevant measures and their shortcomings; and third, it proposes improved strategies for future cybercrime investigations.

2 Overview of Cybercrime and Its Societal Impact

Cybercrime stands for a profound challenge to modern society, fundamentally reshaping how individuals, corporations, and governments view security in the digital age. As Wall asserts, the rapid expansion of digital infrastructures has simultaneously created fertile ground for malicious activities, making cybercrime not just a technological issue, but one that permeates economic, societal, and psychological realms.[3] Brenner concurs, noting that the borderless nature of cyberspace amplifies the complexity of combating cybercrime, with both personal and corporate entities at heightened risk.[4] This multifaceted threat impacts global economies, with McGuire and Dowling estimating the economic toll to exceed trillions annually, when factoring in financial losses, business interruptions, and long-term reputational damage.[5]

---

[1] Susan W. Brenner, *Cybercrime: Criminal Threats from Cyberspace* (Praeger 2010); Marc Goodman, *Future Crimes: Inside the Digital Underground and the Battle for Our Connected World* (Doubleday 2015).
[2] Thomas J. Holt, Adam M. Bossler, and Kathryn C. Seigfried-Spellar, *Cybercrime and Digital Forensics: An Introduction* (2nd edn, Routledge 2017); Roderic Broadhurst et al., 'An Analysis of the Nature of Groups Engaged in Cyber Crime' (2014) 8 International Journal of Cyber Criminology 1.
[3] David S. Wall, *Cybercrime: The Transformation of Crime in the Information Age* (Polity 2007).
[4] Susan W. Brenner, *Cybercrime: Criminal Threats from Cyberspace* (Praeger 2010).
[5] Michael McGuire and Samantha Dowling, *Cybercrime: A Review of the Evidence* (Home Office Research Report 75, 2013).

Further, on an individual level, the increasing vulnerability of citizens to offences such as identity theft, financial fraud, and violations of privacy are of serious worry. The psychological toll of these crimes is significant, often leading to trauma, a diminished sense of security, and a pervasive distrust of online platforms.[6] Deeply personal crimes disrupt daily life, presenting a complex challenge to law enforcement and regulatory agencies, especially where individuals are unaware of the full extent of the damage until it's too late, as is true for many cybercrime cases, exacerbating the emotional and financial costs experienced.[7]

Corporations, likewise, are prime targets for cybercriminals. Businesses, especially those operating critical infrastructures, face existential threats from cyberattacks, which can result in financial losses and operational paralysis. Holt and Bossler underscore the transformative impact of cybercrime on corporate operations, pointing to the rise of sophisticated attacks such as ransomware and data breaches, which pose significant financial burdens. These threats are further compounded by the complex digital ecosystems in which corporations run, creating a challenging environment for ensuring robust cybersecurity measures.[8]

The societal implications of cybercrime extend beyond immediate economic damage. Yar insists that cybercrime undermines public trust in the digital infrastructures that form the backbone of contemporary life, stifling technological innovation and slowing societal progress, highlighting that the pervasive threat of cyberattacks represents a substantial barrier to further digital transformation.[9] The critical role of public trust in supporting digital security cannot be overstated, with Goodman warning that without significant improvements in cybersecurity, the social contract between citizens and digital systems is at risk of breaking down completely.[10]

Consequently, the social ramifications of cybercrime manifest in more insidious ways, particularly in relation to online harassment and exploitation. An interesting investigation done by Holt and Bossler explores the rise of cyberbullying and the exploitation of children through online platforms, illustrating how the anonymity and reach of the internet have worsened these problems. Such crimes not only have severe psychological impacts on victims but also

---

[6] Robert Moore, *Cybercrime: Investigating High-Technology Computer Crime* (Anderson 2010); Marc Goodman, *Future Crimes: Inside the Digital Underground and the Battle for Our Connected World* (Doubleday 2015).
[7] Michael McGuire and Samantha Dowling, *Cybercrime: A Review of the Evidence* (Home Office Research Report 75, 2013).
[8] Thomas J. Holt and Adam M. Bossler, *Cybercrime in Progress: Theory and Prevention of Technology-Enabled Offences* (Routledge 2015).
[9] David S. Wall, *Cybercrime: The Transformation of Crime in the Information Age* (Polity 2007); Majid Yar, *Cybercrime and Society* (2nd edn, SAGE Publications 2013).
[10] Marc Goodman, *Future Crimes: Inside the Digital Underground and the Battle for Our Connected World* (Doubleday 2015).

represent a significant challenge for law enforcement agencies, who must navigate evolving technologies while addressing public demand for enhanced protections.[11]

3 Legal Framework for Cybercrime Investigation

A legal framework for cybercrime investigations is essential in addressing the complexities of a rapidly evolving digital landscape. However, it currently remains rife with inconsistencies, fragmentation, and limitations that hinder effective enforcement and cross-border cooperation. This section critically examines international treaties, national legislation, and case law to highlight the challenges and contradictions that undermine the investigation of cybercrime. A close analysis of these frameworks shows how they simultaneously support and obstruct law enforcement efforts in responding to cyber threats.

3.1 International Treaties and Agreements: Harmonisation vs Fragmentation

International treaties such as the Council of Europe's Convention on Cybercrime in Budapest 2001 are often praised for setting a common legal standard to combat cybercrime. The Budapest Convention, the first international treaty specifically addressing cybercrime, encourages cooperation among states in investigating cyber offences, particularly those with cross-border elements. Yet, its efficacy is undermined by the absence of major players like China and Russia, creating jurisdictional gaps where cybercriminals can evade justice by operating in non-signatory states. This omission exemplifies how geopolitical considerations weaken the harmonising potential of such treaties.[12]

The United Nations Convention against Transnational Organized Crime 2000, although broader in scope, also addresses cybercrime as part of global crime prevention efforts. Like Budapest, its implementation is hampered by the slow pace of international cooperation, particularly in terms of accessing digital evidence. This challenge is further complicated by the reliance on mutual legal assistance treaties (MLATs), which are cumbersome and ineffective in cases requiring rapid access to volatile data.[13]

---

[11] Thomas J. Holt and Adam M. Bossler, *Cybercrime in Progress: Theory and Prevention of Technology-Enabled Offences* (Routledge 2015).
[12] Convention on Cybercrime of the Council of Europe (ETS No. 185, Budapest, 23 November 2001).
[13] United Nations, United Nations Convention against Transnational Organized Crime (2000).

Regional frameworks such as the Inter-American Convention on Cybercrime 1999[14] and the African Union Convention on Cyber Security and Personal Data Protection 2014[15] aim to address cybercrime within specific geographical regions, yet they face similar challenges. Inconsistent legal standards across countries lead to difficulties in enforcing laws, while the lack of widespread adoption further fragments global efforts to effectively tackle the problem. The APEC Cybersecurity Strategy 2005[16] and the NATO Tallinn Manual 2014[17] contribute to regional security but are limited in scope, often reflecting the geopolitical interests of their respective members rather than establishing universally applicable norms.

Moreover, the Additional Protocol to the Convention on Cybercrime 2003, which aims to combat acts of racism and xenophobia committed through computer systems, reveals another layer of complexity in cybercrime law. While it expands the scope of criminalisation, it introduces new legal challenges, especially when addressing freedom of speech concerns and differing national approaches to hate speech including acts of a racist and xenophobic nature.[18]

3.2 National and Regional Legislation: Contradictions

At the national level, countries adopt a variety of legal frameworks to address cybercrime, but these frameworks often conflict with one another, creating legal grey zones for multinational corporations and law enforcement. The Computer Fraud and Abuse Act (CFAA) is a cornerstone of US cybercrime law. Having said this, its broad interpretation of "unauthorised access" has led to criticism for criminalising legitimate activities, such as security research, which could otherwise enhance cybersecurity. This overreach results in a chilling effect, stifling necessary innovation and collaboration between private sector entities and law enforcement.[19]

In the European Union (EU), the General Data Protection Regulation (GDPR) aims to protect individual privacy but complicates cybercrime investigations by limiting the sharing of personal data across borders, especially sharing with non-EU countries. The EU Directive 2013/40/EU[20] on attacks against information systems strengthens the legal framework for

[14] Organization of American States, Inter-American Convention on Cybercrime (1999).
[15] African Union, Convention on Cyber Security and Personal Data Protection (2014).
[16] Asia-Pacific Economic Cooperation (APEC), APEC Cybersecurity Strategy (2005).
[17] NATO Cooperative Cyber Defence Centre of Excellence, Tallinn Manual on the International Law Applicable to Cyber Warfare (2nd edn, CUP 2017).
[18] Council of Europe, Additional Protocol to the Convention on Cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems (Strasbourg, 2003).
[19] Computer Fraud and Abuse Act (CFAA), 18 USC 1030 (United States).
[20] Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA [2013] OJ L218/8.

addressing cyberattacks but remains constrained by the GDPR's stringent data privacy rules, particularly in interactions with US law, which is governed by the Clarifying Lawful Overseas Use of Data Act (CLOUD) Act. This results in legal uncertainty for multinational corporations caught between conflicting legal obligation.[21]

In Japan, the Act on Prohibition of Unauthorised Computer Access focuses on unauthorised access as a criminal offence yet lacks clear provisions for international cooperation, limiting its efficacy in addressing global cybercrime networks.[22] Similarly, the Cybercrime Act (Australia, 2001) and Information Technology Act (India, 2000) highlight the national focus on combating cybercrime but fall short of providing mechanisms for effective cross-border enforcement.[23] In contrast to these examples, Germany's Strafgesetzbuch (StGB) Sections 202a and 202b, which criminalise data espionage, set strict standards for prosecuting unauthorised access to digital data, reflecting the country's emphasis on data protection. Although on the right track, this strictness also complicates international cooperation, particularly in balancing data privacy with the need for law enforcement to access critical information.[24]

3.3 Case Studies: Jurisdictional Ambiguities

The complexities of cybercrime jurisdiction are vividly illustrated in case law, where courts wrestle with the borderless nature of cyberspace. *Microsoft Ireland*[25] highlighted the challenge of accessing data stored overseas, as the U.S. government sought to compel Microsoft to hand over emails stored on servers in Ireland. The case underscored the legal uncertainty regarding the extraterritorial application of national laws to data stored in foreign jurisdictions. Although the issue was addressed through the CLOUD Act, which allows US authorities to request data stored abroad, it still fails to resolve the deeper tension between national sovereignty and global digital infrastructures.[26]

Yahoo!, Inc. v. LICRA starkly illustrates the jurisdictional challenges within cyberspace. A French court ordered Yahoo! to block French users from accessing Nazi memorabilia on its US-based platform, despite such content being legal under US law. This case ignited heated

[21] General Data Protection Regulation (GDPR), Regulation (EU) 2016/679 (European Union); Clarifying Lawful Overseas Use of Data Act (CLOUD Act), 18 USC Chapter 119 (United States).
[22] Act on Prohibition of Unauthorised Computer Access (1999) (Japan).
[23] Information Technology Act 2000 (India); Cybercrime Act 2001 (Cth) (Australia).
[24] Strafgesetzbuch (StGB) Section 202a and 202b (Germany).
[25] *Microsoft Corp. v United States* 829 F.3d 197 (2d Cir. 2016).
[26] Ibid.

debate over the extent to which a nation may impose its laws on foreign entities operating online, and how such extraterritorial enforcement aligns with principles of sovereignty and free expression. It exemplifies the clash between national sovereignty and the borderless nature of the internet, raising critical questions about the limits of jurisdictional authority in cyberspace.[27]

Similarly, the *Google LLC v. CNIL*[28] ruling by the Court of Justice of the European Union (CJEU) addressed the "right to be forgotten" under the GDPR. The CJEU ruled that this right does not extend globally, reflecting the court's reluctance to impose EU data protection standards on non-EU entities. However, this decision leaves a significant gap in protecting EU citizens from cyberthreats emanating from jurisdictions with weaker privacy protections.[29]

The *United States v. Ivanov* case[30] involving a Russian hacker prosecuted under US law for crimes committed outside the United States, is a critical case in understanding the jurisdictional challenges in prosecuting cybercriminals operating in foreign countries. Despite the significant harm caused within US borders, the prosecution struggled with enforcing the judgment due to the hacker's location being within a noncooperative jurisdiction, further showcasing the limitations of current international frameworks for addressing cross-border cybercrime.[31]

In assessing the current legal framework for cybercrime investigations – international, regional, national, it is obvious that, though well-intentioned, suffer from fragmentation and jurisdictional conflicts that undermine their effectiveness. A combination of missing key actors, conflicting priorities between privacy and security, and persistent jurisdictional ambiguities make prosecuting cross-border cybercrime exceedingly difficult. The legal framework then must evolve toward greater international collaboration, clearer jurisdictional boundaries to be more effective.

4 Jurisdictional and Technical Challenges in Cybercrime Investigations Background

[27] *Yahoo! Inc v LICRA* [2006] 433 F 3d 1199 (9th Cir); Jack Goldsmith and Tim Wu, *Who Controls the Internet? Illusions of a Borderless World* (OUP 2006).
[28] *Google Inc. v Commission nationale de l'informatique et des libertés (CNIL) Case* C-507/17 (Court of Justice of the European Union, 24 September 2019).
[29] *Google Spain SL, Google Inc. v Agencia Española de Protección de Datos (AEPD), Mario Costeja González* (Case C-131/12) [2014] ECR I-317.
[30] *United States v Ivanov* 175 F Supp 2d 367 (D Conn 2001).
[31] Ibid.

The jurisdictional and technical barriers confronting law enforcement in the digital realm are arguably among the most pressing issues in cybercrime investigation. The inherently transnational nature of cybercrime is noted as one of the primary obstacles, demonstrating that cybercriminals can operate from any location with internet access, rendering traditional notions of territorial jurisdiction inadequate. Existing legal frameworks, which are often predicated on geographical boundaries, fail to account for the borderless nature of cyberspace. This lack of legal cohesion leads to significant delays in investigations, as law enforcement agencies must navigate a labyrinth of divergent national laws and often cumbersome MLATs.[32] Also, cross-border investigations require extensive collaboration between law enforcement agencies and the absence of streamlined processes and the frequent lack of trust between jurisdictions often hinder progress. For example, the acquisition of electronic evidence from foreign servers can be delayed for months, if not years, impeding timely investigations.[33]

On the technical side, the proliferation of encryption and anonymisation technologies poses significant challenges for cybercrime investigations. Brenner points out that the widespread use of such technologies enables criminals to evade detection, a consequence of which results in law enforcement agencies unable to trace illicit activities effectively.[34] Moreover, dark web marketplaces, which are heavily reliant on encryption and anonymity, have become hubs for cybercriminal activities, further complicating efforts to identify and apprehend offenders by law enforcement agencies.[35] Even when law enforcement *can* track cybercriminals, the admissibility of digital evidence in court remains a contentious issue for our legal system, with many legal systems ill-equipped to handle the intricacies of digital forensics with the procedures in place today.[36]

4.1 Jurisdictional Challenges in Cybercrime Investigations

Jurisdictional challenges in cybercrime investigations reveal more than mere procedural hurdles; they highlight systemic deficiencies within the global legal framework. A pertinent illustration of jurisdictional ambiguities is the example of a cybercriminal in Country A hacking a server in Country B, causing financial harm to victims in Country C. The question of which

---

[32] David S. Wall *Cybercrime: The Transformation of Crime in the Information Age* (Polity 2007); Susan W. Brenner (*Cybercrime: Criminal Threats from Cyberspace* (Praeger 2010).
[33] Smith RG, and Grabosky P and Urbas G, *Cyber Criminals on Trial* (Cambridge University Press 2004)
[34] Susan W. Brenner, *Cybercrime: Criminal Threats from Cyberspace* (Praeger 2010).
[35] David S. Wall *Cybercrime: The Transformation of Crime in the Information Age* (Polity 2007).
[36] Thomas J. Holt and Adam M. Bossler, *Cybercrime in Progress: Theory and Prevention of Technology-Enabled Offences* (Routledge 2015).

country holds the jurisdiction to investigate and prosecute becomes fraught with complexity. While the principle of extraterritoriality allows states to claim jurisdiction over acts committed beyond their borders, provided these acts have a significant impact within their territory, its application remains inconsistent and frequently contested.

These challenges accentuate the discord between the inherently global nature of cyberspace and the territorially confined legal systems of sovereign states. This section offers a sophisticated examination of how jurisdictional conflicts undermine the efficacy of cybercrime investigations, alongside a critical exploration of potential strategies for harmonising the global legal order to better address these transnational crimes.

4.1.1 Jurisdictional and Legal Principles in Cyberspace

The traditional principles of jurisdiction are increasingly inadequate when applied to the digital realm. The principle of "territoriality", which grants states authority over activities within their geographic boundaries, is fundamentally challenged by the borderless nature of cyberspace.[37] In cyberspace, where digital interactions defy physical boundaries, the principle of territoriality becomes anachronistic and is unable to accommodate the fluid and ubiquitous nature of cyber activities.[38]

The principle of territoriality, long central to legal theory, asserts that a state has jurisdiction over crimes committed within its borders. Yet, applying this doctrine to cybercrime proves increasingly problematic, as offences such as hacking, online fraud, and data breaches frequently span multiple jurisdictions. The rigidity of territoriality often leaves significant enforcement gaps, particularly when the perpetrator, victim, and the digital infrastructure used in the crime reside in different countries.

The effects doctrine, which permits a state to assert jurisdiction based on the effects of a cybercrime within its territory, offers a partial remedy but introduces significant complexities.[39] While this doctrine provides a basis for pursuing cybercriminals whose actions affect multiple jurisdictions, it also risks jurisdictional overreach, leading to conflicts between sovereign states. The application of the effects doctrine often results in overlapping jurisdictions, where

---

[37] David R. Johnson and David G. Post, 'Law and Borders: The Rise of Law in Cyberspace' (1996) 48(5) Stanford Law Review 1367; Lawrence B. Solum, 'Models of Internet Jurisdiction' (1998) 1998(4) University of Illinois Law Review 1017.

[38] Anthony D. Trotter, 'Jurisdiction in Cyberspace: Rights and Regulation' (2010) 108(8) Michigan Law Review 1.

[39] Jack L. Goldsmith, 'Against Cyberanarchy' (1998) 65(4) University of Chicago Law Review 1199.

multiple states claim authority based on perceived impacts, thus creating a fragmented enforcement landscape.[40] This fragmentation not only allows cybercriminals to exploit legal inconsistencies but also impedes effective prosecution, undermining the rule of law in cyberspace.[41]

The fundamental mismatch between the global reach of cyber activities and the territorially confined nature of legal systems lies at the heart of jurisdictional challenges in cybercrime investigations. The complexities of territoriality become particularly acute in cases involving multiple jurisdictions, each governed by distinct legal standards and procedural norms.[42] These conflicts are further exacerbated by divergent laws governing cross-border data access, where critical evidence may be stored in jurisdictions with stringent data protection laws, thereby complicating or obstructing law enforcement access.[43]

The principle of double criminality, an element of extradition treaties and MLATs, which requires a crime to be recognised in both the requesting and requested jurisdictions, often impedes the extradition of cybercriminals, particularly in cases where national laws differ significantly.[44] This lack of uniformity in cybercrime legislation across countries creates a fragmented legal landscape that cybercriminals can exploit, often operating from jurisdictions with inadequate enforcement mechanisms.[45] Such exploitation not only constitutes a procedural barrier but also undermines the integrity and effectiveness of international law in the digital era.

4.1.2 Legal Fragmentation

The legal fragmentation within national cybercrime laws has concrete and often detrimental effects on the enforcement of cyber laws. This fragmentation is particularly pronounced in cross-border hacking cases, where the legal frameworks of involved countries may directly conflict.[46] Such conflicts arise from differences in both substantive law – how crimes are

---

[40] Susan W. Brenner, 'Cybercrime Jurisdiction' in Susan. W. Brenner, *Cybercrime: The Transformation of Crime in the Information Age* (Polity 2006).
[41] Dan Jerker B. Svantesson, *Internet Jurisdiction and Choice of Law: Legal Practices in the EU, US and China* (Kluwer Law International 2017).
[42] Dan Jerker B. Svantesson, 'A New Jurisprudence for the Internet?' (2019) 30(3) European Journal of International Law 1071.
[43] Ronald J. Deibert and Masashi Crete-Nishihata, 'Global Governance and the Spread of Cyberspace Controls' (2012) 18(3) Global Governance 339.
[44] M. Cherif Bassiouni, *International Criminal Law: Volume III: Enforcement* (Martinus Nijhoff Publishers 2008).
[45] Abraham D. Sofaer and Seymour E. Goodman, 'Cyber Crime and Security: The Transnational Dimension' in Abraham D. Sofaer and Seymour E. Goodman (eds), *Transnational Dimension of Cyber Crime and Terrorism* (Hoover Institution Press 2001).
[46] Jonathan Clough, *Principles of Cybercrime* (Cambridge University Press 2010).

defined – and procedural law – how evidence is gathered and presented. The lack of harmonisation among national legal frameworks creates a fragmented legal environment in which cybercriminals can manoeuvre with relative ease. Conflicts are then exacerbated by varying national priorities – such as differing approaches to privacy versus security – which can lead to legal impasses that delay or even preclude justice.[47]

The global scale of cybercrime and its jurisdictional challenges are vividly illustrated by real-world examples. The 2017 WannaCry ransomware attack, which affected over 200,000 computers across 150 countries, is a case in point. Attributed to North Korean hackers, the attack exploited vulnerabilities in Microsoft Windows, encrypting users' data and demanding ransom payments in Bitcoin. Coordinating international efforts to trace the attackers and mitigate damage underscored the difficulty of managing a cybercrime spanning multiple jurisdictions. Kuerbis and Badiei highlight the challenges faced by international law enforcement agencies in responding to such a widespread cyberattack, citing the consensus held amongst scholars and experts emphasising the need for more effective global cooperation and information sharing.[48]

The extraterritorial application of laws, exemplified by the US CLOUD Act, further complicates the legal landscape. Although intended to facilitate international data access for law enforcement, such laws often clash with foreign data protection regimes, creating significant legal uncertainties for multinational companies.[49] These companies, caught between conflicting legal obligations, face severe financial and reputational risks, underscoring the urgent need for harmonised international legal standards that effectively balance cybercrime enforcement with respect for national sovereignty and legal traditions.[50]

Conflicting legal standards are particularly problematic in cases involving data protection laws, such as the GDPR, which often clashes with US data disclosure requirements under laws like the CLOUD Act. These conflicts create a complex legal landscape, delaying investigations or, in some cases, rendering the collection of critical evidence impossible. Such legal conflicts can impede the flow of information necessary for cybercrime investigations, highlighting the need

---

[47] Jakub Kulesza, *International Internet Law* (Routledge 2012).
[48] Brenden Kuerbis and Farzaneh Badiei, *Mapping the Cybercrime Ecosystem: Deterring Cybercrime and Increasing Cooperation* (Georgia Tech University 2017).
[49] Urs Gasser, and John Palfrey, *Breaking Down Digital Barriers: When and How ICT Interoperability Drives Innovation* (Berkman Klein Center Research Publication 2007).
[50] Dan Jerker B. Svantesson, *Internet Jurisdiction and Choice of Law: Legal Practices in the EU, US and China* (Kluwer Law International 2017).

for greater harmonisation of data protection laws at the international level.[51] Furthermore, the reluctance of certain countries to extradite their nationals complicates prosecutions, exacerbated by outdated treaties that fail to address the realities of cybercrime. The lack of effective extradition agreements for cybercrime suspects undermines international efforts to bring perpetrators to justice, calling for the modernisation of extradition treaties to reflect the transnational nature of cybercrime.[52]

The struggle to balance data privacy with security concerns highlights the broader challenge of developing a cohesive global legal framework for cybercrime. The absence of such a framework exacerbates jurisdictional challenges, impeding effective law enforcement and undermining global cybersecurity efforts.[53] This situation demands immediate attention from the international legal community to establish integrated and universally accepted legal standards for addressing cybercrime.[54]

4.2 Artificial Intelligence: An Emerging Jurisdictional Challenge

The growing integration of artificial intelligence (AI) into cybercriminal activities introduces novel jurisdictional complexities that traditional legal frameworks struggle to address. AI can automate cyberattacks, making them more difficult to trace and attribute, while operating autonomously across multiple jurisdictions. These developments raise pressing questions about where such crimes are "committed", and which legal systems should hold jurisdiction.

From a legal perspective, the use of AI in law enforcement – particularly in cross-border surveillance – raises concerns about extraterritorial privacy violations. AI-driven surveillance tools may collect data in ways that infringe on the privacy laws of other countries, highlighting the need for legal frameworks that address both AI's unique characteristics and its role in cybercrime.[55] Wagner emphasises that the deployment of AI in law enforcement must be accompanied by robust legal safeguards to protect individual privacy and ensure compliance with international human rights standards.[56] The extraterritorial use of AI surveillance tools

---

[51] Christopher Kuner, 'The Internet and the Global Reach of EU Law' in B. Van der Sloot, D. Broeders and E. Schrijvers (eds*), Exploring the Boundaries of Big Data* (Amsterdam University Press 2020).
[52] M. Cherif Bassiouni, *International Extradition: United States Law and Practice* (6th edn, OUP 2014).
[53] Ronald J. Deibert and Masashi Crete-Nishihata, 'Global Governance and the Spread of Cyberspace Controls' (2012) 18(3) Global Governance 339.
[54] Jack Goldsmith and Tim Wu, *Who Controls the Internet? Illusions of a Borderless World* (OUP 2006).
[55] Ben Wagner, 'AI and Policing: Ethical and Legal Implications' in M. Hildebrandt and K. O'Hara (eds), *Life and the Law in the Era of Data-Driven Agency* (Edward Elgar Publishing 2021).
[56] Ibid.

poses significant legal and ethical challenges, necessitating a careful balancing of security and privacy considerations.

The challenge of assigning accountability in AI-driven cybercrime further complicates jurisdictional issues. Legal frameworks typically assume human actors with clear intent, but AI can autonomously perform actions without direct human oversight. Determining whether responsibility lies with the programmer, user, or system owner becomes a vexing legal question. As noted by Mantelero, the legal principles developed for traditional forms of cybercrime may not be adequate for addressing the complexities introduced by AI. The autonomous nature of AI systems challenges the existing notions of intent and responsibility, requiring a rethinking of legal doctrines to effectively address AI-driven cybercrime.[57]

4.2.1 AI use by law enforcement: Legal and Ethical Implications

The integration of advanced technologies into cybercrime investigations raises critical legal and ethical questions, particularly regarding the tension between security and privacy. The GDPR underscores this conflict, imposing stringent data protection standards that complicate law enforcement efforts to collect and utilise digital evidence.[58] While these regulations are essential for safeguarding individual privacy, they may inadvertently hinder the effective investigation of cybercrime, particularly when evidence is located across multiple jurisdictions.

The ethical implications of AI and machine learning (ML) in law enforcement are profound. Predictive policing, for example, raises concerns about discriminatory practices, particularly where AI systems are used to forecast criminal behaviour. The potential for AI to exacerbate existing biases, particularly against marginalised groups, cannot be overlooked.[59] These technologies, if left unchecked, could erode civil liberties, leading to a surveillance state where privacy is sacrificed in the name of security. Robust legal frameworks and oversight mechanisms must be instituted to ensure transparency, accountability, and respect for fundamental rights.

5 Technological Challenges in Cybercrime Investigations

[57] Alessandro Mantelero, 'AI and Big Data: A Blueprint for a Human Rights, Social and Ethical Impact Assessment' (2019) 34 Computer Law & Security Review 754.
[58] Paul Voigt and Axel von dem Bussche, *The EU General Data Protection Regulation (GDPR): A Practical Guide* (Springer 2017).
[59] Elizabeth E. Joh, 'Policing by Numbers: Big Data and the Fourth Amendment' (2019) 89(1) Washington Law Review 35.

The challenges that law enforcement agencies face in investigating cybercrime are multifaceted and deeply entrenched in the rapid evolution of technology and its interplay with law, policy, and resources. Cybercrime, by its very nature, defies traditional legal and operational frameworks. The pace of technological advancements, the global nature of cybercrime, and the resource limitations within police forces all exacerbate these challenges. A critical analysis reveals that addressing these obstacles requires not only a shift in legal and technological paradigms but also a rethinking of transnational cooperation, training, and resource allocation.

The evolving landscape of cybercrime demands a critical rethinking of how digital evidence is collected and preserved. Unlike traditional physical evidence, digital evidence is defined by its volatility, susceptibility to alteration, and sheer scale. These characteristics challenge law enforcement's ability to gather reliable and admissible data, exacerbating the limitations of established forensic methods. Crucially, the instability of digital evidence, coupled with its volume and ubiquity, often results in investigative delays, contributing to what may be described as a 'data deluge'.[60] This section interrogates the shortcomings of conventional forensic practices while engaging in a nuanced exploration of emerging technologies – such as AI and ML – that could revolutionise investigative capacities.

Traditional forensic techniques are ill-suited to address the rapid advances in cybercrime. These methods, rooted in physical evidence collection, fail to grasp the dynamic nature of digital evidence, which may disappear or be encrypted at the slightest provocation. The inability to address these emerging challenges indicates a systemic flaw in current law enforcement protocols.[61] Further, this analysis delves into how such inadequacies can be mitigated by the integration of cutting-edge technologies, particularly AI and ML, capable of processing vast amounts of data with speed and accuracy unmatched by human investigators. Yet, the efficacy of these technologies' hinges not only on technical competence but also on addressing legal, ethical, and regulatory challenges, which remain substantial hurdles.

5.1 Technological Disparities: A Rapidly Evolving Threat Environment

[60] Marc D. Goodman and Susan W. Brenner, 'The Emerging Consensus on Criminal Conduct in Cyberspace' (2002) 10(2) International Journal of Law and Information Technology 139.
[61] Eoghan Casey, *Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet* (3rd edn, Academic Press 2011).

At the core of the difficulties in cybercrime investigations is the profound technological asymmetry between cybercriminals and law enforcement agencies. As Casey highlights, digital evidence presents unique challenges due to its fragility and transience.[62] Unlike physical evidence, digital data can be altered, hidden, or deleted with little trace, complicating traditional forensic approaches. The rise of sophisticated anonymisation technologies, such as the dark web and virtual private networks (VPNs), exacerbates this issue, allowing criminals to obfuscate their digital footprints with relative ease.[63] The transience of digital evidence not only hinders investigations but also creates a race against time, where critical data can disappear before investigators can preserve it.

Encryption, a double-edged sword in the realm of cybersecurity, further compounds this issue. Brenner underscores how end-to-end encryption has created a "going dark" problem, rendering even legally sanctioned interception of communications ineffective. Law enforcement agencies, confronted with the "going dark" phenomenon, struggle to balance the legitimate need for privacy with national security imperatives.[64] Encryption tools, which render digital communications nearly impenetrable, have become a double-edged sword. They safeguard personal data from malicious actors, yet their pervasive use by cybercriminals creates an impenetrable shield that frustrates legal investigations, even when authorised by court orders.

While encryption protects personal privacy, it also shields illicit activities, making it nearly impossible for law enforcement to access crucial evidence in real time.[65] The fundamental tension between privacy rights and law enforcement needs complicates the legislative framework surrounding digital evidence. The dilemma is magnified by the limited capacity of law enforcement to develop decryption technologies capable of keeping pace with the encryption standards employed by cybercriminals.[66] As a result, law enforcement often finds itself outpaced by the very technologies it seeks to regulate, with minimal tools at its disposal to penetrate these fortified digital walls.

The legislative response to this dilemma is fraught with complexity. Acts such as the UK's Investigatory Powers Act 2016 and the US CLOUD Act 2018 reflect a growing consensus that

---

[62] Ibid.
[63] Robert Moore, *Cybercrime: Investigating High-Technology Computer Crime* (1st edn, Anderson Publishing 2010); Eoghan Casey, *Digital Evidence and Computer Crime* (3rd edn, Academic Press 2011).
[64] Susan Landau, 'Making Sense from Snowden: What's Significant in the NSA Surveillance Revelations' (2013) 11(4) IEEE Security & Privacy 54.
[65] Susan W. Brenner, *Cybercrime: Criminal Threats from Cyberspace* (Praeger 2010).
[66] Ibrahim Baggili and Frank Breitinger, *Digital Forensics and Cyber Crime* (Springer 2019).

service providers must play an active role in assisting law enforcement to decrypt data.[67] Still, the enactment of such laws invites controversy. Critics argue that mandating decryption powers for the state risks undermining civil liberties, particularly in an era where data privacy is increasingly recognised as a fundamental right. In this light, any legislative attempt to regulate encryption must walk a delicate tightrope, balancing state security against the erosion of privacy. Furthermore, this tension is exacerbated by anonymisation technologies, which enable criminal networks to exploit platforms like the dark web. The sophisticated anonymisation methods deployed on these platforms' complicate attribution, frustrating law enforcement efforts to track illicit activities such as drug trafficking and identity theft.[68]

While international operations like Europol's Operation Onymous have demonstrated some success in penetrating dark web networks, the resilience of these networks suggests that current approaches are insufficient. The persistence of the dark web as a locus for criminal activity points to a deeper issue – the limitations of existing forensic and investigative techniques. More innovative approaches, rooted in collaborative international efforts and adaptive technologies, are urgently needed to counteract the technological advantages enjoyed by cybercriminals.

5.2 Forensic Limitations: A Disjuncture in Methodologies

A critical analysis of cybercrime investigations reveals a substantial inadequacy in traditional forensic techniques. Traditional forensic practices, when applied to cybercrime investigations, are often unable to maintain the evidentiary integrity required in court. Central to this problem is the chain of custody – a principle foundational to forensic investigation, yet notoriously difficult to enforce with digital evidence. Unlike physical evidence, which degrades with each replication, digital data can be copied *ad infinitum* without degradation. Therefore, this very attribute makes it susceptible to tampering. Establishing an incontrovertible chain of custody becomes more challenging in cases where digital evidence is transferred across multiple jurisdictions, a situation all too common in the context of transnational cybercrime.[69]

Casey spearheads that the forensic methodologies developed for physical crime scenes are ill-suited to the digital world.[70] Digital evidence is not just fleeting but also highly fragmented and distributed across multiple locations and devices, frequently crossing international borders.

---

[67] Michael D. Green and Ian Kearns, *Encryption and Lawful Access: Resolving the Tensions* (Policy Institute 2021).
[68] Gabriel Weimann, 'Going Dark: Terrorism on the Dark Web' (2016) 62(1) Studies in Conflict & Terrorism 25.
[69] Susan W. Brenner, *Cybercrime: Criminal Threats from Cyberspace* (Praeger 2010).
[70] Eoghan Casey, *Digital Evidence and Computer Crime* (3rd edn, Academic Press 2011).

This contrasts starkly with physical crime scenes, where evidence is typically contained within a single jurisdiction and subject to well established chain-of-custody protocols.[71] The inadequacy of these traditional methods is further exacerbated by the overwhelming volume of data that law enforcement must sift through in cybercrime cases. As Moore notes, the sheer scale of digital evidence – ranging from hard drives to cloud-based storage – makes the collection and preservation of data far more time-consuming than in physical crime investigations.[72]

Moreover, the conventional understanding of jurisdiction and evidence in criminal law struggles to adapt to the digital age. As digital evidence is often stored in multiple jurisdictions, the time-sensitive nature of cybercrime investigations is at odds with the sluggish pace of obtaining mutual legal assistance from foreign authorities.[73] This lag creates significant opportunities for cybercriminals to evade justice by relocating data or by exploiting the legal discrepancies between national jurisdictions. In response to this fragmentation, some scholars suggest that the development of international forensic standards could streamline these processes, but such an initiative requires extensive political and legal cooperation.[74]

Unfortunately, the sheer volume of data encountered in contemporary cybercrime investigations has rendered traditional forensic methodologies obsolete. In complex cases, investigators often face terabytes of data requiring analysis – a quantity that exceeds the capabilities of manual forensic methods.[75] This points to a critical gap: the absence of standardised procedures for the collection and preservation of digital evidence. Inconsistencies in handling this evidence undermine both the credibility of the investigation and its admissibility in court, as demonstrated in high-profile cases where procedural flaws have led to the dismissal of critical evidence.

5.3 Cybercrime-as-a-Service: The Democratisation of Illicit Tools

---

[71] Eoghan Casey, *Digital Evidence and Computer Crime* (3rd edn, Academic Press 2011); Avi Laykin, *Investigative Computer Forensics: The Practical Guide for Lawyers, Accountants, Investigators, and Business Executives* (Wiley 2013).

[72] Robert Moore, *Cybercrime: Investigating High-Technology Computer Crime* (1st edn, Anderson Publishing 2010).

[73] Susan W. Brenner and John Schwerha, 'Cybercrime: A Blueprint for Modernising Our Ability to Investigate and Prosecute' (2002) 19 Journal of Computer Information Systems 1.

[74] Mohamed Chawki et al., *Cybercrime, Digital Forensics and Jurisdiction* (Routledge 2015).

[75] Marie-Francine Moens et al., *Information Retrieval: Uncertainty and Logics: Advanced Models for the Representation and Retrieval of Information* (Springer 2018).

The rise of cybercrime-as-a-Service (CaaS) has fundamentally transformed the nature of cybercrime, lowering the barrier to entry for would-be offenders. Brenner highlights that CaaS allows low-skill actors to access sophisticated tools, dramatically increasing the frequency and complexity of cyberattacks.[76] This shift mirrors broader trends in technology democratisation, where powerful tools are no longer confined to experts but are widely available to the public. The scalability of cybercriminal operations through CaaS platforms creates a substantial challenge for law enforcement, which is already struggling to keep pace with the technical proficiency required to combat cybercrime.[77]

Furthermore, the diffusion of CaaS has created an environment in which attribution – the process of identifying the perpetrators of cybercrime – has become increasingly difficult. The global nature of the internet allows cybercriminals to operate from multiple jurisdictions simultaneously, further complicating efforts to trace their activities back to a single location or individual.[78] In this context, the challenge for law enforcement is twofold: not only must they develop the technological capabilities to identify perpetrators, but they must also navigate the complex legal frameworks governing transnational criminal activity. Without the development of more robust attribution technologies and legal agreements, law enforcement agencies will continue to operate at a significant disadvantage in the fight against cybercrime.

5.4 Emerging Technologies: AI and ML in Cybercrime Investigation

To address the increasing complexities of cybercrime, AI and ML offer innovative, albeit imperfect, solutions. AI's capacity for processing and analysing vast datasets enables law enforcement agencies to identify patterns, prioritise leads, and even anticipate criminal behaviour with unprecedented precision.[79] Similarly, ML algorithms, which refine themselves through exposure to additional data, offer the potential to identify cybercrime trends more effectively than human investigators.

The application of AI in law enforcement is fraught with risks. AI systems are intrinsically limited by the quality of the data they are trained on. As recent studies have shown, biassed or

---

[76] Susan W. Brenner, *Cybercrime: Criminal Threats from Cyberspace* (Praeger 2010).
[77] Sean E. Goodison et al., *Digital Evidence and the US Criminal Justice System* (RAND Corporation 2015).
[78] Peter Grabosky, 'The Globalization of Crime: Notions, Trends, and the Impact on Law Enforcement' (2001) 4 Australian and New Zealand Journal of Criminology 123.
[79] Jeffrey P. Brantingham et al., 'Does Predictive Policing Lead to Biased Arrests? Results from a Randomized Controlled Trial' (2018) 5(1) Statistics and Public Policy 1.

incomplete datasets can lead to erroneous conclusions, resulting in wrongful accusations and unjust prosecutions.[80] Furthermore, the rise of adversarial attacks – whereby malicious actors exploit AI vulnerabilities to manipulate outcomes – presents a significant threat to the integrity of these systems. Moreover, ethical concerns surrounding the deployment of AI in predictive policing, particularly its potential for reinforcing societal biases and exacerbating existing inequalities, demand urgent scrutiny.[81]

5.5 Training and Resource Gaps: A Structural Weakness

The lack of specialised training and resources within law enforcement agencies represents a significant impediment to the effective investigation of cybercrime. As Holt and Bossler make clear, many law enforcement agencies are staffed by officers with limited technical knowledge of cybercrime and digital forensics.[82] These skills gap not only limits the ability of officers to conduct thorough investigations but also hampers their ability to understand and anticipate new developments in cybercrime.

Broadhurst notes that while larger law enforcement agencies may have access to specialised cybercrime units, smaller jurisdictions often lack the resources necessary to conduct even basic digital investigations. This disparity in capabilities is a critical weakness in the global fight against cybercrime, as smaller, under-resourced jurisdictions can become safe havens for cybercriminals.[83] The uneven distribution of resources and expertise leads to a patchwork of enforcement capabilities, where cybercriminals can exploit the weakest links in the global law enforcement network.

6 Addressing the Challenges

This section sets out and critically engages with some of the prominent approaches on facing the challenge posed by cybercrime and explores possible solutions to the issues outlined in the article so far. Budling upon the proposals of others, it shows how ultimately, addressing the jurisdictional and technical challenges of cybercrime requires a coordinated, multi-stakeholder

---

[80] Battista Biggio and Fabio Roli, 'Wild Patterns: Ten Years After the Rise of Adversarial Machine Learning' (2018) 84 Pattern Recognition 317.
[81] Kate Crawford, *Atlas of AI: Power, Politics, and the Planetary Costs of Artificial Intelligence* (Yale University Press 2021).
[82] Thomas J. Holt and Adam M. Bossler, *Cybercrime and Digital Forensics: An Introduction* (Routledge 2015).
[83] Roderic Broadhurst, 'Combating the Cybercrime Threat' in Hossein Bidgoli (ed), *Handbook of Information Security: Information Warfare, Social, Legal, and International Issues and Security Foundations Volume 2* (Wiley 2006).

effort. Harmonisation of legal frameworks, technological advancements, and public-private partnerships are essential to overcoming these obstacles and ensuring that law enforcement agencies have the tools they need to effectively combat cybercrime. As the digital landscape continues to evolve, so too must the legal frameworks that govern it. Developing a truly global legal framework that reflects the borderless nature of the internet is essential for the future of cybercrime investigations.

6.1 The Legal Framework

6.1.1 Is Cybercrime Unexceptional?

In their research, Post critiques the assumption that cyberspace represents a chaotic, lawless domain that fundamentally requires new forms of internet governance, challenging the narratives that have long framed this debate through the concepts of "cyber anarchy" and "cyber unexceptionalism."[84] He suggests that the legal challenges posed by the internet are not unique but are exaggerated by the perception of cyberspace as entirely distinct from the physical world. By promoting "cyber unexceptionalism" Post argues that existing legal frameworks, grounded in traditional jurisdictional principles, can regulate the digital sphere, provided they are applied with sensitivity to the internet's decentralised and transnational character.

While Post's critique of cyber-exceptionalism offers a pragmatic approach to internet regulation, it risks oversimplifying the profound jurisdictional complexities inherent in cyberspace. His view assumes that existing legal doctrines can adapt to the internet without significant modification, overlooking the ways in which the digital landscape subverts traditional notions of sovereignty, territoriality, and control. For instance, the fluidity of cyberspace, where data flows instantaneously across borders, challenges the foundational legal assumption that jurisdiction is inherently tied to physical territory. Post's call for legal continuity may undervalue the need for new transnational legal architectures that are more agile and capable of responding to the novel challenges of a borderless digital environment. In this sense, while Post provides a necessary counter to the overstatement of cyber-exceptionalism, his reluctance to advocate for more radical legal reforms may fall short in addressing the full scope of internet governance challenges.

[84] David G. Post, 'Against 'Against Cyberanarchy'' (1998) 17 Berkeley Technology Law Journal 1365.

In contrast, the view highlighted by Rustad is that the internet has outpaced traditional legal mechanisms such as MLATs with the legal frameworks aiming to govern cyberspace being inadequate to do so effectively given the jurisdictional chaos that arises from the internet's inherently transnational nature.[85] Hence, his focus is advocating for greater harmonisation of international law to resolve the challenges posed by cybercrime, through international state cooperation.

Similarly, Perritt's research into jurisdictional conflicts in cyberspace offers a sophisticated analysis of the competing forces that shape internet governance.[86] Perritt highlights the tension between states' desire to assert territorial jurisdiction over online activity, the extraterritorial reach of certain national laws,[87] and the self-regulatory regimes adopted by tech companies that often operate beyond the effective reach of any single government body. This relationship underscores the complexity of internet regulation, where no single actor – state, corporation, or international body – can effectively control the digital sphere without the intersection of another.

Rustad's proposals often rest on the assumption international law harmonisation is achievable in the short term, without fully grappling with the political and sovereignty-based obstacles that have long hindered international cooperation on this issue. Hence, his critique could benefit from a deeper exploration of the power dynamics that shape transnational internet governance. His emphasis on legal harmonisation does not fully account for the fact that states are often reluctant to cede sovereignty in cyberspace, particularly when it comes to issues of national security, data sovereignty, and economic control. Countries with authoritarian regimes may resist harmonisation that imposes limits on state control over the internet, while liberal democracies might resist frameworks that compromise privacy or freedom of expression. Thus, the call for harmonisation, though ideal in theory, may be unrealistic in practice without a deeper consideration of these entrenched geopolitical tensions.

On the other hand, while Perritt's perspective provides a better account of the shaping power dynamics and aptly captures the jurisdictional tensions, it could be critiqued for placing too little attention on the proposal of greater regulation as a viable governance mechanism to combat cyber challenges. The growing concentration of power among a small number of tech

---

[85] Michael L. Rustad., 'Transnational Internet Governance: Jurisdictional Quandaries' (2009) 44 University of San Francisco Law Review 635.
[86] Henry H. Perritt Jr., 'Jurisdiction in Cyberspace' (1996) 41 Villanova Law Review 1.
[87] Ibid.

giants, often referred to by many researchers as “digital sovereigns”, notably Baldoni and Luna,[88] complicates the notion that self-regulation offers a meaningful check on state overreach. These companies wield enormous power over the global flow of information, often prioritising profit and market dominance over the public safety, undermining the potential of self-regulation as a sustainable or ethical model for governing an increasingly corporatised internet. The extraterritorial application of national laws, especially by powerful global states such as the US, raises questions about digital colonialism, where certain jurisdictions impose their legal norms on the rest of the world without constraint, undermining local sovereignty and legal diversity.

Briefly, both reform proposals expose critical flaws in current internet governance models but should be engaging more deeply with the political, economic, and ethical complexities that complicate efforts to create a unified legal framework for cyberspace. While providing valuable insights, they highlight the need for more comprehensive, critical strategies that consider not only legal principles but also the global power dynamics that shape cyberspace regulation.

Certainly, the fragmented legal frameworks and divergent national laws create a system where cybercriminals can exploit jurisdictional loopholes, rendering prosecution exceedingly difficult. This situation is aggravated by the inadequacies of traditional forensic methodologies, which are often overwhelmed by the volume and complexity of digital evidence. Given these challenges, the current state of cybercrime investigation necessitates a fundamental reassessment of both legal and investigative practices. First, there is an urgent need to establish a long-term plan for international legal harmonisation. Even though it will take time, efforts must be made to update and align legal frameworks to better facilitate cross-border cooperation in cybercrime cases. In particular, the legal admissibility of digital evidence must be revisited, with reforms aimed at ensuring that evidence collected across borders can be reliably used in prosecutions.

6.3 Technical Obstacles

Fewer reform proposals have been made in relation to the technical obstacles faced by law enforcement agencies. Addressing the technical obstacles of cybercrime including the use of encryption, the pervasive use of anonymisation techniques and platforms like the dark web, requires a prioritisation of the adoption of cutting-edge forensic tools and the provision of

[88] Roberto Baldoni and Giuseppe Di Luna, ‘Sovereignty in the digital era: The quest for continuous access to dependable technological capabilities’ (2025) 23(1) IEEE Security Privacy 91.

ongoing training for law enforcing personnel. This includes not only technical training in digital forensics but also comprehensive education on the legal aspects of cybercrime investigation. Even though it might be impossible to eliminate the tension between privacy and security consideration, ensuring that law enforcement officers are equipped with the latest tools and knowledge is essential for maintaining the integrity of cybercrime investigations.[89] The balancing act between security and civil liberties will remain a central issue as cybercrime continues to evolve, and the future of law enforcement will depend on its ability to navigate this delicate terrain.

In addition, ways must be found to address the transient nature of digital evidence, which presents formidable challenges, complicating traditional forensic methods. A potential approach, which would particularly help law enforcement agencies with limited resources, would be to establish international taskforces dedicated to the enhanced coordination of more efficient response for cybercrimes. There must be more advocates for the formation of dedicated cybercrime taskforces to facilitate rapid information sharing and coordinated action across jurisdictions.[90] Significant investment in advanced digital forensic technologies is essential to ensure law enforcement agencies have the necessary tools to keep pace with the technological advancements employed by cybercriminals. Teams with cutting-edge forensic tools and more streamlined processes for digital evidence preservation can help reduce deficiencies in this area.

6.4 Facilitating improvement

6.4.1 A Multi-Stakeholder Approach to Overcome Cybercrime Challenges

A truly effective response to cybercrime cannot rely solely on law enforcement efforts. Instead, a multi-stakeholder approach is essential, incorporating government entities, law enforcement, private sector partners, and international organisations. Public–private partnerships are crucial, as private sector companies, particularly in the technology industry, are often better positioned to develop and provide the advanced forensic tools and threat intelligence needed to combat cybercrime. The involvement of private companies in facilitating lawful access to encrypted

[89] Mohamed Chawki, Abdel-Aziz Darwish, and Mohammad Bin Hassan Khan, *Cybercrime, Digital Forensics and Jurisdiction* (Routledge 2015)
[90] Scott Shackelford, *Managing Cyber Attacks in International Law, Business, and Relations: In Search of Cyber Peace* (CUP 2014).

data, within clear legal frameworks that safeguard privacy, will be a critical component of a successful cybercrime strategy.[91]

The *Microsoft Corp.*[92] and *Ivanov*[93] cases underscore the critical importance of international collaboration in addressing jurisdictional challenges. They also reveal the limitations of current legal frameworks, which often fall short in managing the complexities of cross-border investigations.[94] To address these challenges effectively, the global community must enhance international cooperation and develop more cohesive legal frameworks capable of navigating the intricacies of cyberspace jurisdiction.[95]

To address the jurisdictional challenges posed by cybercrime, it is essential to promote greater international cooperation. This could involve the development of new bilateral or multilateral treaties or agreements that facilitate cross-border investigations and the sharing of digital evidence. International organisations, such as Interpol and Europol, play an equally vital role by providing platforms for cross-border cooperation and intelligence sharing. Emphasis must be attached to the importance of diplomatic engagement in fostering international cooperation and addressing the jurisdictional challenges of cybercrime. The role of cross-border agencies such as Interpol and Europol in streamlining MLA procedures and fostering a more integrated approach to cybercrime investigation cannot be overstated. Governments must also ensure that sufficient resources are allocated towards research and development in the field of digital forensics, particularly in the areas of AI and ML, which offer significant potential for the future of cybercrime investigations.[96]

6.4.2 The Importance of Resource Allocation

To address the ever-growing threat of cybercrime, it is essential to allocate substantial resources towards research, education, and the development of innovative technologies. Cutting-edge forensic tools, such as AI and ML, have the potential to revolutionise cybercrime investigations by processing vast datasets, identifying patterns, and predicting criminal behaviour with unprecedented accuracy.[97] Obviously, these technologies must be accompanied by adequate

---

[91] Rainer Böhme, *Economics of Information Security and Privacy* (Springer 2013).
[92] *Microsoft Corp. v United States* 829 F.3d 197 (2d Cir. 2016).
[93] *United States v Ivanov* 175 F Supp 2d 367 (D Conn 2001).
[94] Susan W. Brenner, 'Cybercrime jurisdiction' (2006) 46(4) Crime Law Social Change 189.
[95] Anthony D. Trotter, 'Jurisdiction in Cyberspace: Rights and Regulation' (2010) 108(8) Michigan Law Review 1.
[96] Timo Rademacher, 'Artificial Intelligence and Law Enforcement' in Thomas Wischmeyer and Timo Rademacher (eds), *Regulating Artificial Intelligence* (Springer 2020).
[97] Ibid.

legal frameworks and oversight to prevent potential abuses and ensure that civil liberties are not infringed.

Specialised training for law enforcement officers is equally important, as it provides them with the technical expertise necessary to handle the complexities of digital evidence. Collaboration with the private sector and academia will also be critical in advancing cybercrime research, as public–private partnerships provide access to state-of-the-art technology and expertise that many law enforcement agencies lack. This approach will ensure that law enforcement agencies remain capable of addressing the increasingly sophisticated methods used by cybercriminals.

6.4.3 Public–Private Partnerships: The Future of Cybercrime Investigations

Considering Ginsburg's triangle, public–private partnerships are essential for addressing the challenges posed by cybercrime. Private sector companies, particularly those in the technology and cybersecurity industries, possess critical resources, intelligence, and expertise that can significantly enhance law enforcement capabilities. Collaboration between law enforcement and the private sector is critical for tackling cybercrime. Such collaborations must be framed within clear legal boundaries to safeguard against the potential misuse of data and to protect individual privacy.[98] Finally, sustained investment in research and development is crucial. International initiatives, such as the Global Forum on Cyber Expertise (GFCE) and Europol's Innovation Lab, exemplify the power of cross-border cooperation in advancing cybercrime investigation techniques.[99]

Private companies often have access to valuable threat intelligence and resources that can aid in investigations. Establishing formal partnerships and information-sharing mechanisms can help bridge the gap between the public and private sectors, fostering a more coordinated and effective response to cybercrime. By establishing formal mechanisms for information sharing, both sectors can work together to combat cybercrime more effectively. However, such partnerships must be carefully regulated to ensure that they respect privacy rights and do not overreach into areas that could harm civil liberties.[100]

Essentially, it is through a multifaceted approach that the jurisdictional and technical challenges of cybercrime investigations can begin to be addressed.

---

[98] Rainer Böhme, *Economics of Information Security and Privacy* (Springer 2013).
[99] Michel J. G. van Eeten and Johann M. Bauer, 'International Cooperation to Address Challenges in Cybersecurity: Institutional Efforts and Regional Coordination' (2009) 35(2) The Information Society 60.
[100] Stephen Mason, *Electronic Evidence* (4th edn, LexisNexis 2020).

7 Conclusion

This paper has explored the complex interplay of jurisdictional and technical challenges, two mutually reinforcing areas, that law enforcement agencies face in investigating cybercrimes. At its core, the investigation of cybercrime is inhibited by two primary obstacles: the borderless nature of cyberspace and the rapid pace of technological advancement.

Jurisdictionally, one of the most significant challenges lies in the fact that cyberspace operates beyond the physical borders of nation-states. This creates substantial difficulties in determining which country's laws apply when cyber-crimes are committed across multiple jurisdictions. The lack of harmonisation between national and international legal frameworks further compounds this issue, as countries often apply different standards regarding what constitutes a cybercrime, what evidence is admissible, and how cooperation between agencies should occur.[101] This has been evidenced by inconsistencies in MLATs, delays in obtaining cross-border data, and jurisdictional overlap that leads to conflict or even impunity for offenders.

From a technical perspective, the investigative process is complicated by a range of challenges, including the encryption of communications, anonymisation tools such as VPNs and the Tor network, and the dynamic nature of malicious software. Additionally, the sheer volume of data and the use of cloud computing systems make it difficult for law enforcement to secure and analyse evidence effectively and diminish the current threats we face. Coupled with the skills gap in digital forensic capabilities among law enforcement personnel, these issues create multiple, substantial barriers to both detecting and prosecuting cybercriminals.

The findings contribute to the growing body of knowledge on cybercrime investigation by clarifying the need for a more coordinated, globally inclusive legal framework. The current fragmented approach to jurisdictional issues necessitates reforms that promote international cooperation. One such reform could be the development of a comprehensive, binding international convention on cybercrime, which would provide clear jurisdictional guidelines for law enforcement agencies and streamline mutual legal assistance processes, to mitigate the inconsistencies that currently hinder countless investigations and prosecutions across jurisdictional borders.

[101] Stein Schjolberg, 'The History of Global Harmonization on Cybercrime Legislation – The Road to the Budapest Convention and Beyond' (2008) Computer Law Review International.

Alongside this, the technical challenges identified in this paper underscore the need for law enforcement agencies to adapt to the rapidly evolving technological landscape. This requires both investment in digital forensic tools and the upskilling of law enforcement personnel to match the sophistication of cybercriminals. A key policy recommendation is for agencies to invest in continuous, specialised training programs that focus on emerging technologies and forensic techniques. In tandem, partnerships between public law enforcement and private sector technology companies should be strengthened to foster real-time data sharing and access to cutting-edge technologies.

For future policymakers, this paper's findings strongly suggest a dual approach is required for a more positive future in cybercrime investigation: one that focuses on legislative harmonisation at the international level and another that ensures technological preparedness at the operational level. By enhancing cross-border legal frameworks and equipping law enforcement with the tools and skills necessary to navigate the complexities of cyberspace, the gap between cybercriminal activity and law enforcement capabilities can be narrowed.

Moving forward, both law enforcement agencies and policymakers must recognise that cybercrime is a constantly evolving challenge requiring an adaptive, multifaceted response. International cooperation, investment in technological capabilities, and a commitment to safeguarding human rights and privacy in the digital space are crucial for creating a more resilient cybercrime investigation framework.

Finally, while there are substantial jurisdictional and technical challenges impeding cybercrime investigations, this paper has shown that these challenges are not insurmountable. With the right policy interventions, investment in training and technology, and a focus on international collaboration, the efficacy of law enforcement in tackling cybercrime can be significantly enhanced. These changes will be essential not only to keep pace with the current landscape of cybercrime but to anticipate and mitigate future threats in an increasingly digital world.