



CYBERCRIME: ANALYSE THE LAWS AND PRACTICES SURROUNDING CYBERCRIME IN DIFFERENT COUNTRIES

Tapasya Sharma* Bhawna Sharma*

ABSTRACT

Cybercrime poses a significant 21st-century threat due to its transnational nature, which often outpaces traditional legal frameworks. The borderless digital realm presents challenges for national laws that are typically limited by territorial boundaries, leading to considerable disparities in legal responses across different countries. These variations stem from diverse legal traditions, technological development levels, and resource availability, ultimately hindering effective international cooperation, a weakness exploited by cybercriminals. Despite extensive existing literature, there is a notable research gap in comprehensive comparative studies that integrate formal cybercrime laws with their practical implementation challenges across a wide range of diverse countries. Current research often focuses on single-country studies, specific international conventions without detailed implementation analysis, technical aspects divorced from legal realities, or comparative studies confined to jurisdictions with similar characteristics. This research aims to bridge this gap by providing a critical comparative analysis of cybercrime legal frameworks and practical approaches in a selection of countries chosen to represent different legal systems, developmental stages, and engagement levels with international standards. The core objectives include systematically comparing substantive criminal law provisions, analysing procedural frameworks and practical investigative/prosecutorial capabilities, critically evaluating legal and practical challenges arising from existing disparities (especially concerning cross-border issues like jurisdiction, Mutual Legal Assistance Treaties (MLATs), and data access), and formulating evidence-based recommendations for legislative reforms and enhanced international cooperation. Utilising a doctrinal and Comparative Legal Research Methodology, complemented by an analysis of secondary sources on practical implementation, this study examines national legislation, case

*SRM UNIVERSITY
*SRM UNIVERSITY

law, and international instruments in selected jurisdictions (e.g., US, Germany, India, Brazil, based on specific criteria. The central hypothesis posits that significant divergences in national cybercrime laws and enforcement capacities substantially impede effective international cooperation, thereby facilitating transnational cybercrime and diminishing accountability. By analysing both "laws on the books" and "laws in action" across diverse nations, this research endeavours to offer a more holistic understanding of the global fight against cybercrime and to inform strategies for strengthening national capacity and fostering international collaboration.

Keywords: Cybercrime, International Cooperation, Comparative Law, Legal Frameworks, Practical Implementation.

INTRODUCTION TO CYBERCRIME AND THE GLOBAL LEGAL LANDSCAPE

Cybercrime, a rapidly evolving threat in our increasingly digitised world, encompasses a broad spectrum of illicit activities utilising computer systems and networks. Its borderless nature and continuous transformation, driven by technological advancements, pose significant challenges for national legal systems and necessitate robust international cooperation. This chapter establishes a foundation for analysing cybercrime laws by defining its scope, exploring typologies, examining the impact of emerging technologies, highlighting its transnational nature, detailing jurisdictional complexities, and reviewing existing national and international legal frameworks.

Defining Cybercrime: Scope, Typologies, and Evolving Nature: Cybercrime refers to any criminal act facilitated by or directed at electronic devices and networks. Its scope is vast, ranging from online fraud to sophisticated state-sponsored attacks.

Categories of Cybercrime

Crimes Against Computer Systems: Offences directly targeting computer systems, networks, and data, such as hacking, denial-of-service (DoS) attacks, malware propagation (viruses, worms, ransomware), and data/system damage.

Computer-Related Fraud: Using computers and networks to facilitate traditional fraud, including online scams (phishing, business email compromise), identity theft, credit card fraud, and illicit goods trading.

Content-Related Offences: Crimes involving the creation, distribution, or access of illegal online content, such as child sexual abuse material, hate speech, and copyright infringement. Other offences include cyberstalking, cyberbullying, online harassment, and cyberterrorism. These categories often blur, with many activities incorporating multiple elements.

THE IMPACT OF TECHNOLOGICAL ADVANCEMENTS ON CYBERCRIME (AI, IOT, DARK WEB)

Technological progress provides new tools for cybercriminals.

Artificial Intelligence (AI): Used to enhance phishing schemes, create evasive malware, automate vulnerability identification, and facilitate deepfakes for fraud. Adversarial AI attacks other AI systems.

Internet of Things (IoT): Proliferation of IoT devices expand the attack surface. Many IoT devices lack robust security, making them vulnerable to compromise and recruitment into botnets for large-scale attacks like DDoS.

Dark Web: Provides anonymity, facilitating illicit activities, serving as a marketplace for stolen data, malware, and weapons, and enabling communication and planning among cybercriminals.

These technologies not only enable new cybercrimes but also amplify the scale and impact of existing ones, complicating the threat landscape.

THE TRANSNATIONAL CHALLENGE OF CYBERCRIME

A defining characteristic of cybercrime is its inherent transnational nature. Digital attacks can originate globally, target victims across borders, and often leave minimal physical traces in the victim's jurisdiction.

Jurisdictional Complexities in a Borderless Digital World: Cyberspace's borderless nature creates significant jurisdictional challenges for law enforcement. Determining which country has legal authority to investigate and prosecute cybercrime is difficult when perpetrators, victims, data, and infrastructure are in different jurisdictions, potentially leading to crimes going unpunished due to conflicting laws or evidence collection difficulties.

THE NEED FOR INTERNATIONAL COOPERATION

International cooperation is essential to effectively combat transnational cybercrime. Sharing information, coordinating investigations, providing mutual legal assistance in evidence gathering, and facilitating extradition are critical for a successful global response. Without seamless collaboration, cybercriminals exploit jurisdictional boundaries to evade detection and prosecution.

Overview of National and International Legal Responses: Countries worldwide are developing national laws and strategies against cybercrime, defining offences, outlining investigative powers, and establishing penalties. However, definitions and classifications of offences vary significantly, leading to inconsistencies. Alongside national efforts, international instruments and initiatives foster cooperation and harmonise legal approaches. The Council of Europe's Convention on Cybercrime (Budapest Convention) is a landmark treaty providing a common framework for criminalising cyber offences, establishing procedural tools, and facilitating international cooperation. Other international and regional bodies also contribute to guidelines, capacity building, and coordinated efforts. Despite advancements, achieving universal adoption and effective implementation of international standards remains a challenge. Combating cybercrime effectively in the 21st century requires collective and coordinated efforts that bridge geographical and legal divides.

Research Gap: A significant gap exists in comprehensive, comparative research that integrates formal legal provisions with their practical implementation and enforcement challenges across diverse countries. Existing research often focuses on:

- Single-country case studies.
- Analysis of international conventions without examining varied implementation.
- Purely technical aspects detached from legal realities.
- Comparative studies limited to countries with similar legal systems, neglecting those with different traditions or resource constraints.

This project aims to address this by:

- Analysing the practical application of laws in investigation, evidence handling, prosecution, and adjudication.
- Including countries with different legal systems and technological development levels

to capture a broader spectrum of challenges and approaches.

- Examining the interplay between national legal/practical differences and obstacles to international cooperation (e.g., mutual legal assistance, extradition).
- By bridging "laws on the books" with "laws in action" across diverse jurisdictions, this research offers a more holistic understanding of the global fight against cybercrime.

LITERATURE REVIEW

The literature review highlights contributions from various authors to understanding and addressing cybercrime globally. Key themes include comparative analyses of legal approaches, international cooperation, jurisdictional issues, data protection, and challenges in developing nations. Noteworthy works examine the Budapest Convention, national cybercrime laws in countries like China, India, the US, and European nations, and the impact of technological advancements on criminal activities. The collective body of work emphasises the necessity of constant international communication, legislative harmonisation, and robust enforcement cooperation to effectively combat the evolving cybercrime landscape.

RESEARCH OBJECTIVES

The detailed objectives of this research project are:

Systematically compare substantive criminal law provisions related to key cybercrime offences across selected countries, examining elements, penalties, and alignment with international standards like the Budapest Convention.

Analyse and contrast procedural legal frameworks and practical capabilities for cybercrime investigation and prosecution in selected countries, including digital search/seizure, data retention, evidence admissibility, investigative techniques, specialised units, and inter-agency collaboration.

Critically evaluate legal, procedural, and practical challenges stemming from disparities in national laws and enforcement, particularly for cross-border issues like jurisdiction, MLAT execution, extradition, cross-border data access, and real-time information sharing.

Formulate evidence-based recommendations for national legislative reforms and propose strategies to enhance law enforcement effectiveness, improve judicial capacity, and strengthen international cooperation in combating cybercrime globally.

RESEARCH QUESTIONS

Based on these objectives, the research seeks to answer:

1. How do definitions, classifications, and elements of major cybercrime offences compare across selected countries, and how do they align with international standards?
2. What specific procedural powers are available for cybercrime investigation in selected countries, how are they utilised, and what practical challenges arise during digital evidence handling in their judicial systems?
3. What are the most significant legal and practical obstacles for authorities in selected countries when asserting jurisdiction, obtaining cross-border data, executing MLATs, and securing extradition for transnational cybercrime?
4. Based on the comparative analysis, what specific legal amendments, operational improvements, and collaborative strategies can enhance national capacity and international cooperation in combating cybercrime?

HYPOTHESIS

Significant divergences in the substantive criminalisation and procedural powers related to cybercrime across national jurisdictions, coupled with varied levels of technical capacity and legal expertise among law enforcement and judicial bodies, create a complex and often fragmented global legal landscape that substantially hinders effective international cooperation mechanisms (such as MLATs and extradition), thereby facilitating the perpetration of transnational cybercrime and diminishing accountability.

RESEARCH METHODOLOGY

This project employs a Doctrinal and Comparative Legal Research Methodology, supplemented by analysis of relevant reports and literature concerning practical implementation.

Doctrinal Research: Involves in-depth study and interpretation of primary legal sources from selected countries and relevant international law, including national legislation, case law, international treaties (e.g., Budapest Convention), policy documents, and academic literature.

Comparative Legal Research: Compares findings from the doctrinal analysis across selected countries based on thematic areas (e.g., definitions of "unauthorised access," procedural powers

for "real-time collection of traffic data," rules on "jurisdiction"). This identifies similarities, differences, trends, and unique approaches, and analyses the reasons behind these divergences to understand their impact on international cooperation.

Analysis of Practical Aspects (via secondary sources): Investigates practical realities through reports from national cybercrime units, police forces, ministries of justice, and publications from international bodies (Interpol, Europol, UNODC, Council of Europe), as well as academic studies, investigative journalism, and NGO reports.

Selection of Countries: A purposive selection of 4-5 countries will be made, justified by criteria such as representation of different major legal traditions (Common Law, Civil Law), varying levels of technological development, engagement with international cooperation mechanisms (e.g., Budapest Convention), distinct strategic approaches to cybercrime, and accessibility of reliable legal texts and secondary information.

Data Analysis: Collected data (legal texts, reports, literature) will be analysed using content analysis (for legal provisions) and thematic analysis (for patterns in challenges, practices, and policy approaches) to answer research questions and test the hypothesis.

HISTORICAL EVOLUTION OF CYBERCRIME LAWS AND INTERNATIONAL COOPERATION

The evolution of cybercrime law parallels the progression of technology. Early computer misuse in the late 20th century exposed the inadequacy of traditional laws. Pioneering national legislation, such as the US Computer Fraud and Abuse Act (CFAA) 1986 and the UK Computer Misuse Act 1990, emerged to specifically criminalise acts like unauthorised access and data alteration.

The internet's explosion in the 1990s escalated cyber threats, leading to new typologies like internet fraud, sophisticated malware (e.g., Melissa, ILOVEYOU), and denial-of-service attacks. This globalised threat revealed critical gaps in national laws, especially concerning jurisdiction and cross-border digital evidence collection, spurring international cooperation efforts. Early initiatives by organisations like the OECD, Council of Europe, and United Nations addressed the transnational nature of cyber risks. This culminated in the Council of Europe's Budapest Convention on Cybercrime (2001), a landmark treaty harmonising substantive cybercrime offences, standardising procedural investigative powers, and

establishing a framework for international mutual legal assistance and extradition. Regional conventions, such as the African Union's Malabo Convention and the Arab Convention, further contributed to building legal capacity and cooperation. This historical evolution reflects the continuous adaptation of legal frameworks and the enhancement of international collaboration to combat an ever-evolving digital threat landscape.

EARLY CONCEPTIONS OF COMPUTER MISUSE AND INITIAL LEGISLATIVE RESPONSES

The advent of computing technology in the mid to late 20th century created new avenues for illicit activities. Early forms of computer misuse were often seen as technical pranks or isolated incidents, primarily involving unauthorised access and data manipulation by individuals with specialised technical knowledge. These acts were often driven by curiosity or intellectual challenge rather than financial gain.

As computers became integrated into critical infrastructure, the potential for harm became evident, with incidents of data alteration, system disruption, and theft of resources surfacing. The intangible nature of digital targets and methods posed challenges for traditional law enforcement. Prosecutors struggled to apply existing laws, leading to legal loopholes and difficulties in prosecuting perpetrators due to a lack of clear legal definitions for terms like "access," "data," and "damage" in the digital context. This period marked the slow recognition of a new class of criminal activity, necessitating a re-evaluation of existing legal frameworks, and the term "computer crime" began to gain traction. In response to increasing incidents and legal inadequacies, pioneering countries enacted specific legislation for computer misuse.

United States: The Computer Fraud and Abuse Act (CFAA), initially passed in 1984 and amended in 1986, criminalised unauthorised access to "federal interest computers," primarily targeting intrusion and information theft. *United States v. Morris* (1991) was a pivotal case under CFAA, demonstrating its application to malicious code (Morris Worm).

United Kingdom: The 1988 "Prestel" case highlighted the legal vacuum when traditional forgery laws failed to cover data manipulation. This led to the Computer Misuse Act (CMA) 1990, which created core offences for unauthorised access, access with intent to commit further offences, and unauthorised modification of computer material. The CMA has since been amended to include offences related to computer function impairment (DoS attacks) and the creation/supply of misuse tools.

Europe: Several European countries introduced computer-specific criminal provisions in the 1980s. Germany amended its penal code in 1986 to include data espionage and computer sabotage. Sweden criminalised unauthorised data access in 1987. France enacted a law in 1988 related to fraudulent access and hindering system function. These early laws, though varied, showed a shared recognition that computer-related offences needed distinct legal definitions and penalties.

THE RISE OF THE INTERNET AND THE GLOBALIZATION OF CYBER THREATS

The internet's proliferation in the 1990s and early 2000s globalised cybercrime, expanding its scale, variety, and reach. Cybercrime transformed into a sophisticated, financially motivated global enterprise.

Expansion of Cybercrime Typologies in the 1990s and 2000s: The internet facilitated a significant diversification and escalation of cybercrime.

Internet Fraud and Scams: Phishing, online auction fraud, non-delivery of goods, and advance-fee scams proliferated, targeting a global pool of victims.

Malware and Malicious Code: The internet became the primary vector for the rapid spread of viruses (Melissa virus, ILOVEYOU worm), causing widespread disruption and economic damage. Trojan horses and ransomware became sophisticated tools.

Denial-of-Service (DoS) and Distributed Denial-of-Service (DDoS) Attacks: Overwhelming websites to make them unavailable became common, used for protest or extortion.

Cyberstalking and Harassment: Internet and early social media facilitated new forms of relentless online harassment.

Child Sexual Exploitation Online: The internet became a major platform for child sexual abuse material, leading to dedicated international efforts.

Copyright Infringement and Piracy: Ease of digital file sharing led to massive unauthorised distribution of copyrighted material, impacting industries.

This era saw cybercrime move from a niche activity to a mainstream problem, with criminals leveraging the internet's reach to target individuals, businesses, and governments on an unprecedented scale.

GROWING RECOGNITION OF THE NEED FOR SPECIALIZED LAWS

The rapid expansion and globalisation of cybercrime quickly outpaced early national computer crime laws, highlighting the urgent need for more comprehensive and harmonised legal frameworks. Key challenges driving this recognition included:

Jurisdictional Hurdles: The borderless nature made establishing jurisdiction exceedingly difficult, leading to criminals exploiting gaps.

Challenges in Digital Evidence Collection and Preservation: Digital evidence is volatile, making it difficult for law enforcement to quickly identify, preserve, and collect data across jurisdictions with differing legal standards.

Lack of Harmonisation in Criminalisation: Varying definitions or lack of specific laws for cybercrimes created "safe havens" for criminals.

Need for Enhanced Investigative Powers: Traditional techniques were insufficient, requiring new legal powers for accessing subscriber information, traffic data, and content data, and for real-time interception, while respecting civil liberties.

This growing awareness led to widespread calls for robust national laws and enhanced international cooperation.

DEVELOPMENT OF INTERNATIONAL AND REGIONAL INITIATIVES

Recognising cybercrime as inherently transnational, international and regional, organisations-initiated efforts to foster cooperation, share best practices, and harmonise legal approaches.

Early Efforts by OECD, Council of Europe, United Nations:

OECD: Focused on information security and privacy, raising awareness of risks and the need for international cooperation.

Council of Europe: Initiated work on a dedicated cybercrime treaty in the late 1990s, recognising the need for a common legal response among member states.

United Nations: Through UNODC, it examined cybercrime within the context of transnational organised crime, providing a platform for discussion and encouraging legal measures.

These early initiatives highlighted the international dimension of cybercrime and built momentum for concrete cooperative efforts.

The Genesis and Aims of the Budapest Convention on Cybercrime: The Council of Europe's Convention on Cybercrime, adopted in Budapest on November 23, 2001, was the most significant outcome of early international efforts. It aimed to:

Harmonisation of National Substantive Criminal Law: Defines cyber-related offences (e.g., illegal access, data interference, computer-related fraud, child sexual abuse material) that State Parties must criminalise, reducing safe havens for criminals.

Harmonisation of National Procedural Law: Provides procedural powers for law enforcement to investigate cybercrime and collect electronic evidence, including expedited preservation of data, real-time traffic data collection, and content interception, overcoming technical and legal challenges.

Establishing a Regime for International Cooperation: Offers a comprehensive framework for international cooperation, including provisions for mutual legal assistance (MLA).

REFERENCES

1. Clough, J. Principles of Cyber Crime.
2. Radziewicz, F. (2025). Cybercrime and the Law: An Analysis of Legal Governance in Europe. Routledge.
3. Comparative Analysis of Cybercrime in the Criminal Law System - Andrei NASTAS & Sergiu CERNOMOREȚ (Author)
4. Cyber Crimes, Cyber Laws & Intellectual Property Rights - Dr. Hanumanthappa M Shivaswamy D S and Hemanth Kumar K GDr. Hanumanthappa M Shivaswamy D S and Hemant...(Author)
5. Global Cybercrime and Cybersecurity Laws and Regulations: Issues and Challenges in the 21st Century - Shahid M. Shahidullah, PhD (Author), Carla D. Coates, PhD (Author), Dorothy Kersha-Aerga, PhD (Author)
6. Laws to Tackle Cyber Crime & Cyber Terrorism - A Comparative Study - Shobhna

Jeet & Shailendra Kumar (Author)

7. Tiwari, G. (2014). *Understanding Laws– Cyber Laws and Cyber Crimes*. LexisNexis.
8. Various Authors. (2022). *Cyber Crime, Regulations and Security – Contemporary Issues and Challenges*. The Law Brigade Publishers.
9. Ahmad, N. (2023). BOOK REVIEW HUMAN CAPITAL AND DEVELOPMENT. *AR-RĀ'IQ*, 6(1), 147–156.
10. Baxi, P. R., & Khan, S. A. (2023). CYBERCRIME AND INTERNATIONAL JURISDICTION: A COMPARATIVE STUDY OF LEGAL RESPONSES IN INDIA. *IJFANS International Journal of Food and Nutritional Sciences*, 12(01), 7134.
11. Council of Europe. (2001). *Convention on Cybercrime (Budapest Convention)*.
12. Council of Europe. (2003). *Additional Protocol to the Convention on Cybercrime Concerning the Criminalisation of Acts of a Racist or Xenophobic Nature Committed Through Computer Systems*.
13. Council of Europe. (2022). *Second Additional Protocol to the Convention on Cybercrime on Enhanced Cooperation and Disclosure of Electronic Evidence*.