Multidisciplinary Reviews

REVIEW ARTICLE
Published Online: September 19, 2024
https://doi.org/10.31893/multirev.2025024

The need for cybercrime regulation on a global scale by the international law and cyber convention

Enver Buçaj[a] ✉ | **Kenan Idrizaj**[b]

[a]Faculty of Law, University of Prizren University Hoti, Prizren, Kosovo.
[b]Law, University of Sarajevo in Bosnia and Herzegovina.

Abstract This study highlights the necessity of controlling the issue of Cybercrime with International Law Principles and treaties, the legal foundation of international cybercrime legislation. The paper pursued normative behavior relying on the legislation of the European Union and countries outside of Europe. The implications of Cybercrime in cyberattack events establish a legal foundation for preventing and punishing cyber criminals wherever they occur. The perceived threats arising from cyberattack activities are grounded in known cyberattack behaviors and literature, underscoring the imminent nature of these threats. The Convention on Cybercrime, inaugurated in Budapest, Hungary, in November 2001, is recognized as a pivotal international agreement addressing Cybercrime and electronic evidence. The negotiation process included the Council of Europe, United States, Japan, Canada, and South African participants. Significantly, nations across Africa, the Americas, and the Asia/Pacific are harnessing this agreement to implement robust strategies against cybercrime. Cybercrime is a new area of international law, namely, International Criminal Law. The international community handles it because no convention has identified Cybercrime globally. It is urgent to govern Cybercrime globally, and statistics imply that the need to regulate Cybercrime under international criminal law is critical. The paper adopts a method designed to deeply understand the global legal structures related to cybercrime. The study employs a comprehensive approach, merging normative legal research to meticulously examine and interpret key legal documents such as the Budapest Convention, with a comparative legal analysis both within the European Union and globally. This analysis scrutinizes various jurisdictions, identifying best practices and discrepancies to inform a holistic understanding of cybercrime regulation. Policy analysis is conducted to critically assess existing strategies and propose innovative solutions, while technological insights are integrated to ensure legal frameworks are attuned to the rapidly evolving landscape of cyber threats. Involving a broad spectrum of stakeholders, including legal scholars and cybersecurity experts, the research offers a diverse perspective. This multifaceted approach aims to balance thorough legal scrutiny with actionable solutions, promoting robust and flexible strategies for international cybercrime regulation. The results of this comprehensive study underscore the urgent need for a global, unified legal response to combat cybercrime effectively. It concludes that the Budapest Convention marks a significant turning point, offering a foundation for international cooperation and legal harmonization in tackling cybercrimes. However, the rapid technological advancements and the evolving sophistication of cyber threats demand that this convention and other international legal instruments adapt and expand accordingly. The study highlights the importance of harmonizing legal definitions and practices across different jurisdictions, both in common law and civil law countries, cybercrime address the borderless nature of cybercrime. The necessity for enhanced collaboration between public and private sectors in cybercrime investigations is emphasized, alongside the importance of establishing ethical data collection and sharing standards.

Keywords: cybercrime, cyberattack, international criminal law, convention on cybercrime and cooperation

1. Introduction

Cyberattacks have become an inextricable part of modern life, posing constant threats to citizens' security and well-being for the stability of state economic development, political systems, the spread of democracy, public safety, and the normal functioning of states. Today, cybercriminals are savvier, more organized, professionally trained, and more advanced in equipment than their forerunners in history. Technological advancements have provided them with new attack targets and updated their technical capabilities (Huang et al., 2018). In the coming years, cybercriminals may have the ability to incite widespread political and social turmoil by harnessing advanced technologies, including the potential for orchestrating events involving chemical, biological, or nuclear incidents. Cybercrime is the intelligent planning of hackers (Levy,1984). They are the most well-managed and evenly equipped members during crime6. In the world of cybercrime, they are considered heroes (Hollinger,1991). There is a long history of internet-based crime worldwide (Choi et al.,2020).

Today's society is composed of and dependent on various social and communication networks. The online system has recently been introduced to streamline national strategic planning, such as food production and distribution; oil and gas pipelines; land, sea, and air traffic; and all essential functions of a state that rely solely on computer and information technology. Cyber attackers have validated the idea that these attacks will last one day.

The definition of cybercrime varies depending on the field of study or the context in which it is applied. In a more focused sense, it can be defined as any action compromising the integrity and accessibility of an individual's or organization's computer records or systems. (Tapia, 2022). We propose an encompassing definition from the Council of Europe's Budapest Convention and the U.S. Department of Justice (DuPont & Whelan, 2021). Cybercrime constitutes any unlawful activity involving a computer, computer network, or networked device. It is conducted deliberately by individuals or groups intending to inflict damage or unauthorized access, modify, expropriate, or annihilate information or data.

The European Commission has acknowledged the lack of a precise definition of cybercrime. Nevertheless, it has been determined that electronic communication networks and information systems are involved in such activities (Koops, 2010). The European Commission defines cybercrime as criminal acts committed using electronic communication networks and information systems or against such networks and systems (Dumchykov et al., 2022). However, the EU faces internal obstacles, such as fragmentation of the legal framework and differences among member states in terms of their efficiency and commitment to fighting against cybercrime (Brandão & Camisão, 2021). This lack of a standard definition of cybercrime impacts its prevention and ignores the significant economic value associated with the commission of this crime worldwide (Mphatheni & Maluleke, 2022). International instruments such as the United Nations Convention against Corruption are planning to make these activities harmonize the countries. Cyberattacks have become a part of modern life and a threat to individuals or lands in their national interest. International instruments such as the United Nations Conventions against Corruption adopted it (The United States Department of Justice, Equality and Law Reform Annual Report 200 I).

Regardless of collaborative efforts by all parties to fight cybercrime, whether national or international, cyberattacks remain destructive and effective in blocking networks on a large scale. Different countries in all regions are fighting this threat. As a result, establishing cybercrime regulations on the basis of international criminal law principles is critical. In recent years, the most devastating cyberattacks have shown that almost no one is investigated or prosecuted for their actions. The International Criminal Court must investigate, prosecute, and convict those responsible for such crimes (Back, Lee, & Soor, 2018).

This paper aims to contribute to the discourse on global cybercrime regulation by providing a comprehensive analysis, identifying key challenges, and proposing actionable strategies for international cooperation and legal harmonization. The primary goal of this research is to investigate the current state of international cybercrime legislation by evaluating legal frameworks such as the Budapest Convention for their effectiveness in addressing the dynamic nature of cybercrime. It seeks to dissect and comprehend the multifaceted challenges inherent in combating cybercrime on a global scale, considering the borderless nature of cybercrime, the diversity of legal systems, and the complexities involved in international collaboration and legal harmonization. Furthermore, this study endeavors to propose strategic recommendations to enhance the regulation of global cybercrime. This consists of proposing actionable insights and strategies designed to update and refine existing legal frameworks, bolster international cooperation, and cultivate strong public–private partnerships that effectively counter cybercrime.

To achieve these goals, the research is structured, including a comprehensive literature review that involves a meticulous examination of academic research, legal commentaries, and reports from international bodies to grasp the prevailing state of cybercrime and its legal management worldwide. A comparative legal analysis is also conducted, shedding light on the diversity in legal practices across different jurisdictions and emphasizing the need for harmonization. Additionally, the paper integrates case studies of significant cybercrime incidents, offers practical insights and underscores the existing gaps and strengths in the current legal responses. Much of the research is dedicated to policy analysis and formulating strategic recommendations to address the identified challenges. This includes advocating for harmonizing legal definitions and standards across various legal systems to foster a unified approach to combatting cybercrime effectively. The paper also emphasizes the pivotal role of public–private partnerships, outlining strategies to increase collaboration between governments, tech companies, and internet service providers. Furthermore, it stresses the importance of ensuring legal safeguards to protect individual privacy and human rights to regulate cybercrime efficiently. In its concluding sections, the paper synthesizes the insights gained from the research, reflecting on the initial goals and the extent to which they have been met. It reiterates the importance of the recommended strategies and advocates for their adoption in international cybercrime regulation. The bibliography provides a detailed reference list, acknowledging the contributions of various scholars and practitioners whose work has significantly shaped the field of cybercrime regulation.

2. Methodology

The study's approach is designed to offer a thorough understanding of the international legal framework governing cybercrime, identifying key areas requiring further development or harmonization. The use of a normative legal research approach effectively dissects and comprehends legal principles, doctrines, and a range of international instruments. This

approach lies in an in-depth examination of the Convention on Cybercrime (Budapest Convention) and other relevant international and national legal texts. Such an examination extends beyond mere legal analysis to explore these legal instruments' effectiveness and broader implications in addressing global cybercrime challenges.

The methodological approach adopted in this research is multifaceted and designed to address the complex challenges of cybercrime regulation comprehensively on a global scale. This approach incorporates normative legal research to dissect and understand the principles, doctrines, and various international instruments pivotal to international cybercrime legislation, focusing on the Convention on Cybercrime (Budapest Convention) and other relevant international and national legal texts. A comparative analysis across European and global jurisdictions is central to this methodology, aiming to identify the diverse approaches and challenges in cybercrime legislation. This method is further enriched by case studies of notable cybercrime incidents, offering practical insights into the effectiveness of existing legal frameworks and highlighting the gaps and strengths in current legal responses. The methodology is grounded in an extensive literature review, including academic research, legal commentaries, and reports from international bodies, ensuring a robust and well-rounded understanding of the subject matter. Additionally, it involves a critical evaluation of the impacts of cyberattacks, examining their wide-ranging implications for individuals, organizations, and states. The research method culminates in a comprehensive policy analysis and development of strategic recommendations, aiming to propose actionable strategies that effectively enhance international cooperation and legal harmonization in combating cybercrime.

3. Global Impacts and Multifaceted Challenges

Various types of cybercrime are reported annually, such as online shopping fraud, online bank-related fraud, and different types of individual victim threats, such as cyberbullying (Reep-van et al., 2018). Most countries are spending money on prevention and handling the prevention of security measures to make them cost-effective. Prevention measures require reliable crime data so that governments can act appropriately (Gasket, 2019; Armin et al., 2015). The most victimized public members are usually the younger people who use the internet and are affected by computer viruses. The 2011--2012 crime survey for England revealed that approximately 37% of the younger age group experienced a greater impact than did the older group (McGuire, & Dowling, 2013).

Cybercriminals distribute illicit materials through various platforms, including social media websites, emails, online forums, and chat rooms. Compared with conventional crime, the use of enormous channels for single criminal activity is another unique challenge for law enforcement agencies in tracing and identifying criminal activity. There are various hurdles in the overall process; sometimes, even victims do not consider themselves victims. One of the suggestions for this approach is automatic authorship analysis to identify the address of the criminal or problem-creating (Zheng et al., 2003).

Cyberbullying is increasing globally due to increasing access to the internet and mobile technology. Most people in developed or underdeveloped countries use this technology in every field, including education, business, industry, etc. (Smith, 2009). This increased number of uses has welcomed criminal-minded people who have intentionally committed crimes repeatedly. This abusive relationship with the victim is considered cyberbullying. Various problems exist in investigating cyberbullying and taking action against it (Herrero et al., F& Urueña, 2021).

International collaboration, regulation, and legal safeguards in cyberspace are paramount. This is because, much like other global commons such as land, sea, air, and space, cyberspace spans various territorial boundaries, necessitating a coordinated approach for effective management and protection. The global community has acknowledged the urgency of a collective international effort to address swiftly escalating threats in cyberspace. An agreement or set of accords undersigned by the United Nations for establishing and maintaining peace, justice, and security in cyberspace. There needs to be an immediate response to a global treaty because of the rapid evolution of international cyberattacks, as seen in sovereign states that have faced coordinated attacks.

Therefore, the Budapest Convention transcends its status as a mere legal text; it enables numerous practitioners from participating parties to exchange experiences and foster relationships that promote cooperation in various cases, including emergencies, extending beyond the Convention's specified provisions. In their 2019 study, Maimon and Louderback provided an interdisciplinary review of cyber-dependent crimes, a category that may encompass a portion of the 7,427 computer-related crimes reported (Maimon & Louderback, 2019).

In 2010, the Commonwealth of Australia, along with the New Zealand Police and ACPO 2009, engaged in a cooperative effort focused on developing cyber-related crime and criminology strategies with an eye toward future developments (Pickering, 2010).

4. Cybercrime Legislation Worldwide

The dynamic nature of cybercrime, characterized by its continuous evolution and the sophisticated methods employed by perpetrators, poses significant challenges to the global legal framework. This complexity is further compounded by the diversity in the legal landscapes of different jurisdictions, each with its own set of laws, enforcement strategies, and challenges.

An in-depth analysis of these jurisdictions and the prevalent types of cybercrime is crucial for developing effective global cybersecurity measures.

The legal frameworks governing cybercrime vary widely across regions, reflecting differences in legislative priorities, technological advancements, and the perceived threat level of cyber activities. For example, countries within the European Union operate under a relatively harmonized legal framework, owing in part to directives and regulations such as the General Data Protection Regulation (GDPR) and the Directive on Security of Network and Information Systems (NIS Directive). Conversely, countries in regions with less harmonized legal systems face challenges in ensuring consistent cybercrime regulation and enforcement (Pickering, 2010; Wicki-Birchler, 2020). A series of case studies highlights the legislative nuances and challenges faced by different jurisdictions. For example, a case study on Japan reveals how the country's Cybercrime Control Law, amended to address evolving cyber threats, incorporates specific provisions for crimes such as unauthorized access to computers and the creation of malicious software (Holt, 2012). Moreover, a case study in Brazil highlights the challenges of enforcing the Marco Civil da internet in a rapidly growing digital environment, emphasizing jurisdiction, data retention, and privacy issues (Medeiros & Bygrave, 2015).

In addition to the detailed exploration of Japan's and Brazil's approaches to cybercrime legislation, it is imperative to consider examples from other jurisdictions that further illustrate the global challenge of combating cybercrime. These examples highlight the diversity of legal responses and the common hurdles in aligning national laws with international norms. The United States presents a comprehensive approach to cybersecurity, with various laws targeting cybercrime, including the Computer Fraud and Abuse Act (CFAA), which serves as the foundational statute for prosecuting cybercrimes involving unauthorized computer access (Mancosu & Vegetti, 2020). The U.S. also actively participates in international efforts to combat cybercrime, exemplifying the critical role of international cooperation in this domain. However, challenges remain in balancing security measures with privacy rights, a debate exemplified by the ongoing discussions around data encryption and law enforcement access to digital evidence.

India's Information Technology Act, 2000 (IT Act) and its subsequent amendments highlight the country's efforts to address the complexities of cybercrime within its rapidly growing digital economy (Nagarathna, 2020). The IT Act provides a legal framework for electronic governance, data protection, and cybercrime, reflecting an attempt to keep pace with technological advancements. However, enforcing these laws faces challenges, including jurisdictional issues and requiring more excellent technical expertise among law enforcement agencies.

Germany stands out for its stringent data protection laws and proactive cybersecurity measures. The Federal Data Protection Act (BDSG), in conjunction with the GDPR, sets high standards for personal data protection. Germany's Network Enforcement Act (NetzDG) further demonstrates the country's commitment to combating online crimes, including hate speech and misinformation (Schmitz & Berndt,2018). These efforts highlight the balance Germany seeks between individual rights and national security, serving as a model for other nations grappling with similar issues.

Nigeria's Cybercrimes (prohibition, prevention, etc.) Act of 2015 marked a significant step toward addressing cybercrime in a context characterized by rapid digital adoption and pervasive cyber fraud. The act covers many offenses, including cyber fraud, identity theft, and cyberstalk, reflecting the Nigerian government's recognition of the economic and social impacts of cybercrime. Implementation and enforcement, however, remain significant challenges, exacerbated by limited resources and the need for international collaboration (Kpae, 2020).

Australia's cybersecurity strategy emphasizes collaboration among the government, private sector, and international partners. The Cybercrime Act of 2001 and the recent Critical Infrastructure Security Reforms are part of Australia's legislative framework to protect national interests from cyber threats (Soldani,2020 and Gerald 2023). These laws are complemented by active participation in international agreements and partnerships, such as the Budapest Convention, demonstrating Australia's commitment to global cybersecurity efforts.

Given the dynamic and sophisticated nature of cybercrime, which presents significant challenges across various legal landscapes, a structured algorithm for international cybercrime investigation is proposed in Table 1. This algorithm is designed to address the complexities of differing regional laws, enforcement strategies, and nuances highlighted by case studies across jurisdictions such as Japan, Brazil, the United States, India, Germany, Nigeria, and Australia.

The Budapest Convention on Cybercrime, while serving as a cornerstone in the international fight against cybercrime, encounters limitations in its adaptability to rapidly emerging technologies and faces challenges owing to the varying levels of commitment among member states. These limitations can significantly hinder the Convention's effectiveness. The fast-paced evolution of digital technologies often outpaces the Convention's ability to adapt its legal frameworks accordingly, leaving gaps in regulations that cybercriminals can exploit (Le et al., 2021). Moreover, the disparity in commitment levels among member states to fully implement and enforce the Convention's provisions creates inconsistencies in global cybercrime prevention and prosecution efforts. This variance in enforcement and commitment can lead to jurisdictional loopholes, making it easier for cybercriminals to operate within or target countries with less stringent cybersecurity measures. As a result, the full potential of the Budapest Convention as a unified global effort to combat cybercrime has yet to be realized, underscoring the need for continuous updates to its legal instruments and enhanced cooperation and commitment among all member states.

Table 1 Structured Algorithm for International Cybercrime Investigation within Diverse Legal Frameworks.

Phase 1: Identification and Initial Assessment	1.1 Incident Reporting: Cybercrime incidents are identified through alerts, victim reports, or cybersecurity teams and are immediately reported to the designated national cybercrime unit. 1.2 Preliminary Analysis: Conduct a quick assessment to determine the nature, scope, and potential international elements of cybercrime, considering the type prevalent in the jurisdiction.
Phase 2: Jurisdictional Determination and Legal Framework Analysis	2.1 Determining Applicable Jurisdictions: Identifying the jurisdictions involved on the basis of the cybercrime's origin, targets, and data transit paths. 2.2 Analyze Legal Frameworks: Review the legal frameworks relevant to the jurisdictions identified, focusing on laws governing cybercrime, data protection, and international cooperation mechanisms.
Phase 3: Evidence Preservation and Collection	3.1 Secure Evidence: Implement measures to preserve volatile and nonvolatile digital evidence, adhering to the legal standards of the involved jurisdictions. 3.2 Collecting evidence: Systematically collecting digital evidence ensures that the process aligns with jurisdictions' varied legal requirements and maintains the integrity of evidence for international legal proceedings.
Phase 4: International Cooperation and Legal Instrument Application	4.1 Engaging International Instruments: Utilizing international legal instruments, such as the Budapest Convention, to facilitate cross-border evidence gathering, sharing, and law enforcement collaboration. 4.2 Coordinating with international agencies: Working with international bodies (e.g., INTERPOL, Europe) for support in navigating legal complexities and operational coordination among the jurisdictions involved.
Phase 5: In-depth Analysis and Attribution	5.1 Conducting forensic analysis: Analyze collected evidence via forensic methodologies compatible with the legal requirements of the involved jurisdictions to identify the perpetrators and their methods. 5.2 Attribution: Attempts to attribute cybercrime to specific individuals or groups, considering the legal nuances of direct and indirect evidence across jurisdictions.
Phase 6: Legal Action Preparation and Execution	6.1 Preparing legal documentation: Compile evidence, forensic analysis reports, and jurisdictional legal analyses into comprehensive documentation for legal proceedings. 6.2 Pursue Legal Action: Initiate legal actions following the most relevant jurisdiction(s), leveraging extradition agreements and mutual legal assistance treaties (MLATs) as necessary.
Phase 7: Post-Investigation Review and Policy Enhancement	7.1 Conduct Review: Analyze the effectiveness of the investigation, focusing on the interplay between national and international laws and the challenges encountered. 7.2 Enhancing policies and cooperation: On the basis of the lessons learned, we propose enhancements to national policies and international cooperation frameworks to streamline future investigations and strengthen global cybersecurity measures.

5. Global Collaboration in Cybersecurity: The Impact of the Budapest Convention on Combating Cybercrime

The legal frameworks and initiatives to combat cybercrime in the European Union represent a critical component within the broader global context of cybercrime regulation. The European Union has been at the forefront of addressing cyber threats through comprehensive legal measures, such as the Directive on Security of Network and Information Systems (NIS Directive) and the General Data Protection Regulation (GDPR) (Saqib et al., 2018). These frameworks are designed to enhance the security of network and information systems across the EU and to protect personal data. However, the fight against cybercrime in Europe is fraught with specific challenges, including the intricacies of implementing the NIS Directive's requirements across

diverse member states and ensuring GDPR compliance without impeding cybersecurity efforts. Cybercrime significantly impacts access to justice within Europe, complicating individuals' and organizations' ability to seek and secure justice. Jurisdictional complexities often arise in cybercrime cases, given the internet's borderless nature, leading to difficulties in determining which nation's laws apply and how to pursue legal action across borders. The nuances of cross-border legal cooperation and the enforcement of judgments in cybercrime cases further exacerbate these challenges, as differing legal standards and procedural requirements across EU member states can hinder effective collaboration and timely resolution of cases.

Despite these obstacles, digital innovation holds transformative potential for enhancing access to justice in the European context amidst the challenges posed by cybercrime. The adoption of digital platforms, online dispute resolution mechanisms, and the latest forensic technologies can revolutionize the justice landscape in cybercrime cases. For example, digital evidence-gathering tools and sophisticated cyber forensics can streamline investigations and facilitate the prosecution of cybercriminals. Moreover, online dispute resolution offers a faster, more accessible means for victims to seek redress.

The dual nature of challenges and opportunities presented by the digital transformation of European justice systems requires careful analysis. While technological advancements can significantly improve access to justice in cybercrime scenarios, they also raise concerns about data protection, privacy, and the potential for digital divides that could impede equal access to these new forms of justice (Calderoni, 2010). Case studies specific to the European context, such as cross-border investigations and the prosecution of the "Avalanche" network, exemplify the complexities and successes of legal responses to cybercrime. This case highlights the effectiveness of cross-border cooperation within the EU and between EU and non-EU countries, highlighting the critical role of Europe and the European Cybercrime Centre (EC3) in facilitating such collaboration. However, it also underscores the need for ongoing efforts to streamline legal processes and enhance the interoperability of justice systems across Europe to combat cybercrime effectively (Evans-Brown & Sedefov, 2018).

The Budapest Convention on Cybercrime establishes a comprehensive international framework for combating cybercrime, underscoring the necessity of harmonizing legal definitions and enhancing cooperation across jurisdictions. As the first international treaty targeting cybercrime, it provides crucial legal benchmarks for criminalization, procedural laws, and international cooperation mechanisms (Council of Europe, Budapest Convention on Cybercrime, ETS No. 185). The Convention's provisions, such as Article 2 on illegal access, Article 3 on illegal interception, and Article 4 on data interference, are pivotal in guiding the incorporation of these standards into the national legislation of European Union member states, aiming for a cohesive approach to cyber threats (Csonka, 2007).

Furthermore, the emphasis on mutual assistance (Article 25) and the expedited preservation of stored computer data (Article 29) within the Convention highlights essential areas for enhancing the capabilities of EU frameworks for efficient cross-border cooperation in cybercrime investigations. These elements underscore the argument for improved legal mechanisms within the EU, promoting streamlined processes in line with the Convention’s provisions for mutual legal assistance and data preservation (Polyzoidou, 2021).

The evolving nature of cyber threats, including challenges posed by encryption and cloud computing, necessitates updates to the Convention and corresponding EU legislation. The Convention’s structure, allowing for amendments, supports the continuous evolution of legal tools against cybercrime, reflecting the dynamic digital threat landscape. By referencing the Budapest Convention, the argument for adopting and adapting its standards within the EU has strengthened, advocating for a unified and robust legal framework against cybercrime (Wicki-Birchler, 2020). This approach aligns with global efforts, enhancing the EU’s ability to safeguard its digital domain against the growing challenge of cyber threats.

When the Council of Europe's Cybercrime Convention went into effect on July 1, 2004 (Imam et al., 2008). This represented a critical turning point in the battle against illegal online activities. The treaty became available for signatures on November 23, 2001, in Budapest, allowing both member and nonmember states participating in its development to sign it. Additionally, it was open for ratification by other nonmember states (Talimonchik, 2020).

The total number of ratifications/accessions is 67 (sixty-seven), and the number of signatures not accompanied by subsequent ratifications is two (Council of Europe: Chart of signatures and ratifications of Treaty 185. Convention on Cybercrime (ETS No. 185, 2022). The 67 states that ratified the Convention included member countries, the Council of Europe, and nations outside membership. In 2013, a decision extended an invitation to a nonmember state to join the treaty, which has remained in effect for five years since its inception. The initial global agreement on dealing with cybercrime has been revised.

The Budapest Convention was created approximately two decades ago to align legal frameworks and enhance international collaboration in addressing cybercrimes, such as denial-of-service attacks and the emerging menace of computer viruses, which could harm numerous nations (Moore et al., 2006). Nevertheless, it was authored before the internet's rapid expansion, the emergence of cloud computing, and the transformation of almost all forms of communication into digital formats (Mirkovic et al., 2004).

6. Application of International Law in Cyberspace

International law has no specifically tailored rules for regulating cyberspace. There are a few notable exceptions (for example, the Budapest Convention on Cybercrime and the still-in-forced African Union Convention on Cybersecurity and

Personal Data Protection). This is because technology is very recent and is progressing very quickly. Because of this, it took some time for people to determine whether established international law norms had applied to cyberspace.

Numerous states and international entities, including the European Union, ASEAN, the Organization of American States (OAS), and the G20, have recognized the applicability of current international law to the use of information and communication technologies (ICTs) within national boundaries. This acknowledgment underlines the importance of adhering to established legal frameworks in the rapidly evolving domain of ICT (Haataja & Akhtar-Khavari, 2018). Additionally, Sutter (2003) addresses information control in the online environment, emphasizing the global nature of such issues and the necessity for international cooperation and regulation (Sutter, 2003).

Although advanced countries have more internet users than do developing countries, cybercrime currently affects both developed and developing countries. It is combating effectively with cybercrime. It will demand broader engagement and collaboration, involving more nations than those who have signed the Council of Europe Convention on Cybercrime. This poses a formidable challenge. Reverting to the initial stages of creating a comprehensive convention from the beginning could entail years of diplomatic disagreements, a struggle that might fail to yield success (Buçaj, 2017). Unlike many other international and national concerns, cyberspace governance results from academic institutions and business entities constructing the internet with government funds.

It is widely recognized that international law lacks adequate standards in cyberspace. Nevertheless, some countries and entities contend that existing international law is sufficient to govern state actions in this domain. Conversely, numerous governments and stakeholders have asserted that the current legal framework contains gaps and inefficiencies necessitating the creation of new rules.

Recently, the efforts of United Nations member countries in addressing issues of international law in the cyber and ICT domains have increased. In addition to the original U.N. Group of Governmental Experts, these endeavors now include a newly formed Open-Ended Working Group under the UN General Assembly's First Committee and a separate initiative in the Third Committee to create a U.N. treaty on cybercrime. It is still being determined whether the United Nations will continue to be the primary hub for shaping discussions on the use of international law in this field. Regional entities such as the European Union could provide an alternative, occasionally circumventing specific geopolitical elements in UN discussions. Additional or forthcoming multistakeholder procedures could also assume a similar role (Hollis, 2021). The growing movement toward implementing principles of digital sovereignty is expected to have only a slight influence on how international law will be applied concerning the actions of nations in cyberspace.

Independent expert groups, distinct from state actors, played a pivotal role in formulating the Tallinn guidelines, significantly shaping the discourse on regulating state cyber activities within the international law framework. The influence of international legal experts is evident in three recent declarations from Oxford, offering new perspectives and insights into the medical industry and vaccine development during the COVID-19 pandemic and external interference in the 2020 U.S. presidential election (Le et al., 2020). These declarations highlight the challenges and protective measures needed in the healthcare sector amid the pandemic and the complexities of political processes during such crises (Patel et al., 2022). Additionally, the analysis by Flores (2022) on the Latino media's role in the 2020 U.S. presidential election offers insights into the election's context and external influences (De los Ángeles Flores, 2022).

The role of soft law in regulating cyberspace activities, which inherently possess international dimensions, is increasingly critical in an era where traditional legal frameworks struggle to keep pace with the global nature of digital interactions. Soft laws, including guidelines, codes of conduct, best practices, and voluntary standards, offer flexible and adaptive approaches to governance in the rapidly evolving digital landscape. Unlike complex law, which encompasses enforceable legal obligations, soft law provides a mechanism for cooperation and coordination that can quickly adapt to new challenges and technologies without formal ratification processes or legislative action (Yuliia & Lyudmyla, 2020).

One of the primary advantages of soft law in cyberspace is its ability to bridge gaps left by the limitations of traditional legal systems. These systems often face jurisdictional challenges and enforcement difficulties when dealing with cyber activities that transcend national boundaries. Soft laws, by contrast, can facilitate international collaboration by establishing common principles and norms that guide state and nonstate actors in a shared digital environment.

For example, the Tallinn Manual on International Law Applicable to Cyber Warfare, developed by an international group of legal scholars and practitioners, prominently illustrates soft law's utility in cyberspace (Schmitt, 2013). While not legally binding, the Tallinn Manual offers a comprehensive analysis of how existing international law applies to cyber conflicts, providing states and organizations with a reference point for navigating the complex legalities of cyber warfare. This manual has become an influential resource in shaping policies and strategies for cyber defense, demonstrating how soft law can effectively complement traditional legal frameworks in governing the multifaceted domain of cyberspace.

Moreover, soft law is pivotal in promoting cybersecurity standards and practices across different sectors. Initiatives such as the NIST Cybersecurity Framework in the United States exemplify how voluntary guidelines can drive the adoption of robust cybersecurity measures among critical infrastructure operators and other key stakeholders (Goodwin, 2022). Soft law instruments such as the NIST Framework enhance collective cybersecurity resilience without imposing rigid regulatory requirements by encouraging best practices in risk management and incident response.

7. Recommendations

On the basis of a comprehensive examination of legal frameworks, technical protocols, and scholarly discourse, the following recommendations have emerged to enhance the global response to cybercrime. These suggestions are predicated on an in-depth analysis of authoritative legal doctrines, contemporary technical standards, and expert opinions, ensuring their relevance and applicability to both present and future cybercrime challenges. The recommendations are rooted in a rigorous analysis of existing research, legal precedents, and technical guidelines. Implementing these measures will significantly enhance the international community's ability to confront and mitigate the challenges posed by cybercrime, ensuring a safer digital environment for all.

Consistent with evolving technological landscapes and emerging cyber threats, the Budapest Convention requires regular updates. This includes the integration of provisions for cloud computing, the challenges of encryption, and nascent cybercrime methodologies. Such updates should be based on recent technical standards (e.g., ISO/IEC 27001 for information security management) and expert recommendations, ensuring that legal instruments remain effective against sophisticated cyber threats.

Drawing from a comparative analysis of legal systems and technical protocols, we recommend harmonizing legal definitions and standards across jurisdictions. This harmonization should consider diverse legal traditions (common law vs. civil law) and the technical specificity of cybercrimes, as outlined in the relevant literature and international legal instruments. Harmonization will facilitate a more unified and efficient global legal apparatus to combat cybercrime.

To improve the efficiency of mutual legal assistance and extradition processes, we advocate for streamlined procedures that reflect best practices in international law and digital evidence handling. This includes adopting standardized protocols for electronic evidence preservation and exchange, as recommended by the Council of Europe's Electronic Evidence Guide, to increase the speed and reliability of cross-border legal responses.

By focusing on the critical role of technology companies and ISPs in cybercrime prevention, we propose bolstering partnerships between governments and the private sector. This involves creating formal frameworks for information sharing and cyber threat intelligence grounded in successful collaboration models (e.g., the EU's NIS Directive on the security of network and information systems) and respecting privacy and data protection standards.

Recognizing the limitations of existing treaties in addressing the full spectrum of cybercrime, we suggest exploring the development of new legal instruments under the auspices of the United Nations or other global entities. These instruments should specifically address cybercrime, incorporating insights from technical standards bodies (such as the internet Engineering Task Force) and leveraging lessons learned from existing conventions to craft comprehensive and adaptable legal responses.

We emphasize the importance of equipping law enforcement and judicial authorities with the necessary skills to address cybercrime, so we recommend investing in global training initiatives. These programs should cover digital forensics, cybercrime investigation techniques, and the application of international legal frameworks, referencing best practices from organizations such as INTERPOL and the International Association of Cybercrime Prevention.

To mitigate the risk of cybercrime at its source, we propose global campaigns to increase awareness of cybersecurity best practices among individuals, businesses, and government entities. These campaigns should be informed by psychological and educational research on effective messaging and utilize platforms and methodologies that ensure widespread reach and impact.

Creating specialized research and policy centers is essential to sustaining the momentum of legal and policy innovation in cybercrime prevention. These centers continuously monitor cybercrime trends, policy development, and advocacy, ensuring that legislative and technical responses remain aligned with the evolving cyber threat landscape.

Finally, efforts to combat cybercrime must balance protecting individual privacy and human rights. Recommendations must include developing legal safeguards that prevent overreach and abuse, guided by human rights frameworks and ethical considerations in cybersecurity practices.

8. Conclusions

This paper underscores the urgent necessity for comprehensive global regulation of cybercrime through international law and conventions. We advocate for a unified approach encompassing updates to existing frameworks, enhanced international cooperation, and broader stakeholder involvement in the fight against cyber threats. The Budapest Convention serves as a crucial milestone, highlighting the imperative for global collaboration and the alignment of legal strategies to address the multifaceted challenges posed by cybercrime effectively. However, we emphasize the need for the continuous evolution of such conventions to keep pace with rapid technological advancements and the increasingly sophisticated nature of cyber threats.

Our study emphasizes that the borderless nature of cybercrime demands a unified response that transcends national boundaries and legal systems. Given the diversity in legal practices across countries, particularly in common law and civil law jurisdictions, we stress the importance of a flexible yet cohesive approach to defining and prosecuting cybercrimes.

Additionally, the rise of sophisticated cyberattacks targeting critical infrastructures worldwide underscores the vulnerability of nations. It emphasizes the necessity of a coordinated international response involving government agencies and private sectors.

While applying international law in cyberspace poses challenges due to the novelty and complexity of technology, it remains crucial. We advocate adapting and expanding existing legal norms to cover cyberspace effectively. International treaties such as the Budapest Convention are vital in setting legal standards and facilitating collaboration and information sharing among nations.

Furthermore, our research identifies the critical need for enhanced cooperation between the public and private sectors in cybercrime investigations, emphasizing the importance of establishing legitimate and ethical data collection and sharing methods. Such collaboration is essential for effective law enforcement while respecting individual rights and privacy.

Our findings underscore the imperative to comprehensively strengthen international legal instruments and cooperation to address the growing cybercrime threat. We urge the international community, including states, intergovernmental organizations, and the private sector, to collaborate more closely and develop comprehensive strategies. These strategies should focus on the legal prosecution of cybercrimes and preventive measures, public awareness, and the development of robust cybersecurity infrastructures. By doing so, we believe that the international community can better safeguard against the ever-evolving landscape of cyber threats and ensure the stability and security of the digital world.

Ethical Considerations

Not applicable.

Conflict of Interest

The authors declare that they have no conflicts of interest.

Funding

This research did not receive any financial support.

References

Armin, J., Thompson, B., Ariu, D., Giacinto, G., Roli, F., & Kijewski, P. (2015, August). Two thousand twenty cybercrime economic costs: No measure, no solution. In *2015, the 10th International Conference on Availability, Reliability, and Security* (pp. 701-710). IEEE.

Back, S., Lee, J., & Soor, S. (2018). Spatial and temporal patterns of cyberattacks: Effective cybercrime prevention strategies around the globe. *J-Institute, 3*(1), 7-13. https://doi.org/10.22471/protective.2018.3.1.07

Barezzani, S. (2023). General data protection regulation (GDPR). In *Encyclopedia of Cryptography, Security and Privacy* (pp. 1-6). https://doi.org/10.1007/978-3-642-27739-9_1811-1

Brandão, A., & Camisão, I. (2021). Playing the market card: The Commission's strategy to shape EU cybersecurity policy. *JCMS Journal of Common Market Studies, 60*(5), 1335-1355. https://doi.org/10.1111/jcms.13158

Buçaj, E. (2017). The need for regulation of cyber terrorism phenomena in line with principles of international criminal law. *Acta Universitatis, 13*(1), 141-162.

Calderoni, F. (2010). The European legal framework on cybercrime: Striving for an effective implementation. *Crime, Law and Social Change, 54*(5), 339-357. https://doi.org/10.1007/s10611-010-9261-6

Choi, K. S., Lee, C. S., & Louderback, E. R. (2020). Historical evolutions of cybercrime: From computer crime to cybercrime. In *The Palgrave Handbook of International Cybercrime and Cyber Deviance* (pp. 27-43). Palgrave Macmillan.

Council of Europe. (2022). Chart of signatures and ratifications of Treaty 185. *Convention on Cybercrime* (ETS No. 185). Status as of 17/09/2022.

Csonka, P. (2007). The Council of Europe's Convention on Cyber-crime and other European initiatives. *Revue Internationale de Droit Pénal, 77*(3), 473-501. https://doi.org/10.3917/ridp.773.0473

De los Ángeles Flores, M. (2022). Intermedia agenda-setting effect of Latino television in the 2020 US presidential election: A comparative study of Telemundo and Univision. In *Contemporary Politics, Communication, and the Impact on Democracy* (pp. 186-208). IGI Global.

Dumchykov, M., Utkina, M., & Bondarenko, O. (2022). Cybercrime as a threat to the national security of the Baltic States and Ukraine: The comparative analysis. *International Journal of Safety and Security Engineering, 12*(4), 481-490. https://doi.org/10.18280/ijsse.120409

Dupont, B., & Whelan, C. (2021). Enhancing relationships between criminology and cybersecurity. *Journal of Criminology, 54*(1), 76-92. https://doi.org/10.1177/00048658211003925

Evans-Brown, M., & Sedefov, R. (2018). Responding to new psychoactive substances in the European Union: Early warning, risk assessment, and control measures. In *New Psychoactive Substances* (pp. 3-49). https://doi.org/10.1007/164_2018_160

Gasket, B. (2019). *Reader's Guide to Understanding the US Cyber Enforcement Architecture and Budget*. Third Way.

Goodwin, S. (2022). The need for a financial sector legal standard to support the NIST Cybersecurity Framework. In *SoutheastCon 2022* (pp. 89-95). https://doi.org/10.1109/SoutheastCon48659.2022.9764006

Haataja, S., & Akhtar-Khavari, A. (2018). Stuxnet and international law on the use of force: An informational approach. *Cambridge International Law Journal, 7*(1), 99-121.

Herrero, J., Torres, A., Vivas, P., Hidalgo, A., Rodríguez, F. J., & Urueña, A. (2021). Smartphone addiction and cybercrime victimization in the context of lifestyles routine activities and self-control theories: The user's dual vulnerability model of cybercrime victimization. *International Journal of Environmental Research and Public Health, 18*(7), 3763. https://doi.org/10.3390/ijerph18073763

Hollinger, R. C. (1991). Hackers: Computer heroes or electronic highwaymen? *ACM SIGCAS Computers and Society, 21*(1), 6-17.

Hollis, D. (2021). A brief primer on international law and cyberspace. *Carnegie Endowment for International Peace*. https://carnegieendowment.org/2021/06/14/brief-primer-on-international-law-and-cyberspace-pub-84763

Holt, T. J. (2012). Examining the forces shaping cybercrime markets online. *Social Science Computer Review, 31*(2), 165-177. https://doi.org/10.1177/0894439312452998

Huang, H., Siegel, J., & Madnick, S. (2018). Systematically understanding the cyber attack business: A survey. *ACM Computing Surveys (CSUR)*, 51(4), 1-36. https://doi.org/10.1145/3192948

Imam, A., Mohammed, B., Wilson, D. C., & Cheeseman, C. R. (2008). Solid waste management in Abuja, Nigeria. *Waste Management, 28*(2), 468-472. https://doi.org/10.1016/j.wasman.2007.01.014

Koops, B. (2010). The internet and its opportunities for cybercrime. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.1738223

Kpae, G. (2020). Cyber threat to critical infrastructure and defending national security in Nigeria. *International Journal of Economics, Business and Management Studies, 7*(2), 214-223. https://doi.org/10.20448/802.72.214.223

Le Nguyen, C., & Golman, W. (2021). Diffusion of the Budapest Convention on cybercrime and the development of cybercrime legislation in Pacific Island countries: 'Law on the books' vs 'law in action'. *Computer Law & Security Review, 40*, 105521. https://doi.org/10.1016/j.clsr.2021.105521

Le, T. T., Andreadakis, Z., Kumar, A., Román, R. G., Tollefsen, S., Saville, M., & Mayhew, S. (2020). The COVID-19 vaccine development landscape. *Nature Reviews Drug Discovery, 19*(5), 305-306. https://doi.org/10.1038/d41573-020-00073-5

Levy, S. (1984). *Hackers: Heroes of the computer revolution* (Vol. 14). Garden City, NY: Anchor Press/Doubleday.

M Aditya Gerald. (2023). Efforts to enhance Australia's cyber security by developing a partnership with Indonesia in the field of cyber diplomacy. *Global Local Interactions: Journal of International Relations, 3*(2), 93-102. https://doi.org/10.22219/gli.v3i2.28049

Maimon, D., & Louderback, E. R. (2019). Cyber-dependent crimes: An interdisciplinary review. *Annual Review of Criminology, 2*, 191-216. https://doi.org/10.1146/annurev-criminol-011518-024659

Mancosu, M., & Vegetti, F. (2020). What you can scrape and what is right to scrape: A proposal for a tool to collect public Facebook data. *Social Media + Society, 6*(3), 205630512094070. https://doi.org/10.1177/2056305120940703

McGuire, M., & Dowling, S. (2013). *Cybercrime: A review of the evidence. Summary of key findings and implications*. Home Office Research Report, 75, 1-35.

Medeiros, F. A., & Bygrave, L. A. (2015). Brazil's Marco Civil da Internet: Does it live up to the hype? *Computer Law & Security Review, 31*(1), 120-130. https://doi.org/10.1016/j.clsr.2014.12.001

Mirkovic, J., Dietrich, S., Dittrich, D., & Reiher, P. (2004). *Internet denial of service: Attack and defense mechanisms*. Prentice Hall PTR.

Moore, D., Shannon, C., Brown, D. J., Voelker, G. M., & Savage, S. (2006). Inferring internet denial-of-service activity. *ACM Transactions on Computer Systems (TOCS), 24*(2), 115-139. https://doi.org/10.1145/1133305.1133307

Mphatheni, M., & Maluleke, W. (2022). Cybersecurity as a response to combating cybercrime. *International Journal of Research in Business and Social Science, 11*(4), 384-396. https://doi.org/10.20525/ijrbs.v11i4.1714

Nagarathna, A. (2020). Cybercrime regulation through laws and strategies: A glimpse into the Indian experience. *International Journal of Digital Law, 1*(1), 53-64. https://doi.org/10.47975/ijdl/1nagarathna

Patel, R., Kaki, M., Potluri, V. S., Kahar, P., & Khanna, D. (2022). A comprehensive review of SARS-CoV-2 vaccines: Pfizer, Moderna & Johnson & Johnson. *Human Vaccines & Immunotherapeutics, 18*(1), 2002083. https://doi.org/10.1080/21645515.2021.2002083

Pickering, S. (2010). Editorial. *Australian & New Zealand Journal of Criminology, 43*(1), iii-iii. https://doi.org/10.1375/acri.43.1.iii

Polyzoidou, V. (2021). Combatting cybercrime: Thoughts based on the second additional protocol (draft) to the Budapest Convention on Cybercrime. In *EU Internet Law in the Digital Single Market* (pp. 285-306). https://doi.org/10.1007/978-3-030-69583-5_15

Reep-van den Bergh, C. M., & Junger, M. (2018). Victims of cybercrime in Europe: A review of victim surveys. *Crime Science, 7*(1), 1-15. https://doi.org/10.1186/s40163-018-0084-6

Saqib, N., Germanos, V., Zeng, W., & Maglaras, L. (2018). Mapping of the security requirements of GDPR and NISD. *EAI Endorsed Transactions on Security and Safety, 7*(e2). https://doi.org/10.4108/eai.30-6-2020.166283

Schmitt, M. (2013). *Tallinn Manual on the International Law Applicable to Cyber Warfare: The law of cyber armed conflict*. Cambridge University Press. https://doi.org/10.1017/CBO9781139169288

Schmitz, S., & Berndt, C. M. (2018). The German Act on Improving Law Enforcement on Social Networks (NetzDG): A blunt sword? *Available at SSRN 3306964*. https://doi.org/10.2139/ssrn.3306964

Smith, P. K. (2009). Cyberbullying: Abusive relationships in cyberspace. *Zeitschrift für Psychologie/Journal of Psychology, 217*(4), 180-181. https://doi.org/10.1027/0044-3409.217.4.180

Soldani, D. (2020). On Australia's cyber and critical technology international engagement strategy towards 6G: How Australia may become a leader in cyberspace. *Journal of Telecommunications and the Digital Economy, 8*(4), 127-158. https://doi.org/10.18080/jtde.v8n4.340

Sutter, G. (2003). Introduction: Controlling information in the online environment. *International Review of Law, Computers & Technology, 17*(3), 251-254. https://doi.org/10.1080/1360086032000163151

Talimonchik, V. P. (2020). Legal aspects of international information security. In *Security and Privacy from a Legal, Ethical, and Technical Perspective* (pp. 55-74). https://doi.org/10.5772/intechopen.86119

Tapia, J. (2022). The Budapest Convention on Cybercrime. https://doi.org/10.13140/rg.2.2.12758.32323

The United States Department of Justice. (2001). *Equality and Law Reform Annual Report*. p. 51.

Wicki-Birchler, D. (2020). The Budapest Convention and the General Data Protection Regulation: Acting in concert to curb cybercrime? *International Cybersecurity Law Review, 1*(1-2), 63-72. https://doi.org/10.1365/s43439-020-00012-5

Yuliia, Y., & Lyudmyla, H. (2020). International aspects of legal regulation of information relations in the global internet. *Law, 11*. https://doi.org/10.31548/law2020.03.022

Zheng, R., Qin, Y., Huang, Z., & Chen, H. (2003). Authorship analysis in cybercrime investigation. In *Intelligence and Security Informatics: First NSF/NIJ Symposium, ISI 2003, Tucson, AZ, USA, June 2–3, 2003 Proceedings 1* (pp. 59-73). Springer Berlin Heidelberg. https://doi.org/10.1007/978-3-540-40081-7_8