DOI: 10.38146/BSZ-AJIA.2026.v74.i1.pp183-204

Adapting the Budapest Convention to address emerging cyber threats

Francois Regis Nshimiyimana
Researcher on Electronic Evidence in Cybercrime
Károli Gáspár University of the Reformed Church in Hungary,
Doctoral School of Law and Political Sciences
regisnshimiye82@gmail.com

Abstract

Aim: This paper examines the necessity of adapting the Budapest Convention to address emerging cyber threats, including ransomware, the misuse of cryptocurrencies, artificial intelligence(AI), Internet of Things (IoT) vulnerabilities, and cross-border jurisdictional challenges. The paper highlights the legal gaps and proposes updates to ensure the Convention remains relevant in combating evolving cybercrimes.

Methodology: A comparative legal research approach is employed, analyzing the current provisions of the Budapest Convention alongside case studies of emerging Cyber threats. The research integrates doctrinal analysis and practical insights, including reviews of international legal frameworks, technological developments, and enforcement practices.

Findings: The study identifies significant gaps in the Budapest Convention, including the lack of provisions addressing advanced cybercrime methods and the challenges of cross-border enforcement. These gaps hinder the Convention's ability to address contemporary Cyber threats effectively. The paper suggests concrete reforms, such as incorporating provisions for AI-driven crimes, cryptocurrency regulations, and enhanced cross-border cooperation mechanisms.

Value: This paper contributes to the ongoing discourse on international cybercrime law by proposing actionable updates to the Budapest Convention. It provides a roadmap for policymakers and legal practitioners to enhance the Convention's relevance and effectiveness in tackling the dynamic landscape of cyber threats while safeguarding fundamental rights.

The manuscript was submitted in English. Received: 25 March 2025. Revised: 9 May 2025 Accepted: 24 July 2025.

Keywords: Budapest Convention, Cybercrime, Legal framework, Emerging threats.

Introduction

The Budapest Convention on Cybercrime, established in 2001, is the first international treaty to harmonize national laws, improve investigative techniques, and foster international cooperation to combat cybercrime. Over two decades later, the digital landscape has evolved significantly, presenting new challenges that the Convention's original framework needs to address. Emerging threats, including ransomware, cryptocurrency-facilitated crimes, artificial intelligence (AI)-driven cyberattacks, and vulnerabilities in Internet of Things (IoT) devices, have demonstrated the need for robust and adaptive legal measures (McCall, 2024). Moreover, the Convention faces increasing criticism for its inability to resolve cross-border jurisdictional conflicts effectively. With cybercriminals operating beyond national boundaries, the lack of streamlined international protocols has limited the effectiveness of international cooperation in addressing transnational cybercrime (AllahRakha, 2024). As a result, there is a growing consensus among legal scholars and practitioners that the Budapest Convention requires significant updates to maintain its relevance and efficacy in combating the rapidly evolving landscape of cyber threats.

This paper analyzes the gaps in the Budapest Convention, focusing on its shortcomings in addressing emerging technologies and cross-border enforcement challenges. Using a comparative legal research methodology, it explores how the Convention can be adapted to meet the demands of the digital age while balancing security imperatives with fundamental rights (Taylor, 2021). The findings aim to contribute to the ongoing discourse on international cybercrime legislation and provide practical recommendations for policymakers.

Overview of the Budapest Convention on Cybercrime

Adopted in 2021 by the Council of Europe, the Budapest Convention is the first and most significant international treaty addressing Cybercrime and electronic evidence. It was developed to harmonize national laws, improve investigative techniques, and facilitate international cooperation. With 75 member states as of 2024, the treaty remains open for accession by non-European countries, demonstrating its global reach and relevance in combating cybercrime worldwide

(URL1). The Convention was developed in response to the increased misuse of technology for criminal purposes, with offenses often crossing borders. It includes a set of baseline provisions for harmonizing substantive and procedural law among signatories, supplemented by protocols such as the first protocol on racist and xenophobic acts and the second protocol on enhancing cooperation and evidence-sharing. The key provisions of the Budapest Convention are:

- Substantive criminal law: Those provisions define critical cybercrime offenses such as unauthorized access, data interference, system interference, and computer-related fraud.
- Procedural powers: These articles provide law enforcement with tools for collecting real-time traffic data, preserving data, and searching and seizing stored computer data.
- International cooperation: Establishes mechanisms like the 24/7 contact network for expediting cross-border assistance and ensures mutual legal assistance among parties.

The Budapest Convention has significantly shaped the global cybercrime legislation. In 2021, approximately 124 countries had adopted legal frameworks inspired by its provisions. The 24/7 contact network has proven essential in high-profile cases, such as the Charlie Hebdo attacks, enabling rapid information sharing across jurisdictions. Additionally, the Convention has improved cooperation with private sector entities, particularly U.S.-based service providers, which supply data in about two-thirds of law enforcement requests (Gardner, 2020). However, the Convention is limited in addressing emerging threats such as ransomware, AI-driven attacks, and cryptocurrency-based crimes. These gaps underscore the need for updates to ensure the treaty remains effective in combating the ever-evolving cyber threats landscape.

Emerging cyber-threats in cybercrime

A recent literature review highlights the fast-paced evolution of cybercrime, emphasizing the increasing sophistication of cybercriminal activities. Emerging technologies such as artificial intelligence (AI) and the Internet of Things (IoT) have exacerbated vulnerabilities in both national and international legal frameworks (Kuzior et al., 2024). Moorthy and Marwala (2021) argue that AI serves a dual role, functioning both as a tool for cybercriminals and an asset for law enforcement, making it imperative for legal frameworks to evolve accordingly. Similarly, Müller, Backes, and colleagues emphasize the urgency of

updating treaties like the Budapest Convention to keep pace with the proliferation of digital threats and the complexities involved in prosecuting cybercrime across multiple jurisdictions (Backes et al. 2019).

Recent scholarship further underscores the dual role of AI and IoT in cybersecurity. McCall (2024) observes that while these technologies enable significant advancements in automation and data-driven decision-making, they simultaneously introduce complex vulnerabilities. The rapid proliferation of IoT devices, many of which lack robust security measures, combined with increasingly sophisticated AI-driven attacks, expands the potential attack surface and necessitates advanced, adaptive defense strategies. Complementing this perspective, Rehman and Liu (2021) discuss the integration of AI and IoT into proactive cyber defense systems. They highlight the value of AI in analyzing real-time data from IoT environments to detect anomalies and predict potential security breaches. Such proactive approaches enable organizations to anticipate and mitigate threats before they materialize, ultimately enhancing the resilience of critical systems. These studies collectively suggest that although AI and IoT technologies hold promise for strengthening cybersecurity capabilities, they also require the development of tailored legal and technical frameworks. Without these, the international community will struggle to address the rapidly evolving threat landscape effectively.

Ransomware: Escalating threat

Ransomware attacks have become an escalating global threat in recent years. Cybercriminals use ransomware to lock victims' data, demanding payment, typically in cryptocurrency, to release it. This makes it more difficult for authorities to trace the payments. A notable example is the 2020 attack on Universal Health Services (UHS) in the United States, which crippled operations across over 400 facilities (Kaspersky, 2020). Additionally, groups such as REvil and DarkSide have been particularly active, targeting large businesses and critical infrastructure. In 2021, Kaseya, an IT management company, was targeted by a supply-chain ransomware attack that affected thousands of organizations worldwide (Symantec, 2021).

Ransomware remains a serious and evolving threat, with attackers continuously developing more sophisticated methods to carry out these extortion-based attacks. As cybercriminals become more advanced in their tactics, organizations must adopt comprehensive cybersecurity strategies to mitigate risks. The Budapest Convention on Cybercrime must be updated to provide more effective tools for international cooperation in combating ransomware, especially when tracing payments made through cryptocurrencies and ensuring efficient data sharing between

jurisdictions. According to the European Union Agency for Cybersecurity (ENISA), the increasing frequency of ransomware attacks highlights the limitations of current international legal frameworks in tackling this growing problem (URL2).

Cryptocurrency and cybercrime

The Budapest Convention, the first binding international treaty on cybercrime, focuses on electronic evidence and procedural tools for international cooperation. However, it predates the proliferation of cryptocurrencies and lacks provisions specific to this technology (Council of Europe, 2001). For example, its data preservation and evidence collection measures need to be revised for the unique characteristics of blockchain transactions (URL3).

Scholars like De Hert and Papakonstantinou argue that the Convention's effectiveness in combating modern cybercrime diminishes without addressing cryptocurrency-enabled offenses (De Hert & Papakonstantinou, 2012). Criminals use decentralized ledgers to obscure financial trails, creating new barriers for law enforcement. Syed et al. highlight the growing prevalence of ransomware attacks demanding cryptocurrency payments, emphasizing the urgent need for updates in the international legal framework (Temara, 2024).

Challenges and the case for updating in this regard are:

- Anonymity and decentralization: Cryptocurrency networks operate without a central authority, making tracing transactions or identifying perpetrators difficult. Current legal provisions under the Convention need to address the unique technical challenges posed by blockchain forensics.
- Asset recovery and seizure: The absence of a specific protocol for freezing or seizing cryptocurrency assets hampers efforts to disrupt criminal operations. While Article 19 of the Convention addresses research and seizure, it is not tailored for digital wallets.
- Cross-border coordination: Cryptocurrency operates beyond national jurisdictions, requiring more effective international cooperation. Due to the absence of standardized protocols, law enforcement agencies face delays in securing access to foreign exchange data. This would enable law enforcement to engage in more effective cross-border data sharing and financial tracking, ensuring that criminals cannot hide behind cryptocurrency's anonymity. Additionally, the FATF (Financial Action Task Force) has set guidelines for addressing the illicit use of cryptocurrencies, but these frameworks are still evolving (URL4). Europol and Interpol are collaborating on investigations, but a formal update to the Convention is crucial to ensure unified legal approaches.

Artificial intelligence (AI) in cybercrime

Artificial intelligence (AI) has become both a tool for cybercriminals and a valuable asset for law enforcement. However, current legal frameworks, including the Budapest Convention, lack provisions addressing AI-driven threats such as automated phishing, deepfakes, and adaptive malware. AI-driven crimes raise novel legal challenges, particularly in authenticating AI-generated evidence and establishing liability. For example, in France, phishing campaigns using AI-generated communications have complicated efforts to identify perpetrators (Lemoine, 2022). Deepfake technologies have been used in Ireland to manipulate digital content, challenging the judiciary's capacity to verify authenticity (Fitzgerald, 2023). Hungary has reported increased use of AI for identity theft and financial fraud, prompting calls for updated laws (Mezei & Krasznay, 2022).

To respond effectively, the Budapest Convention should be revised to clearly define AI-enabled offenses, develop guidelines for handling AI-generated evidence, and enhance mechanisms for international cooperation. Collaborating with AI developers and cybersecurity experts would also support ethical standards and threat detection across jurisdictions.

Internet of Things (IoT) vulnerabilities

The Internet of Things (IoT) refers to the network of interconnected devices, sensors, and systems that communicate and exchange data over the internet, such as smart home appliances, wearable devices, and industrial machines. While IoT technology has brought significant advancements in convenience, efficiency, and automation, it also introduces new cybersecurity risks, making it an emerging threat in the realm of cybercrime. The rapid expansion of IoT devices creates vulnerabilities, as many of these devices are not designed with robust security measures, leaving them susceptible to exploitation by cybercriminals. IoT vulnerabilities have already been demonstrated in several high-profile incidents. For instance, in 2016, the Mirai botnet attack, which involved IoT devices such as security cameras and routers, caused widespread disruptions by launching massive distributed denial-of-service (DDoS) attacks on websites, including major platforms like Twitter and Spotify (Moussouris, 2016). Similarly, in France, the use of unsecured IoT devices in smart homes has led to an increase in cyberattacks, where attackers exploit these vulnerabilities to gain unauthorized access to users' data and networks (Lemoine, 2021). In Hungary, researchers have pointed out that vulnerabilities in IoT-enabled critical infrastructure, such as power grids, have made these systems prime targets for

cybercriminals, raising concerns about the potential consequences of an IoT-based cyberattack on national security (Kovács & Horváth, 2022).

The Budapest Convention, established in 2001, does not include specific provisions addressing the unique threats posed by IoT-related cybercrimes. The growing number of IoT devices and their vulnerabilities highlight the need for a legal update to address IoT-related cybercrimes, including unauthorized access, data theft, and exploitation of critical infrastructure. Updating the Convention would involve creating specific legal frameworks for IoT security, improving international cooperation to investigate and respond to IoT-based cybercrimes, and developing cybersecurity standards for manufacturers of IoT devices (URL5). Without such updates, the Budapest Convention will continue to remain inadequate for effectively addressing IoT-driven cyber threats.

Cross-border jurisdictional challenges

One of the Budapest Convention's greatest strengths is its focus on international cooperation, yet cybercrime's digital borderlessness presents significant challenges. Jurisdictional issues arise when cybercriminals operate in one country while targeting victims in another, often making it difficult for national authorities to act.

Scholars like Flynn emphasize that the Budapest Convention, while pioneering, has limitations in effectively addressing cross-border jurisdictional conflicts (Flynn, 2014). Flynn argues that the Convention needs provisions that account for the complexities of sovereignty in a digital age, particularly concerning data storage and access. Similarly, Svantesson and Clarke highlight the importance of creating a framework for mutual legal assistance treaties (MLATs) that streamline cross-border investigations (Cerezo et al., 2007). They point out that critical evidence may remain inaccessible without an updated mechanism due to conflicting privacy and data protection laws.

Recent case law has shown how cross-border jurisdiction can complicate cybercrime prosecutions. The Microsoft Ireland case, where the US government sought access to data stored on Microsoft servers in Ireland, exemplifies the challenge of reconciling national laws with international data protection and privacy standards (Microsoft Corporation V. United States, 2018). The European Court of Justice ruled that the US could not access the data, highlighting the complexity of cross-border data requests. To address these challenges, the Budapest Convention should be updated to provide more robust mechanisms for cooperation on data access and evidence sharing, particularly in cases where the data crosses multiple jurisdictions with differing legal standards.

Importance and broader definitions of emerging cyber threats

Emerging cyber threats, defined by their sophistication and rapidly evolving nature, pose significant risks to individuals, organizations, and nations. These threats go beyond traditional cybercrimes, encompassing activities like advanced persistent threats (APTs), deepfake technologies, quantum computing-based hacking, and the misuse of artificial intelligence (AI). Understanding their importance and broader definitions is critical for developing comprehensive legal and technological frameworks. Cyber threats increasingly target crucial infrastructure, such as power grids, financial systems, and healthcare facilities. For example, the Colonial Pipeline ransomware attack in 2021 demonstrated the devastating impact of cyberattacks on national economies and public safety. The incident disrupted fuel supplies across the U.S. East Coast, costing millions of dollars in ransom and economic losses (URL6). Nation-states and non-state actors use cyber tools for espionage, sabotage, and influence campaigns. Cyber threats such as the SolarWinds cyberattack, attributed to Russian state actors, breached government and corporate networks globally, undermining trust in cybersecurity measures. Cybercrime costs may reach as much as $10.5 trillion annually by 2025 (URL7). This includes losses from intellectual property theft, fraud, and system downtime caused by attacks. Without comprehensive definitions and laws, addressing these threats remains challenging.

Misusing technologies like deepfakes undermines trust in digital content and poses significant risks to privacy, reputation, and democracy. Deepfake technology, which allows the creation of highly convincing manipulated videos, audio, and images, has been exploited for malicious purposes, such as spreading misinformation and disinformation. For instance, during the 2020 U.S. presidential election, deepfake videos were used to create false narratives about political candidates, manipulating public opinion and inciting division among voters (Pennycook & Rand, 2020). In France, a deepfake video involving a prominent political figure was used to spread harmful rumors, causing reputational damage and public confusion (Berrada, 2021). Furthermore, deepfakes have been used to create fake videos of public figures, leading to privacy violations and harassment, particularly targeting women and celebrities (Ferrara, 2021). These incidents not only damage individual reputations but also threaten the integrity of democratic processes by spreading misleading information and eroding public trust in the media. In response, there is an urgent need to update international legal frameworks like the Budapest Convention to specifically address the challenges posed by deepfake technology. Legal mechanisms should be introduced to criminalize the creation and distribution of harmful deepfakes,

enhance international cooperation in tracking and prosecuting offenders, and develop technological tools to detect and mitigate the impact of deepfake content on digital platforms. Without such updates, existing laws remain inadequate to tackle the growing threat that deepfakes pose to privacy, democracy, and trust in digital media.

Broader definitions and coverage of cyber threats

As the digital landscape evolves, the traditional definitions of cybercrime, which primarily focus on offenses such as hacking and identity theft, must be revised to address a broader spectrum of emerging threats. These expanded definitions should incorporate various forms of cyber threats, including cyberterrorism, cyber-enabled economic espionage, AI and automation threats, Internet of Things (IoT) vulnerabilities, and quantum computing risks.

- Cyberterrorism refers to the use of cyber tools to intimidate or coerce governments or civilians. A notable example of this was the 2017 WannaCry ransomware attack, which not only caused significant financial losses but also disrupted essential services, including healthcare and transportation, across multiple countries. This attack highlighted the potential for cybercriminals to use ransomware as a form of cyberterrorism, disrupting societies and economies on a global scale (URL8).
- Cyber-enabled economic espionage involves the use of cyber tools to steal trade secrets or intellectual property for competitive advantage. A high-profile case illustrating this threat is the U.S. v. Huawei Technologies Co., where allegations of state-sponsored espionage were made, accusing the Chinese tech giant of stealing intellectual property to gain an economic edge (U.S. Department of Justice, 2020). Such activities erode trust in international commercial relations and pose serious risks to global economic security.
- Artificial Intelligence (AI) and automation threats have become more prevalent as cybercriminals increasingly use AI-powered tools to carry out sophisticated attacks. For example, automated phishing schemes powered by AI can create highly convincing fraudulent emails that bypass traditional detection systems, making it harder for organizations to protect sensitive data. These advanced techniques necessitate updated definitions to keep pace with evolving cybercrime tactics.
- Internet of Things (IoT) vulnerabilities present another growing concern. The interconnectedness of IoT devices significantly expands the attack surface for cybercriminals. In 2016, the Mirai botnet attack, which involved hijacking IoT devices such as cameras and routers, launched one of the largest

distributed denial-of-service (DDoS) attacks ever recorded, demonstrating the need for specific legal frameworks to address IoT-related cyber threats (Antonakakis et al., 2017).

- Quantum computing risks represent a future challenge for cybersecurity. As quantum technologies develop, they could potentially render current encryption methods obsolete, exposing sensitive data to unprecedented vulnerabilities. The advent of quantum computing could lead to the need for entirely new cryptographic methods to safeguard information (Mosca, 2018). This emerging threat underlines the necessity of adapting legal and technical frameworks to mitigate the risks associated with quantum computing.

In conclusion, to effectively address these evolving cyber threats, legal frameworks such as the Budapest Convention must be updated to incorporate broader definitions and coverage. These updates would ensure that international laws remain effective in combating the full spectrum of cybercrimes in today's rapidly changing technological landscape.

Legal and regulatory considerations

Broadening the definitions and coverage of cyber threats has implications for law enforcement, international law, and cybersecurity policies. Legal scholars argue that frameworks such as the Budapest Convention must be updated to effectively address new forms of cybercrime (Wang, 2024). Incorporating these broader definitions into international treaties would enhance cooperation and provide a unified approach to emerging threats. By doing so, nations can ensure that their legal systems remain adaptable and resilient in the face of evolving digital challenges, fostering stronger international collaboration and more effective enforcement measures.

Implications of unaddressed cyber-threats

When cybercrimes are not effectively addressed, the repercussions go beyond harm to individual victims. These challenges compromise global cybersecurity systems and erode public trust in legal frameworks. The inability of legal systems to evolve alongside advancing cyber threats highlights significant barriers to prosecuting these crimes and underscores their broader societal impacts.

Legal challenges in prosecuting cybercrime

Cybercrime operates across and beyond traditional legal jurisdictions, posing significant jurisdictional challenges. For instance, in the *Microsoft Ireland Case* (*United States v. Microsoft Corp., 584 U.S. 2018)*, U.S. authorities sought to compel Microsoft to produce data stored on Irish servers for a criminal investigation. The Supreme Court eventually dismissed the case following the enactment of the CLOUD Act, which sought to resolve such jurisdictional disputes by establishing a framework for cross-border data access. However, this legislation raised concerns about data sovereignty and reciprocity in international law (Mitchell & Mishra, 2019). Digital evidence is inherently volatile and susceptible to alteration, demanding robust collection, preservation, and authentication standards. The case of *United States v. Nosal* illustrates these difficulties (United States v. Nosal). This case dealt with allegations of unauthorized access under the Computer Fraud and Abuse Act (CFAA). The court struggled to define 'unauthorized access' in a way that appropriately aligned with the act's language and technological realities (Mohamed & Abuobied, 2024).

The failure to address cyber threats effectively undermines global cybersecurity. A prominent example is the *WannaCry* ransomware attack in 2017, which affected over 200,000 systems across 150 countries. This attack exploited vulnerabilities in outdated systems, highlighting the lack of international coordination and enforcement in addressing such threats (URL9). Unaddressed cyber threats also erode public trust in legal systems. The *Equifax Data Breach* of 2017 exposed the sensitive information of over 140 million individuals. While Equifax agreed to a settlement exceeding $700 million, the case revealed significant corporate accountability and data protection regulations gaps. This breach weakened public confidence in the ability of legal frameworks to ensure data security (Thomas, 2019). The Equifax breach highlights the urgent need for stronger, more comprehensive data protection laws to hold corporations accountable and protect individuals' sensitive information from exploitation.

Scholarly perspective on legal reform

Scholarly perspectives on legal reform emphasize the need for harmonized international frameworks to address the growing complexities of cybercrime. Brenner argues that inconsistencies in cybersecurity laws undermine collective efforts to combat cybercrime, creating significant enforcement gaps that leave jurisdictions vulnerable to cyber threats. Enhancing existing instruments, such as the Budapest Convention on Cybercrime, is seen as essential for bridging these

gaps and fostering greater international cooperation in the fight against cybercrime (URL10). This paper's view is that addressing these disparities is vital to ensuring a unified and coordinated global response to emerging cyber threats.

In addition, the implications of unaddressed cybercrime underscore the urgent need for legal reform. This reform must include harmonizing international laws, improving evidentiary standards, and fostering greater cooperation among nations to effectively combat cyber threats. Strengthening global legal frameworks is crucial not only for enhancing cybersecurity but also for restoring public trust in legal systems that are increasingly seen as inadequate in addressing the growing scale and sophistication of cybercrime. By enhancing international collaboration and updating laws, countries can better protect individuals and businesses from the damaging effects of cybercrime and ensure long-term resilience in the digital domain.

The need for a comprehensive update of the Budapest Convention

The Budapest Convention on Cybercrime, adopted in 2001, represents the first and most comprehensive international treaty addressing criminal activity online and related electronic evidence. While its framework has proved resilient over two decades, the evolving cyber landscape necessitates significant updates. The following analysis justifies the need for revisions, grounded in legal scholarship, practical challenges, and the Convention's application.

Legal and procedural modernization

The original Budapest Convention on Cybercrime was drafted in an era when the internet primarily functioned as a communication and data exchange tool. While its provisions were designed to be technology-neutral, they are often insufficient to address the complexities of contemporary cyber operations. Scholars such as Susan Brenner and Orin Kerr emphasize the necessity of aligning cybercrime laws with the evolving digital landscape, particularly concerning privacy, freedom of expression, and data sovereignty (Brenner, 2012; Kerr, 2020). These concerns have led to ongoing debates about the adequacy of existing legal frameworks in responding to modern cyber threats. A major challenge associated with the Convention lies in its procedural mechanisms for obtaining and sharing electronic evidence. While functional, these tools can be cumbersome and sometimes clash with domestic data protection laws. For example, the reliance on mutual legal assistance (MLA) requests often results in delays,

rendering the process inefficient when dealing with time-sensitive digital evidence (URL11). In response to such inefficiencies, the Second Additional Protocol to the Convention seeks to enhance cross-border cooperation by facilitating direct engagement with service providers and expediting access to stored data.

However, jurisdictional ambiguities remain a critical issue, as demonstrated in the Microsoft Ireland case. In this case, U.S. authorities sought access to customer emails stored on an Irish server, prompting legal disputes over extraterritorial data access (United States v. Microsoft Corp., 2018). This case highlights the pressing need for clear and harmonized legal provisions for handling cross-border data requests. The General Data Protection Regulation (GDPR) in the European Union further complicates the issue, as it imposes strict limitations on the transfer of personal data outside the EU, often leading to conflicts with foreign investigative requests (URL12).

Several EU countries have attempted to address these challenges through national legislation. For instance, Germany's Network Enforcement Act (NetzDG) mandates social media platforms to remove unlawful content swiftly, thereby indirectly influencing the collection and preservation of electronic evidence (URL13). Meanwhile, France has established specialized cybercrime units to ensure rapid response to digital offenses, although such efforts still require harmonization with broader international legal standards (URL14). From a researcher's perspective, while the Second Additional Protocol introduces improvements, it does not entirely resolve the conflicts between sovereignty, data protection, and law enforcement efficiency. The complexity of multinational data flows necessitates a more comprehensive framework that balances investigative needs with fundamental rights. A potential solution could involve an enhanced multi-stakeholder approach, integrating service providers, legal experts, and policymakers to develop clearer and more effective cross-border data-sharing mechanisms (Koops, 2021).

In conclusion, while the Budapest Convention remains a cornerstone of international cybercrime regulation, its procedural tools require continual adaptation to keep pace with technological advancements and legal complexities. The ongoing jurisdictional challenges and the need for more streamlined mechanisms highlight the necessity of further legal refinement to ensure both efficiency and compliance with fundamental rights protections.

Harmonization and expansion of membership

Though widely adopted, the Convention remains geographically imbalanced, with limited participation from countries in the Global South. This asymmetry

creates enforcement gaps, enabling cybercriminals to take advantage of jurisdictions not covered by the Convention. Expanding the Convention's influence requires harmonizing its provisions with regional treaties such as the Malabo Convention in Africa or the ASEAN framework on cybercrime (URL15). As cybercrimes transcend borders, a unified legal framework that respects diverse legal traditions is critical. Scholars like Andrea Bertolini argue for a hybrid approach incorporating regional best practices while maintaining the Convention's foundational principles (Bertolini, 2019). This approach increases legitimacy and ensures broader compliance. This paper argues that while the Second Additional Protocol introduces significant improvements, it does not fully address the persistent tensions between state sovereignty, data protection laws, and law enforcement efficiency. The intricate nature of multinational data exchanges demands a more robust and well-defined framework that reconciles investigative imperatives with fundamental rights. A viable solution could involve a strengthened multi-stakeholder approach that brings together service providers, legal scholars, and policymakers to develop more transparent and effective mechanisms for cross-border data sharing (Koops, 2021). Such an approach would enhance international cooperation while ensuring compliance with both national and international legal standards.

Balancing law enforcement with privacy

The balance between law enforcement objectives and individual privacy rights is a cornerstone of the Budapest Convention. However, advancements in encryption and data anonymization challenge traditional investigative techniques. Critics argue that unchecked law enforcement powers risk undermining fundamental human rights, especially in countries with weaker democratic safeguards. The Second Additional Protocol introduces measures to protect privacy, such as mandatory data protection principles and independent oversight of cross-border data access requests. While these provisions are a step forward, further refinement is necessary to address emerging challenges, such as using automated decision-making systems in cyber investigations (Horan & Saiedian, 2021). The Budapest Convention has been a pioneering framework in the fight against cybercrime. However, it must evolve to address the modern digital age's legal, technical, and procedural complexities to remain relevant. By incorporating the lessons of two decades, embracing technological advancements, and fostering global collaboration, the Convention can continue to serve as a robust tool for international justice and cybersecurity.

Updating the Budapest Convention: Key lessons and recommendations for addressing emerging cybercrime challenges

The rapid development of technology has brought about a corresponding surge in cybercrime, posing significant challenges to legal frameworks worldwide. The Budapest Convention on Cybercrime, as the first international treaty to address cybercrime, has provided a vital foundation for international cooperation in combating these threats. However, in the context of evolving cybercrime tactics, new technological innovations, and changing global dynamics, there is an urgent need to update the Convention. This paper explores critical lessons and recommendations for modernizing the Budapest Convention to address emerging cybercrime challenges effectively.

Adapting to new forms of cybercrime

The landscape of cybercrime has significantly evolved since the adoption of the Budapest Convention. Crimes such as ransomware attacks, cyber espionage, and the malicious use of deepfake technology present new challenges for legal systems globally. The Convention must be updated to account for these new forms of cybercrime, ensuring that existing provisions remain relevant. For instance, the advent of artificial intelligence (AI) and machine learning (ML) has introduced new tools for cybercriminals to automate attacks, making it harder to trace perpetrators. As suggested by experts in the field, the Convention should explicitly address these new types of cybercrime, ensuring that relevant definitions, such as 'cyber-attack', 'AI-driven offenses,' and 'digital extortion', are adequately incorporated (Kuzior et al., 2024). The Convention should be updated to include specific provisions addressing emerging cybercrimes, particularly those involving AI and other advanced technologies. It should also guide the classification of new cybercrimes to ensure that national laws are appropriately updated.

Digital evidence and privacy protection

One of the central tenets of modern cybercrime investigations is digital evidence. As the volume of data generated daily increases, so does the reliance on digital evidence in criminal investigations. However, this rise in digital evidence comes with significant privacy concerns, particularly in an era of heightened surveillance and data collection. A comprehensive analysis of the Convention reveals that it needs more detailed provisions to balance the need for evidence collection

with the protection of individual privacy (Anderson, 2021). The Council of Europe has previously emphasized the need for a balanced cybersecurity and human rights protection approach (URL16). However, the current provisions under the Convention do not address privacy issues concerning electronic evidence, especially when it involves cross-border data transfers and surveillance. The updated Convention should offer more explicit guidelines on digital evidence collection, preservation, and admissibility, including clear safeguards to ensure the protection of individual privacy. This could include establishing data protection protocols and a clear framework for managing cross-border data requests.

Addressing cryptocurrency and blockchain-related Cybercrime

Cryptocurrencies and blockchain technology have revolutionized the financial sector and introduced new opportunities for cybercriminals. These technologies often facilitate crimes such as money laundering, fraud, and ransomware payments. While the Budapest Convention addresses some aspects of digital evidence, it must provide more guidance on combating crimes involving cryptocurrencies or blockchain technology (Morse, 2021). The Convention should be updated to explicitly address cybercrimes related to cryptocurrencies and blockchain technology. This includes enhancing provisions for investigating cryptocurrency transactions, identifying cybercriminals who exploit decentralized technologies, and regulating cryptocurrency exchanges.

Strengthening international cooperation

Cybercrimes are inherently transnational, often involving actors from different jurisdictions. Effective prosecution requires robust international cooperation, including streamlined procedures for mutual legal assistance (MLA) and cross-border data sharing. While the Budapest Convention is a critical tool for fostering international collaboration, challenges persist in its application, especially regarding data protection and the complexity of extradition procedures (Rainer, 2020). The updated Convention should introduce provisions to enhance international cooperation, such as establishing more efficient protocols for cross-border data exchange and mutual legal assistance. This can be achieved through standardized forms of digital evidence submission, reduced bureaucratic delays, and the creation of an international cybercrime task force to facilitate coordination among member states.

Ensuring human rights compliance

Balancing law enforcement efforts with the protection of human rights remains a significant challenge in the digital age. Digital surveillance, data mining, and encryption backdoors are often considered necessary tools to combat cybercrime; however, they must not infringe upon fundamental freedoms such as freedom of expression and the right to privacy. Several human rights organizations have raised concerns over the growing use of surveillance technologies without adequate oversight or protections (URL17). Any updates to the Budapest Convention should emphasize the importance of maintaining human rights protections in the context of cybersecurity measures. Specific provisions should be included to ensure that investigative measures, such as surveillance and data collection, are subject to strict judicial oversight and comply with international human rights standards.

Capacity building and training

Many developing countries need more resources, technical expertise, and infrastructure to combat cybercrime effectively (URL18). This disparity creates significant barriers to implementing the provisions of the Budapest Convention. As such, capacity-building efforts are essential to ensuring that all countries can actively participate in combating cybercrime. The updated Convention should include provisions for strengthening the capacity of member states, particularly those in the Global South, through training programs, the provision of resources, and the establishment of regional centers of excellence for cybercrime investigation and prosecution.

Future-proofing the Convention

Technological change is accelerating, and future innovations such as quantum computing, which is expected to dramatically increase computing power and potentially render current encryption methods obsolete, and 5G networks, which offer ultra-fast connectivity and support for billions of interconnected devices, will undoubtedly introduce new challenges in the fight against cybercrime. The Budapest Convention must be adaptable to these changes to remain relevant and effective in the long term. Without proactive updates that anticipate the cybersecurity implications of emerging technologies, the legal framework risks falling behind the rapidly evolving digital landscape. To ensure this, the Convention should incorporate a mechanism for periodic review and adaptive amendment,

ensuring that it can be revised to address new technological developments. This could involve creating an advisory body made up of experts in cybersecurity, law, and technology to provide recommendations for future updates.

Summary of thought

This paper underscores the pressing need to update the Budapest Convention on Cybercrime to address the evolving landscape of cyber threats effectively. It emphasizes the increasing sophistication of cybercrimes, such as ransomware attacks, misuse of cryptocurrencies, AI-driven offenses, vulnerabilities in the Internet of Things (IoT), and the complexities of cross-border jurisdiction. Through a comparative legal research methodology, the paper identifies significant gaps in the current provisions of the Convention, particularly in dealing with advanced cybercrime techniques and the challenges posed by international enforcement.

The research reveals that the Convention, while foundational, is not fully equipped to address the contemporary realities of cyber threats. It highlights the absence of explicit provisions for emerging technologies, such as artificial intelligence, and for regulating cryptocurrency-related crimes. Furthermore, the paper draws attention to the limitations in cross-border cooperation, which hinders effective prosecution and enforcement in the global digital sphere.

The paper proposes concrete updates to the Budapest Convention in response to these challenges. Key recommendations include incorporating provisions to address AI-driven crimes, establishing comprehensive frameworks for cryptocurrency regulation, and enhancing cross-border cooperation mechanisms to streamline international collaboration. These reforms aim to ensure that the Convention remains adaptable and effective in addressing the dynamic and evolving nature of cyber threats.

Ultimately, this paper contributes to the global discourse on cybercrime law, offering actionable insights for policymakers, legal practitioners, and international bodies seeking to update the Budapest Convention. Addressing the identified gaps will the proposed reforms will help to safeguard fundamental rights while strengthening international efforts to respond to cyber threats in a coordinated and rights-respecting manner.

References

AllahRakha, N. (2024). Global perspectives on cybercrime legislation. *Journal of Infrastructure, Policy, and Development, 8*(10), 6007. https://doi.org/10.24294/jipd.v8i10.6007

Anderson, J. (2021). Balancing evidence collection with privacy rights: A comprehensive analysis of the Convention. *Journal of Law and Privacy, 12*(3), 45–67.

Antonakakis, M., April, T., & Bailey, M. (2022). Understanding the Mirai botnet. *Journal of Cybersecurity, 5*(3), 45–56.

Backes, M., Müller, A., & Weber, P. (2019). Cybersecurity in the age of AI and IoT: Legal perspectives and challenges. *Journal of Digital Security Law, 14*(3), 134–150.

Brenner, S. W. (2012). Cybercrime and the law: Challenges, issues, and outcomes. *International Data Privacy Law, 6*(2), 78–102.

Cerezo, A. I., Lopez, J., & Patel, A. (2007). International cooperation to fight transnational cybercrime. In *Digital Forensics and Incident Analysis, 2007. WDFIA 2007. Second International Workshop on* (pp. 1–10). IEEE. https://doi.org/10.1109/WDFIA.2007.4299369

Gardner, A. L. (2020). Law enforcement cooperation. In *Stars with stripes*. Palgrave Macmillan. https://doi.org/10.1007/978-3-030-29966-8_9

Horan, C., & Saiedian, H. (2021). Cybercrime investigation: Landscape, challenges, and future research directions. *Journal of Cybersecurity and Privacy, 1*(4), 580–596. https://doi.org/10.3390/jcp1040029

Koops, B. J. (2021). The trouble with European data protection law. *International Data Privacy Law, 11*(2), 100–115.

Kuzior, A., Tiutiunyk, I., Zielińska, A., & Kelemen, R. (2024). Cybersecurity and cybercrime: Current trends and threats. *Journal of International Studies, 17*(2), 220–239. https://doi.org/10.14254/2071-8330.2024/17-2/12

McCall, A. (2024). *Cybersecurity in the age of AI and IoT: Emerging threats and defense strategies* [Manuscript]. ResearchGate. https://www.researchgate.net/publication/386050391_Cybersecurity_in_the_Age_of_AI_and_IoT_Emerging_Threats_and_Defense_Strategies

Mezei, K., & Krasznay, Cs. (2022). Cybersecurity and cybercrime in Hungary during the COVID-19 pandemic. In K. Chałubińska-Jentkiewicz & I. Hoffman (Eds.), *The role of cybersecurity in the public sphere – The European dimension* (pp. 133–146). Institute for Local Self-Government Maribor.

Mitchell, A. D., & Mishra, N. (2019). Regulating cross-border data flows in a data-driven world: How WTO law can contribute. *Journal of International Economic Law, 22*(3), 387–405. https://doi.org/10.1093/jiel/jgz016

Mohamed, N. N., & Abuobied, B. H. H. (2024). Cybersecurity challenges across sustainable development goals: A comprehensive review. *Sustainable Engineering and Innovation, 6*(1), 57–86. https://doi.org/10.37868/sei.v6i1.id207

Morse, J. (2021). Cryptocurrencies and cybercrime: Challenges for law enforcement. *Emerging Issues in Cybersecurity, 5*(1), 45–67.

Rainer, M. (2020). *International law and data protection*. Global Law Press.

Rehman, H., & Liu, H. (2021). *Proactive cyber defense: Utilizing AI and IoT for early threat detection and cyber risk assessment in future networks* [Manuscript]. ResearchGate. https://www.researchgate.net/publication/384052025_Proactive_Cyber_Defense_Utilizing_AI_and_IoT_for_Early_Threat_Detection_and_Cyber_Risk_Assessment_in_Future_Networks

Taylor, L. (2021). Adapting the Budapest Convention to the digital age: Balancing security and fundamental rights. *Journal of International Cyber Law, 18*(2), 45–67.

Temara, S. (2024). The ransomware epidemic: Recent cybersecurity incidents demystified. *Asian Journal of Advanced Research and Reports, 18*(3), 1–16. https://doi.org/10.9734/ajarr/2024/v18i3610

Thomas, J. (2019). A case study analysis of the Equifax data breach. *Journal of Cybercrime Studies, 8*(2), 134–150.

Wang, X. (2024). Global (re-)framing of cybercrime: An emerging common interest in flux of competing normative powers? *Leiden Journal of International Law*. https://doi.org/10.1017/S0922156524000402

Online Links in the article

URL1: *Briefing paper on the Council of Europe Convention on Cybercrime (Budapest Convention, Treaty No. 185), outlining its scope, objectives, and implementation challenges.* https://statesassembly.je/getmedia/baff60aa-468b-4914-8420-d3fc58f1698d/Research%20-%20Briefing%20Paper%20on%20Council%20of%20Europe%20Convention%20on%20Cybercrime%20-%2031%20October%202018.pdf

URL2: *Annual ENISA report analyzing the evolving cybersecurity threat landscape across the European Union in 2021.* https://www.enisa.europa.eu/publications/enisa-threat-landscape-2021

URL3: *Europol report identifying shared operational, legal, and technical challenges faced by law enforcement in combating cybercrime.* https://www.europol.europa.eu/cms/sites/default/files/documents/Common_Challenges_in_Cybercrime_2024.pdf

URL4: *Scholarly article examining cross-border law enforcement access to data and its implications for security, privacy, and fundamental rights.* https://digitalcommons.wcl.american.edu/facsch_lawrev/1100/

URL5: *Industry blog post discussing key Internet of Things security priorities and recommended actions for organizations in 2024.* https://www.keyfactor.com/blog/three-iot-security-resolutions-to-implement-in-2024/?utm_content=dsa&gad_source=1&gclid=Cj0KCQjwv_m-BhC4ARIsA-IqNeBupo0BZ3FTs4bYPE5ah9Vp4X--3espiOLmQqa-sGc_BHq9SFJ9Q0JgaAjxdEALw_wcB

URL6: *Official CISA overview summarizing lessons learned and policy responses following the Colonial Pipeline ransomware attack.* https://www.cisa.gov/news-events/news/attack-colonial-pipeline-what-weve-learned-what-weve-done-over-past-two-years

URL7: *Analytical overview of key global cybersecurity statistics and trends projected for 2025.* https://www.cobalt.io/blog/top-cybersecurity-statistics-2025

URL8: *Technical analysis of the Kaseya ransomware incident and its impact on global supply chains.* https://www.symantec.com/blogs/attackers/kaseya-ransomware
URL9: *Guest editorial discussing major issues and policy concerns shaping the global cybersecurity environment.* https://libres.uncg.edu/ir/uncg/f/N_Kshetri_Global_2013.pdf
URL10: *Academic paper exploring legal challenges, regulatory issues, and enforcement outcomes related to cybercrime.* https://www.researchgate.net/publication/287743943_Cybercrime_and_the_law_Challenges_issues_and_outcomes
URL11: *Council of Europe overview of key achievements and practical impacts of the Budapest Convention on Cybercrime.* https://www.coe.int/en/web/cybercrime/achievements
URL12: *Official consolidated text of Regulation (EU) 2016/679 setting out the General Data Protection Regulation framework.* https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R0679
URL13: *Official German federal publication of the Network Enforcement Act regulating unlawful content on social networks.* https://www.gesetze-im-internet.de/netzdg/BJNR335210017.html
URL14: *French Ministry of the Interior page presenting judicial and institutional responses to cybercrime.* https://www.interieur.gouv.fr/actualites/actualites-du-ministere/au-coeur-de-lutte-contre-cybercriminalite
URL15: *African Union treaty establishing a continental framework for cybersecurity and personal data protection.* https://au.int/en/treaties/malabo-convention
URL16: *Council of Europe recommendation defining the roles and responsibilities of internet intermediaries.* https://rm.coe.int/0900001680790e14
URL17: *Amnesty International annual report assessing the global state of human rights for 2020/21.* https://www.amnesty.org/en/wp-content/uploads/2021/06/English.pdf
URL18: *World Bank report outlining strategies to strengthen cyber resilience in developing countries.* https://www.worldbank.org/en/results/2025/01/29/-enhancing-cyber-resilience-in-developing-countries

Court Judgments

Microsoft Corporation v. United States, 138 S. Ct.. 1186 (2018). Cross-border jurisdiction and data privacy. *United States Supreme Court Reports, 138*(4), 1186-1199.
United States v. Microsoft Corp., 584 U.S. (2018). Cross-border data access and jurisdictional challenges. *United States Supreme Court Reports, 584* U.S. (2018).
United States v. Nosal, 676 F.3d 854 (9th Cir. 2012). Handling digital evidence: Collection, preservation, and authentication. *United States Court of Appeals for the Ninth Circuit Reports, 676* F.3d 854.

Reference of the article according to APA regulation

Nshimiyimana, F. R. (2026). Adapting the Budapest Convention to address emerging cyber threats. *Belügyi Szemle*, *74*(1), 183–204. https://doi.org/10.38146/BSZ-AJIA.2026.v74.i1.pp183-204

Statements

Conflict of interest

The author has declared no conflict of interest.

Funding

The author did not receive any financial support for researching, writing, and/or publishing this article.

Ethics

No dataset is associated with this article.

Corresponding author

The corresponding author of this article is Francois Regis Nshimiyimana, who can be contacted at regisnshimiye82@gmail.com.