KrimOJ Kriminologie – Das Online-Journal
Criminology – The Online Journal

No. 1/2025

Enver Buçaj & Arsim Thaqi

Global Regulation of Cybercrime through International Law and Cyberconventions

Background: This study examines the necessity of regulating cybercrime through international law and treaties, emphasising the role of the Budapest Convention as a foundational agreement. It explores the perception of global realities of cyberspace, prospects for legislative harmonization, and an international response to the legal status of the problem. The study highlights the urgent need to regulate cybercrime within the framework of international criminal law because of its persuasive threats across the globe. In terms of method, it uses normative legal research, analysing the international legal foundations based on the Budapest Convention and contrasting them with other types of comparative legal reasoning in and outside of the European Union. Technological insight is also looked at with a view to monitoring existing programs and recommending more effective mechanisms to combat cybercrime. Foremost among the findings is the irrefutable need for a legally interned unified world system of legal framework to fight cybercrime. The Budapest Convention serves as a starting point, while the ever-morphing nature of threats justifies the development of newer legal norms through the continuous transformation of reactive law. It discusses the need for uniform definitions of the law, better interaction between the public and private sectors, and better ethical definitions and practices of data collection and dissemination.

Keywords: Convention on Cybercrime and Cooperation, Cyberattack, Cybercrime, International Criminal Law

Globale Regulierung von Cyberkriminalität durch Internationales Recht und Cyber-Konventionen

Hintergrund: In dieser Studie wird die Notwendigkeit einer Regulierung der Cyberkriminalität durch internationales Recht und Verträge untersucht, wobei die Rolle der Budapester Konvention als grundlegendes Abkommen hervorgehoben wird. Sie untersucht die Wahrnehmung globaler Realitäten des Cyberspace, die Aussichten für eine Abstimmung der Gesetze und eine internationale Antwort auf rechtliche Fragen der Thematik. Die vorliegende Studie unterstreicht die Notwendigkeit, Cyberkriminalität im Rahmen des internationalen Strafrechts zu regeln, da sie weltweit eine relevante Bedrohung darstellt. *Methoden*: Es wird eine rechtsnormative Untersuchung durchgeführt, bei der die internationalen Rechtsgrundlagen auf Grundlage der Budapester Konvention analysiert und anderen Arten von rechtsvergleichenden Überlegungen innerhalb und außerhalb der Europäischen Union gegenübergestellt werden. Auch technologische Erkenntnisse werden im Hinblick auf die Überwachung bestehender Programme und die Empfehlung wirksamerer Mechanismen zur Bekämpfung der Internetkriminalität untersucht. *Ergebnis*: An erster Stelle steht die unbestreitbare Notwendigkeit eines rechtlich verankerten, weltweit einheitlichen Rechtsrahmens zur Bekämpfung von Cyberkriminalität. Die Budapester Konvention dient als Grundlage, während die sich ständig verändernde Natur der Bedrohungen die Entwicklung neuer Rechtsnormen durch die kontinuierliche Umgestaltung des reaktiven Rechts rechtfertigt. Es wird erörtert, dass einheitliche Rechtsdefinitionen, eine bessere Interaktion zwischen öffentlichem und

https://doi.org/10.18716/ojs/krimoj/2025.1.9

privatem Sektor sowie bessere ethische Definitionen und Praktiken der Datenerfassung und -weitergabe erforderlich sind

Schlagwörter: Cyberangriff, Cyberkriminalität, internationales Strafrecht, Übereinkommen über Cyberkriminalität und Zusammenarbeit

1. Introduction

Cyber-attacks are an alarming fact of modern life: they provide constant threats to citizens' safety and security in respect to stability for state economic and political systems, democracy, public safety, and normal functioning within states. Today, cybercriminals are far more equipped than those in the course of human history. The technological advancement provided them with enhanced targets for their attacks as well as new technical advancements (Huang et al., 2018). In the years to come, advanced technologies may enable some cybercriminals to instigate political and social unrest on a massive scale-attacks, which could even be chemical, biological, or nuclear. Cybercrime is the intelligent hack mapping by hackers (Levy,1984). They happen to be the best organized and well-equipped members involved in the crime. Considered practically in the cybercrime world, these hackers are heroes (Hollinger,1991). In the annals of the world, the history of internet-based crime (Choi et al.,2020)

Current governance, national strategic planning, food production and distribution, oil and gas pipelines communication, land, sea, and air traffic, all other state activities, rest solely on computer and information technology, and their operations are becoming increasingly computerized. The hypothesis that these institutions will be attacked at one point in time has undergone confirmations by cyber criminals who carry out attacks against sensitive systems and institutions.

The definition of cybercrime is gleaned from the respective fields of study from which it is taken and where it is applied. To be precise, it refers to the execution of any act that disrupts the integrity of an individual's or organizations computer records or systems (Tapia, 2022). Based on the definitions of the Budapest Convention and the U.S. Department of Justice, we offer an all-encompassing definition (Dupont & Whelan, 2021). Basically, cybercrime is any illegal act perpetrated using or in conjunction with a computer, computer network, or other networked devices. It is performed deliberately by persons or groups intending to inflict damage on, unlawfully access, alter, appropriate, or destroy the information or data of a person or entity.

In short, the European Commission acknowledged with no little lack of precision the definition of cybercrime as involving activity related to electronic communication networks and information systems (Koops, 2010). It was agreed upon that cybercrime shall constitute acts committed by electronic communications networks and the information systems, or against such networks and systems (Dumchykov et al., 2022). However, EU confronts some internal problems represented as legal fragmentation, and differences among the member states in terms of efficiency in combating cybercrime (Brandão & Camisão, 2021). Such a universal definition being still non-existent has had an effect on its prevention and quite a significant economic dimension in terms of the sustained perpetration of this crime worldwide (Mphatheni & Maluleke, 2022). International instruments like the United Nations Convention against Corruption are planning to make these activities harmonize the countries. Cyber-attacks have be-

come a part of modern life and a threat to individuals or lands in their national interest. International instruments like the United Nations Conventions against Corruption adopted it (The United States Department of Justice, Equality and Law Reform Annual Report 200 I, 2002). Irrespective of all the collaborative efforts by all the parties to fight cybercrime, either national or international, cyberattacks remain savage, further able to block networks on a considerable scale. The various countries are combating this threat in all regions. Thus, it is imperative to establish such regulations addressing cyber-crime based on international criminal law principles. In recent years, numerous criminal acts have demonstrated that scarce, if any, have faced scrutiny and prosecution on behalf of their acts. The International Criminal Court should investigate, prosecute, and gauge the suspects of such crime (Back et al., 2018). The paper is to input into the debate on global cybercrime regulation by giving an extensive expansion on certain pressing challenges and state solutions that could be jointly implemented through international cooperation and legal harmonization.

The main aim of the study is to explore the current condition of international statutes on cyberinaction by evaluating legislative apparatuses like the Budapest Convention for effectiveness in responding to the very changing nature of cybercrime. It, therefore, seeks to deconstruct and understand the multifaceted challenges underpinned behind combating cybercrime globally, atocentric for the nature of cybercrime in creeping through borderless dimensions and the vastness and diversity of legal systems, hence the complications of multi-layered partnerships due to the dynamics of international collaboration and tacit legal harmonization. Other principles of action include proposing policy and legal measures directed to lengthen continuity and guide on transparency and an observatory focus on fine-tuning any such procedures and jurisdictions towards an enhanced course of action.

The results of the analysis point to two core questions: (1) Is the Budapest Convention effective in establishing a worldwide legal framework for countering cybercrime? (2) What legal and policy measures will enhance international cooperation in cybercrime regulation?

The research has a very good structure; its literature review is wide-ranging and comprises meticulous work with academic research, legal commentaries, and reports from international bodies that analyze the current state of cybercrime and its legal control worldwide. A comparative legal analysis further explains the difference in legal practices among states, justifying the need for harmonization. Besides, the research includes case studies of major incidents of cybercrime that review practical experience and highlight existing gaps and strengths in legal responses. This part of the research includes analysis of polices, formulating recommendations that aim to address the problems mentioned. This suggests the harmonization of legal definitions and standards among various legal systems to achieve a cooperative effort for combating cybercrime. Some of the critical arguments outline how future partnerships between private firms, governments, and ISPs can be analyzed to facilitate a win-win proposition for both private and public interests. It concludes with proper explanations as to how the protection of individual privacy and human rights can be ensured while regulating cybercrime. Finally, the paper provides a synthesis of the main ideas generated throughout the research, providing feedback on the original objectives and assessing the extent to which they have been achieved. The recommended strategies are outlined once again, their relevance noted, and appeal is made for their adoption in international cybercrime regulation. The bibliography contains a detailed list of sources cited, recognizing the numerous contributions of different scholars and practitioners whose works permeate and positively shape 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. Utilizing a normative legal research approach, it effectively dissects and comprehends legal principles, doctrines, and a range of international instruments. This approach is founded upon a thorough investigation of the Convention on Cybercrime (Budapest Convention) and other pertinent international and national legal texts. Such an analysis stretches beyond the simple study of law toward examining the effectiveness of these legal instruments and their wider implications for world crime problems.

The selected case studies come from different jurisdictions which reflect various legislative practices and the global legacy of cybercrime. The cases were compared through various methodologies-including the method used to handle similar incidents across nations-and looked at the practical effect of legislative measures. The analysis of the legal framework focuses on international legal principles and instruments such as the Budapest Convention and the way these norms have been implemented at the National level. In contrast, the examination of practical application looks at different concrete cases of cybercrime and the effectiveness of the enforcement of six existing laws through the use of statistics, reports and practices of law enforcement institutions. This methodological departure will facilitate a deeper understanding of legislative and legal effectiveness in the international fight against cybercrime. Within this context, the present study has a multi-pronged methodological focus, which includes the use of normative legal scholarship and comparative law with special reference to the Budapest Conventions and relevant instruments within European and other global contexts, alongside case studies of real instances of cybercrime incidents that give perspective on the practical effect and gaps in legislation. A literature review, including all of the academic works and reports devoted to the issue, will thus provide for a better grasp. Hence, the study will analyze the impacts induced by cyberattacks, conduct a background analysis, and make strategic recommendations for further international cooperation practices and harmonization of laws in responding to such criminal behavior.

3. Global impacts and multifaceted challenges

Every year, there are other forms of cybercrimes like online shopping and internet banking frauds, and any other different threats met by individual victims, like cyberbullying (Reep-van den Bergh & Junger, 2018). Most of the countries are putting money to curb and punish cybercrime to ensure cost-effective security measures. Security measure prevention needs dependable crime statistics so governments can formulate meaningful measures (Gasket, 2019; Armin et al., 2015). The target audience is mainly youngsters using the Internet; these people are the most victimized by computer viruses. Between them, the younger age group got severely affected during the 2011-12 crime survey for England than the older group (McGuire & Dowling, 2013).

Cybercriminals spread illicit materials through various channels: social media websites, through emails, online forums, and chat rooms. The usage of sizeable channels for one criminal activity poses another unique challenge for law enforcement in iring and pinpointing them as compared to conventional crime. An assortment of hurdles rests along the way, often making

them improbable; in such cases, victims fail to classify themselves as such. It is suggested that the approach of automatically analyzing authorship with a view to identifying the address of a criminal or one giving trouble be used (Zheng et al.,2003).

The increase in cyberbullying is worldwide and links with the increase in Internet access and mobile technology. People from developed and underdeveloped countries alike have used this technology in several fields, from education to business to industry (Smith, 2009). The number of uses since learning has, in turn, become a greater attraction to irresponsible criminals who repeatedly commit offenses. This is a manner of abusing the power and trust by one act in a way meant to insult, ignore, or violate the basic right of somebody. There are several issues with investigating the rising scourge of cyberbullying and taking action against it (Herrero et al., 2021).

International cooperation and the establishment of strong regulations for cybersecurity are therefore essential (Henderson, 2021). Like globally shared spaces such as land, sea, air and outer space, cyberspace also requires a coordinated approach for effective management and protection. The international community recognizes the urgency of the issue of broad agreement set forth with UN support to guaranteeing security and justice in cyberspace. The lack of a comprehensive convention makes it necessary to create a global treaty whereby cyberattacks can be addressed, particularly in the event of different states being the target of coordinated attacks. In this context, the Budapest Convention is, never mind anything else, a platform that permits cooperation on the part of the states in exchanging experiences to form effective mechanisms to deal with cyber emergencies (Peters & Jordan, 2019). However, to gain wider acceptance, the convention would have to increase the number of countries adopting it and improve the implementation mechanisms on an international scale. In the year 2019, Maimon and Louderback (2019) reviewed technology-related cybercrime and, in their research, encountered over 7,427 reported cases of computer-related crimes. This calls for broader work to be done tending toward the strengthening of preventive measures and raising awareness of a growing global threat.

The experience of Australia and New Zealand in developing cybercrime strategies is an important example of a proactive approach. In 2010, these two countries, with ACPO (Pickering, 2010), developed a joint strategy to deal with the challenges of cybercrime (Pickering, 2010). While these initiatives are vital, the isolated initiative is by no means sufficient to address a phenomenon that knows no borders. Therefore, states must strengthen their cooperation, not only through the existing treaties but also through new coordinated mechanisms that can address the continuous dynamism of cyber threats.

4. Cybercrime legislation globally

The dynamic nature of cybercrime, which continuously evolves and uses sophisticated techniques by perpetrators, presents a challenge to global legal frameworks. Compounding this complexity is the diversity in the legal landscapes of different jurisdictions, with each having its own laws, enforcement strategies, and challenges. An in-depth analysis of these jurisdictions and the types of cybercrime ever prevalent is critical in developing proper strategies for global cybersecurity.

The regulation of cybercrime varies considerably across regions, reflecting differences in legislative priorities, development technologies, and perceived threats from cyber activities. For

instance, the countries of the European Union operate under a relatively harmonized legal framework, owing, at least 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). Whereas the countries in other areas with less harmonized systems face challenges in ensuring the consistency of regulation and enforcement in cybercrime (Pickering, 2010; Wicki-Birchler, 2020). A series of case studies indicates the legislative nuances and challenges that different jurisdictions contend with. For instance, in Japan, the Cybercrime Control Law, modified to tackle evolving cyber threats, specifically provides for offenses such as unauthorized access to computers and the creation of malicious software (Holt, 2012). In Brazil, however, the study points out the difficulties the Marco Civil da Internet faces in enforcement against the growing backdrop of digital activity, emphasizing jurisdictional, data retention, and privacy issues (Medeiros & Bygrave, 2015).

Any thorough examination of the approaches to cybercrime lawmaking in Japan and Brazil must take into consideration examples from other jurisdictions, which further exemplify the global challenge of cybercrime. These examples illustrate the varied nature of legal responses and the common challenges of the alignment of national laws with international standards. The United States has put forward a comprehensive range of approaches to cybersecurity in enacting such laws as the Computer Fraud and Abuse Act (CFAA), the leading statute in prosecuting cybercrime for unauthorized access to computers (Mancosu & Vegetti, 2020). The U. S. also actively participates in international efforts to combat cybercrime, thus exemplifying the essential role that international cooperation will play in this regard. Nonetheless, a balancing act remains in contention between security measures and privacy rights; an ongoing debate exemplified by the discussions on data encryption and law enforcement access to digital evidence.

The Information Technology Act of 2000, along with the subsequent amendments by India, offers some views of the approaches the country has adopted towards overcoming cybercrime challenges in the ambit of a rapidly growing digital economy (Nagarathna, 2020). The IT Act set forth a criminological framework for electronic governance, data protection, and dealing with cybercrimes in an arrangement that signifies a good pace with the developments in technology. But enforcement of these laws involves the interplay of various factors, including jurisdictional questions and demands for greater technical know-how among law enforcement personnel.

Data protection laws in Germany are strict, and the country is doing great with its combat against cybercrimes. The Federal Data Protection Act (BDSG), together with GDPR, has high standards for the protection of personal data. The Network Enforcement Act (NetzDG) further highlights Germany's stance on combating online crimes, such as hate speech and misinformation (Schmitz & Berndt,2018). These actions demonstrate a balance sought by Germany between protecting individual rights and national security, one that other countries could envy in their quest of reconciling similar tensions.

The Cybercrime (Prohibition, Prevention, etc.) Act of 2015 is an incredibly significant step toward fighting cybercrime in a fast-digitalized country grappling with diverse forms of cyberspace fraud. The Act includes many offenses, such as cyber fraud, identity theft, and cyberstalking, and exhibits Nigeria's recognition of the economic and social impact of cybercrime. However, issues with enforcement and implementation have remained, exacerbated by limited resources and the need for international cooperation (Kpae, 2020).

Australia's cybersecurity strategy involves collaboration between the government, the private sector, and international partners. The Cybercrime Act 2001 and more recent Critical Infrastructure Security Reforms are among Australia's legislative frameworks to safeguard national interests against cyber threat (Gerald 2023; Soldani,2020). These laws, combined with their active involvement in international treaties and partnerships such as the Budapest Convention, exhibit their commitment to global cybersecurity measures.

Given the ever-changing and increasing sophistication of cybercrime, which presents major challenges across quite disparate legal spectrums, a framework algorithm for the management of international cybercrime investigation is proposed Table 1. This algorithm intends to work through the consequences and difficulties engendered by differing regional laws, enforcement methodologies, and the finer points highlighted by case studies involving Japan, Brazil, the United States, India, Germany, Nigeria, and Australia.

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

Phaze	Steps Completed
Phase 1: Identification and Initial Assessment	1.1 Incident Reporting
	1.2 Initial Assessment
Phase 2: Jurisdiction Determination and Legal Framework Analysis	2.1 Determining Applicable Jurisdictions
	2.2 Analyzing Legal Frameworks
Phase 3: Evidence Preservation and Collection	3.1 Securing Evidence
	3.2 Collecting Evidence
Phase 4: International Cooperation and Application of Legal Instruments	4.1 Using International Instruments
	4.2 Coordination with International Agencies
Phase 5: In-Depth Analysis and Attribution	5.1 Conducting Forensic Analysis
	5.2 Attribution
Phase 6: Preparation and Execution of Legal Actions	6.1 Preparing Legal Documentation
	6.2 Pursuing Legal Actions
Phase 7: Post-Investigation Review and Policy Refinement	7.1 Conducting Review
	7.2 Improving International Policy and Cooperation

The Budapest Convention on Cybercrime, while a cornerstone of the international fight against cybercrime, has to grapple with limitations of its flexibility vis- -vis the rapidly developing technologies and sometimes the differences in levels of commitment shown by member states. This limitation can sometimes have a catastrophic effect on the Convention. The fast-paced developments which are seen in the arena of digital technologies are in itself very rarely matched by the grow-up of the Convention's corresponding rules and regulations, leaving upon sufficient room for opportunistic conduct by cybercriminals to take advantage of regulatory voids and exploit opportunities (Le Nguyen & Golman, 2021). Likewise, while the commitment difference between member states should full-scale implement and enforce provisions identified in the convention, creates inconsistencies in the prosecution and prevention clauses of global cybercrime. These variances in commitment and enforcement can create jurisdictional loopholes that would make it a lot easier for cybercriminals to either operate within or target countries with less stringent cybersecurity measures. Thus, the Budapest Convention as a comprehensive global effort toward fighting cybercrime still falls short of achieving its fullest potential, further

stressing the need for constant revisions of its legal instruments and better cooperation and commitment among all member states.

Table 2: Summary of Steps of the Cybercrime Investigation Algorithm

Phaze	Main Activities
Phase 1: Identification and Assessment	Reporting and initial assessment of cybercrime
Phase 2: Jurisdiction and Legal Framework	Determination of jurisdiction and analysis of relevant legal frameworks
Phase 3: Preservation and Collection of Evidence	Securing and collecting digital evidence, respecting the legal standards involved
Phase 4: International Cooperation	Use of international instruments and coordination with agencies such as INTERPOL and Europol
Phase 5: Forensic Analysis and Attribution	Conducting forensic analysis and attributing criminal acts to individuals/groups
Phase 6: Legal Action	Preparing documentation and pursuing legal actions in relevant jurisdictions
Phase 7: Review and Refinement	Reviewing the process and improving international cooperation policies and mechanisms

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

The legal frameworks and initiatives for countering cybercrime in the EU provide another vital element to map the global context for cybercrime regulation. The EU has positioned itself at the helm of preventing cyber threats through comprehensive legal measures, which have included, notably, the NIS Directive and GDPR (Saqib et al., 2018). While they look to enhance the security of the network and information systems across the EU, on the one hand, and provide personal data protection on the other, the fight against cybercrime in Europe bears with it certain challenges: the different interpretations of the Member States on what is commensurate with the requirements set forth in the directive concerned, demands for quicker sanctions under GDPR that do not hinder cybersecurity measures, etc. Cybercrime in and of itself affects the access to justice in Europe. By such patterns, the access to justice seems to be complicated for individuals and organizations alike. Given the borderless nature of the internet, this very complexity underlines the jurisdictional issues that would either involve determining which laws govern a cybercrime case, how a legal action ought to be pursued in different nations, etc. In addition to the other challenges, this nuance of cross-border legal cooperation and enforcing the judgments in the nature of a cybercrime between the EU member states can be tremendously influenced by the disparity in their laws and procedures in the light of collaboration and expeditious resolution of a case being at stake.

Even though that is the case, digital innovation has the potential to facilitate and transform access to justice in the face of such challenges posed within the European context by cybercrime. The application of digital platforms, online dispute resolution, and the latest advances in forensic technology can drastically reform the course of justice in cybercrime cases. For example, tools for gathering digital evidence and sophisticated cyber forensics may accelerate the

investigative process, allowing prosecuting attorneys to act swiftly and with power against cybercriminals while offering online dispute resolution as an opportunity for victims to seek relief in an expedited and user-friendly manner.

The challenges turn into opportunities for possible improvements in EU justice systems, high tech will serve justice in cyberspace, but there are concerns regarding data protection, privacy, and possible digital divide (Calderoni, 2010). It has been illustrated, particularly in some case studies of the European scenario, such as the cross-border investigation and prosecution of the "Avalanche" network, how complicated and concurrently successful legal responses are to cybercrime. This case showed the effective working of cross-border cooperation within the EU and between EU and non-EU countries, and it put the services of Europol and the European Cybercrime Centre (EC3) into the spotlight. However, it also put into stark focus the need for continuous efforts to streamline the processes of law and for an increased interoperability of justice systems throughout Europe in the fight against cyber-crime (Evans-Brown & Sedefov, 2018).

Adopted in Budapest in 2001, the Budapest Convention on Cybercrime defines a broad international framework for fighting against cybercrime, emphasizing the need to bring about conformity concerning legal definitions and cooperation among the jurisdictions. The first international treaty to specifically target cybercrime, it provides an important legal reference point for criminalization, procedural law, and mechanisms for international cooperation (Council of Europe, Budapest Convention on Cybercrime, ETS No.185). The Convention's provisions, including, but not limited to, Articles 2 on illegal access, on illegal interception in Article 3, and on data interference in Article 4, are crucial in discarding these rules into the domestic laws of European Union member states, aimed at delivering uniformity in the approach to cyber threats (Csonka, 2007).

Besides, Article 25 on mutual assistance and Article 29 on expedited preservation of stored computer data in the Convention highlight important areas for improving the capabilities of EU frameworks for effective cross-border cooperation for cybercrime investigations. These emphasize the call for improved legal mechanisms at the EU level. The argument supports simplicity in processes consistent with the provisions of the Convention for mutual legal assistance and data preservation (Polyzoidou, 2021).

Changing cyber threats posed by encryption and cloud computing warrant attempts to realign the Convention and, correspondingly, EU legislation. In the event that the Convention permits amendments, it would allow legal tools against cybercrime to include developments that reflect changing digital adversities. Alluding to the Budapest Convention enhances the argument for adopting and adapting its standards within the EU, thus reinforcing the call for a unified and powerful legal framework against cybercrime (Wicki-Birchler, 2020). This strategy is in vain with the larger effort on the plane, allowing the EU to better defend its digital realm against the ever-increasing threat of cybercrime.

According to the Cybercrime Convention, which was an important step in the fight against online criminals, it took effect on July 1, 2004 (Imam et al., 2008). The Convention was released for signing on November 23, 2001, in Budapest. This applied to the member states and non-member states that contributed to the Convention. Other struggling non-member states were also allowed to ratify the treaty (Talimonchik, 2020). There was a total of 67 ratifications/accessions, while two signatures were not followed by any ratifications (Council of Europe: Chart of signatures and ratifications of the Treaty 185, Convention on Cybercrime (ETS No. 185, 2022). These were 67 states, either members of the Council of Europe or non-member

countries, that ratified the Convention. In 2013, non-member states were discussed upon which an invitation to the treaty should be offered for five years since its inception. This was the first global agreement dealing with cybercrime and thus it raised concerns and even some amendments.

Created around two decades ago to harmonize legal frameworks and improve international cooperation against cybercrimes including denial-of-service attacks and the emerging threat of viruses, the Budapest Convention is expected to enter into force in many countries (Moore et al., 2006). In all actuality, however, it was drafted before the Internet had grown wildly and the more modern emergence of cloud computing and nearly any communication venue going fully digital (Mirkovic et al., 2004).

6. The Application of International Law in Cyberspace

There isn't a dedicated set of rules or regulations pertaining to International Law in cyberspace. Exceptions to this include the Budapest Convention on Cybercrime and the African Union Convention on Cybersecurity and Personal Data Protection; they prevail differently owing to technology being new and evolving at a breakneck pace. The determination of whether established norms of international law really apply in cyberspace took considerable time.

Numerous governments and international organizations, such as the EU, ASEAN, the Organization of American States, and the G20, acknowledge the applicability of already existing international law to the application of information and communication technologies within national borders. This recognition emphasizes the importance of adhering to pre-existing legal frameworks in the rapidly evolving arena of ICT (Haataja & Akhtar-Khavari, 2018). Further, (Sutter, 2003) speaks volumes on information control in cyberspace, the global nature of those issues, and the need for nut international cooperation and regulation.

Cybercrime currently threatens both developed and developing states; it is being tackled effectively. Cybercrime will thus require concerted action and cooperation engaging more nations than those that have signed the Council of Europe Convention on Cybercrime. This poses a challenge of mammoth proportions. Appealing to the original years of constructing a comprehensive convention from the beginning, it may take years of diplomatic impasses that may end unsuccessfully (Buçaj, 2017). Cyber governance, unlike many other subjects pertaining to international and national concerns, arises from academic institutions and what business-building interests construct over the internet with government funding.

The opinion exists among many that international Law is deficient as concerns standards in cyberspace. However, some countries and entities argue that the already existing International Law is adequate for bringing under its influence the actions of states on this field. On the other hand, many governments and other stakeholders have asserted that the existing framework of laws is in need of revision.

Very recently, efforts undertaken by member states in the area of international law concerning cyberspace and ICT have swiveled noticeably. Besides the original U.N. Group of Governmental Experts, these endeavors now comprise a newly formed Open-Ended Working Group under the UN General Assembly's First Committee, and a separate initiative in the Third Committee for a U.N. Cybercrime Treaty. The dispute remains as to whether the U.N will continue to be a primary hub for shaping any debate about the implications of international law in this field. Regional bodies such as the European Union can be an alternative sometimes, avoiding certain

geopolitical dynamics in the UN discussions. Other, in addition to forthcoming multistakeholder processes, can also assume the role (Hollis, 2021). While there is a widening movement geared toward implementing the principles of digital sovereignty, only a tiny fraction of this is expected to affect the application of International Law regarding nation-state behavior in cyberspace.

Independent expert groups played a very great role in the preparation of the Tallinn Guidelines; thus, the debate regarding the regulation of state cyber activities emerges within the framework of international law. The influence of international legal experts is apparent in three recent declarations from Oxford, providing new angles and insights on 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 address the many challenges and safeguards necessary in the health sector in the face of pandemic calamity and the political processes' complexities during any such crisis (Patel et al., 2022). The analysis of De los Ángeles Flores (2022) on the role of Latino media during the 2020 U.S. presidential election gives insights into the electoral context and external influences.

In the current era when more traditional legal frameworks are unable to keep pace with the global features of cyber interactions, the role of soft law in regulating cyberspace activities inherently bearing international dimensions is growingly important. Soft law, such as guidelines, codes of conduct, best practices, and voluntary standards, offers a flexible approach to governance that adapts itself to a fast-evolving digital landscape. In contrast to complex law, which involves enforceable legal obligations, soft law provides the basis of cooperation and coordination to meet new challenges and technological advancements without formal ratification processes or legislative involvement (Yuliia & Lyudmyla, 2020).

Some of the major advantages of soft law in cyberspace include its potential of filling the gaps existing and highlighted by the limitations of traditional legal systems. Traditional legal regimes invariably encounter jurisdictional challenges and enforcement difficulties when cyber activities overrun borders; soft laws seem capable of creating a framework under which international cooperation can be readily undertaken by providing common attributes and standards that state and non-state actors may hold on a shared and converging digital environment.

An example of the Tallinn Manual, which outlines the international law applicable to cyber warfare and was developed by an international group of scholars and practitioners to highlight soft law's utilities, supports its general conception (Schmitt, 2013). Although not binding in nature, the Manual offers a comprehensive analysis of applying existing international law to cyber conflicts and thus provides states and organizations with a reference point for navigating through the complexities that surround cyber warfare law. The Manual has become quite a dynamic resource in establishing the policy and strategy setting for cyber defense, which, in a greater sense, demonstrates how soft law can supplement traditional legal frameworks for governance over the diverse domain of cyberspace.

Soft law is also decisive in promoting cybersecurity standards and practices across the sectors. The NIST cybersecurity framework in the United States evokes voluntary guidelines that push the operators of critical infrastructures and other key stakeholders to undertake sound cybersecurity practices (Goodwin, 2022). Soft law instruments foster collective cybersecurity resilience, enhancing NIST Framework without stringent regulatory requirements when best practices are recommended in risk management and incident recovery.

7. Conclusions

The paper stresses the pressing need for an overarching framework on cybercrime through international legal instruments and conventions. The paper stresses updating Budapest Convention and other binding legal instruments, international cooperation, and involving as many stakeholders in the battle against the increasing threats posed by cyberspace.

The study enunciated the safe proactive evolution of the legal framework in parallel as per accelerated advances in novel technologies and the evolving ferocity of cyber threats. In the case of cybercrime, being cross-national in nature, it necessitates a unified blame mechanism to seek a unilateral jurisdictional blanketing of law and its definitions. Likewise, this evolution of sophisticated attacks on critical infrastructures indicates the vulnerability of nations and the urgent need for coordinated action. We recommend the public-private sectors work together to facilitate an open dialogue while reaching some negotiated terms outlining exactly how sensitive information will be shared between them. In so doing, it means that there must be some corresponding laws fashioned, not to exclude technological changes.

Our research concludes that the future of possible international lending instruments and cooperation dovetails into a myriad route of counteracting the growing threat of cybercrime. The authors recommended enhanced collaboration between the states, international organizations, and the private sector on prosecuting offenders, preventing threats, promoting public awareness, and establishing credible infrastructures against cybersecurity threats. They will be a great help in securing the ends of cyberspace from evolving cyber threats.

To enhance the worldwide response to cybercrime, integrated and harmonized legal and technical measures are necessary. First, the Budapest Convention needs to be revised to address new challenges such as cloud computing, encryption, and new forms of cybercrime. This should be done according to international technical standards such as ISO/IEC 27001 that are recommended by experts in this area. In parallel, harmonization of definitions and standards between countries would facilitate international cooperation and enhance the efficiency of criminal prosecutions.

Differences between various jurisdictions, such as those between civil law and common law systems, often create hurdles in the implementation of a common legal framework for cybercrime. For instance, in those jurisdictions that have a civil law system, such as most of the countries in the European Union, a well-structured and clearly defined framework for cybercrime is likely to exist. In jurisdictions that have a common law system, such as the United States of America, it is likely that case law will feature prominently and there is likely to be more flexibility. Such differences have got the potential to affect the way cybercrime is dealt with and how evidence gathered from sources is admissible. Therefore, an analysis of these challenges is necessary to prepare recommendations for harmonization of legislation for effective international cooperation. Improvements in mutual legal assistance and extradition mechanisms are also necessary.

This is possible through unified protocols for the preservation and exchange of electronic evidence, in keeping with the Council of Europe Guidelines on Digital Evidence. Active collaboration between governments and ISPs and technology companies is needed to exchange information concerning such cyber threats. There ought to be a commitment toward training for law enforcement and judicial authorities and campaigns about raising awareness towards cy-

bersecurity in order to better prevent and manage these threats. It is equally important to consider establishing research and policy centers to adapt anti-cybercrime strategies continuously in meeting new technological developments.

References

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

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). *Encyclopedia of Cryptography, Security and Privacy*, 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. https://journals.univ-danubius.ro/index.php/juridica/article/view/3882/3949 (2025, 18 March).

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. *The Palgrave handbook of international cybercrime and cyber deviance, 27-43. of Europe: Chart of signatures and ratifications of Treaty 185. Convention on Cybercrime* (ETS No. 185) Status as of 17/09/2022. https://link.springer.com/referenceworkentry/10.1007/978-3-319-78440-3_2

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. *Contemporary Politics, Communication, and the Impact on Democracy* (pp. 186-208). IGI Global. https://www.igi-global.com/chapter/intermedia-agenda-setting-effect-of-latino-television-in-the-2020-us-presidential-election/292690

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

Dutchak, S., Opolska, N., Shchokin, R., Durman, O., & Shevtsiv, M. (2020). International aspects of legal regulation of information relations in the global internet network. *Journal of Legal, Ethical & Regulatory Issues, 23(*3), 1–7. https://doi.org/10.31548/law2020.03.022

Evans-Brown, M. & Sedefov, R. (2018). Responding to new psychoactive substances in the European Union: early warning, risk assessment, and control measures. *New Psychoactive Substances*, 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. *SoutheastCon*, 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. https://doi.org/10.4337/cilj.2018.01.05

Henderson, C. (2021). The United Nations and the regulation of cyber-security. In N. Tsagourias & R. Buchan (Eds.), *Research handbook on international law and cyberspace* (*pp. 582–614)*. Edward Elgar Publishing.

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/briefprimer-oninternational-law-and-cyberspace-pub-84763 , приступљено, 15, 2022.

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, K., Siegel, M., & Madnick, S. (2018) Systematically understanding the cyber attack business: A survey. *ACM Computing Surveys (CSUR), 51*(4), 1-36. https://doi.org/10.1145/3199674

Koops, B. (2010). The internet and its opportunities for cybercrime. *SSRN Electronic Journal, 1*(1). 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*(1). https://doi.org/10.1016/j.clsr.2020.105521

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

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

Gerald, M. A. (2023). Efforts to enhance Australia's cyber security by developing of 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*(1), 191-216. https://doi.org/10.1146/annurev-criminol-032317-092057

Mancosu, M. and 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), 1-11. 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. https://citeseerx.ist.psu.edu/document?repid=rep1&type=pdf&doi=5e089b9bac3cdba577724cf0cd23f648a4f952d9 (2025, 18 March).

Medeiros, F. A. & Bygrave, L. A. (2015). Brazil's Marco civil da internet: does it live up to the hype?. *Computer Law &Amp; 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 (Radia Perlman Computer Networking and Security)*. 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/10.1080/21645515.2021.2002083

Mphatheni, M. and Maluleke, W. (2022). Cybersecurity as a response to combating cybercrime: Demystifying the prevailing threats and offering recommendations to the African regions. *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), 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 the Cybercrime: Thoughts Based on the Second Additional Protocol (Draft) to the Budapest Convention on Cybercrime. EU Internet Law in the Digital Single Market*. https://doi.org/10.1007/978-3-030-69583-5_15

Peters, A., & Jordan, A. (2019). Countering the cyber enforcement gap: Strengthening global capacity on cybercrime. *Journal of National Security Law & Policy, 10*, 487.

Redmond, D. (2002). Report to the Department of Justice, Equality and Law Reform.

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/s40163-018-0079-3

Saqib, N., Germanos, V., Zeng, W., & Maglaras, L. (2018). Mapping of the Security Requirements of GDPR and NISD. EAI Endorsed Trans. *Security Safety, 7*(24). 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*. 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*? SSRN. 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/10.1080/1360086032000174351

Talimonchik, V. P. (2019). Legal aspects of international information security. In *Security and Privacy From a Legal, Ethical, and Technical Perspective*. IntechOpen.

Tapia, J. (2022). *The Budapest convention on cybercrime*. https://doi.org/10.13140/rg.2.2.12758.32323

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

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.

Kontakt | Contact

Enver Buçaj | University Ukshin Hoti, Prizren | enver.buqaj@uni-prizren.com

Arsim Thaqi | University Ukshin Hoti, Prizren | arsim.thaqi@uni-prizren.com