A Critical Review of The Jordanian Legal Frameworks on International Cooperation in Combating Cybercrime

Huthaifa Albustanji [1], Paulovics Anita [2]

[1, 2] University of Miskolc, Hungary

[1] **bustanjiii@yahoo.com**

Abstract

Jordan has seen a significant rise in cybercrime over the past decade, highlighting the need for stronger international cooperation. This study aims to strengthen Jordanian authorities' efforts to adhere to the most prominent international conventions on cybercrime, particularly the Budapest Convention. Using a disciplinary normative approach, the study examines Jordan's current legal frameworks, identifying gaps in jurisdiction, extradition, mutual legal assistance, and cross-border digital evidence handling. The analysis reveals that Jordan's reliance on the Arab Convention on Combating Information Technology Crime, enacted in 2010, is inadequate due to the evolving nature of cybercrimes. Despite efforts to foster regional and global collaboration, Jordan's non-participation in the Budapest Convention limits its effectiveness. The study concludes that aligning Jordan's legal framework with international conventions (e.g., the Budapest Convention) and strengthening national legislation are crucial for combating cybercrime.

Keywords: Cybercrime; International Law; UN Convention; Cybersecurity; Budapest Convention.

Received: 23/01/2025 **Revised: 31/03/2025** **Accepted: 16/04/2025**

مراجعة نقدية للأطر القانونية الأردنية في مجال التعاون الدولي لمكافحة الجرائم الإلكترونية

حذيفة البوستنجي [1]، بولوفيتش أنيتا [2]

[2،1] جامعة ميسكولك، المجر

bustanjiii@yahoo.com [1]

الملخص:

شهد الأردن زيادة كبيرة في الجرائم الإلكترونية خلال العقد الماضي، مما يبرز الحاجة إلى تعزيز التعاون الدولي لمكافحة الجرائم الإلكترونية التي تتجاوز الحدود الوطنية والإقليمية. لذا، تهدف هذه الدراسة إلى تعزيز جهود السلطات الأردنية في التزامها بأهم الاتفاقيات الدولية المتعلقة بالجرائم الإلكترونية، وبشكل خاص اتفاقية بودابست. تتبنى الدراسة المنهج المعياري لاستعراض الأطر القانونية المتعلقة بمكافحة الجرائم الإلكترونية في الأردن، مع تحديد الفجوات في مجالات الاختصاص، والتسليم، والمساعدة القانونية المتبادلة، والتعامل مع الأدلة الرقمية عبر الحدود. تبين الدراسة أن اعتماد الأردن على اتفاقية مكافحة جرائم تكنولوجيا المعلومات العربية، التي تم إقرارها في عام 2010، أصبح غير كافٍ بسبب تطور أساليب الجرائم الإلكترونية. وعلى الرغم من الجهود المبذولة لتعزيز التعاون الإقليمي والدولي، إلا أن عدم انضمام الأردن إلى اتفاقية بودابست يحد من فعاليته. لذا خلصت الدراسة إلى أن مواءمة الإطار القانوني الأردني مع الاتفاقيات الدولية، مثل اتفاقية بودابست، وتعزيز التشريعات الوطنية أمران حاسمان لتحسين قدرة الأردن على مكافحة الجرائم الإلكترونية

الكلمات المفتاحية: الجرائم الإلكترونية؛ القانون الدولي؛ الأردن؛ اتفاقية الأمم المتحدة؛ الأمن السيبراني؛ اتفاقية بودابست

1. Introduction

In the twenty-first century, the world has seen a huge increase in cybercriminal acts, whether they target nations, individuals, or information systems. Despite advanced measures being taken by many states to combat cybercrime, the recurrence of cybercrime violations has risen in the second decade of the century. As a result, these crimes have become cross-continent issues, no longer restricted by geographical boundaries. Therefore, they are considered one of the biggest concerns for the global economy and security systems (Sviatun et al., 2021, p. 751).

Amid the rise of these unconventional crimes, many states around the world have realized the urgent necessity of establishing adequate regional and international collaboration to fight this cross-border phenomenon by forming agreements and harmonizing both substantive and procedural cybercrime legislation across different states to enable swift and efficient international cooperation in this area.

In light of these international concerns, with Jordan being no exception, the Jordanian government decided to engage in regional consultations to enact harmonized regional cybercrime rules in the Arab region in 2010. These efforts resulted in the enactment of the Arab Convention on Combating Information Technology Crime, which serves as a foundation for regional collaboration in combating cybercrimes across Arab countries (League of Arab States, 2010).

It is clear that since Jordan signed the Arab Convention on Combating Information Technology Crime, the authorities have primarily focused on regional collaboration, leading to a noticeable pause in pursuing further international agreements aimed at broader collaboration in cybercrime prevention. This focus has, for now, limited Jordan's engagement in broader international cybercrime agreements, such as the Budapest Convention on Cybercrime (Council of Europe ,2001). This limited scope raises critical questions about the adequacy of Jordan's current strategy in facing cross-border cyber threats that increasingly demand international, not just regional, responses. Therefore, the central question of this study is: Does Jordan's exclusive reliance on the Arab Convention on Combating Information Technology Crime adequately strengthen its ability to prevent and effectively respond to cross-border cyberattacks? The sub question of the study is : How can Jordan's accession to the Budapest Convention strengthen its legal response to cyber threats?

The study examines the problem embodied in the weakness of Jordan's efforts in combating cybercrime due to its limited engagement in international legal frameworks and overreliance on regional collaboration. Despite its regional cooperation efforts, Jordan's legal frameworks are not adequately aligned with international standards on cybercrime cooperation. In this context, the study aims to assess the extent to which alignment with broader international instruments,

such as the Budapest Convention, could strengthen Jordan's legal and operational response to cybercrime.

The significance of this study lies in its effort to shed light on the challenges that Jordan faces when limiting itself to regional mechanisms for combating cybercrime in an era where cyber threats are inherently global. By critically analyzing Jordan's current engagement under the Arab Convention, the study highlights the limitations of regional-only approaches and underscores the need for broader international cooperation. The findings are especially relevant for legislators, policymakers, and international partners, as they provide a clearer understanding of the potential benefits of broader legal harmonization and participation in global cybercrime conventions, such as the Budapest Convention.

2. Literature Review

The increasing reliance on digital infrastructure for commerce, communication, and governance has elevated cybercrime into a serious global legal challenge. As criminal activities transcend national borders, traditional legal frameworks struggle to address the jurisdictional and evidentiary complexities of cybercrime (Nuroni, Sumartono, Darmawan, Asykur, & Koynja, 2024, p.200).

In response, a number of multilateral and regional conventions have emerged, most notably the Budapest Convention on Cybercrime (2001), the Arab Convention on Combating Information Technology Crimes (2010), and the ongoing negotiations surrounding the United Nations Draft Convention on Cybercrime. These instruments vary in their legal philosophy, scope of cooperation, and treatment of sovereignty, leading to active academic debate about their effectiveness and compatibility with domestic legal systems.

Jordan, while not yet a party to the Budapest Convention, has actively developed its domestic cybercrime framework and engaged in regional and bilateral cooperation mechanisms. However, the literature assessing Jordan's position within this international legal landscape remains limited, particularly in terms of critical doctrinal analysis and comparative legal evaluation. A study titled International and National Efforts to Protect Cyber Security: Jordan Case Study provides a general overview of the Jordanian Cybersecurity Law of 2019 (Al-Kasassbeh, Abu Ghazleh, Kareem, & Breizat, 2023). However, it does not delve into specific elements of international cooperation, such as jurisdiction, mutual legal assistance, or engagement with various international conventions.

A central legal issue in cybercrime regulation is jurisdiction—how states assert authority over offences committed across digital borders. Jordan made a key procedural reform with the 2006

amendment to Article 5 of its Criminal Procedure Law, allowing courts to claim jurisdiction over cybercrimes committed abroad if they produce effects in the Kingdom or harm Jordanian citizens (Jordanian Criminal Procedure Law No. 9 of 1961). This provision aligns partially with the effects doctrine, which are debated in international legal scholarship (Razmetaeva, Ponomarova, & Bylya

Sabadash, 2021, p.175). In contrast, the Budapest Convention offers multiple jurisdictional bases under Article 22, including territoriality, nationality, and the location of the offence's effects (Council of Europe, 2001, article 22). Critics argue that such broad jurisdiction may invite legal overreach and create tension between cooperating states. Meanwhile, the Arab Convention offers less detailed guidance on jurisdiction, often deferring to domestic laws, which may limit its practical enforceability. (League of Arab States, 2010).

For the purpose of enhancing international collaboration in cybersecurity, especially in the context of Mutual legal Assistance, Jordan signed a cooperation agreement with Tunisia to bolster cybersecurity measures between the two nations. Further, it entered into a Memorandum of Understanding (MoU) with the United Kingdom to advance cybersecurity frameworks and practices 2019. Additionally, Jordan became a member of the International Telecommunication Union (ITU) has actively in initiatives such as CyberSouth, in partnership with the European Union, further strengthening its global cybersecurity presence (National Cyber Security Center, 2025). In 2019, Jordan reinforced the efforts for combating cybercrimes by strengthening its cybersecurity measures. To this end, the government established the Jordanian National Cybersecurity Center, which is responsible for regulating cybersecurity operations and promoting collaboration at both the national and international levels.

Despite these efforts, the increasing success of cyberattacks shows that the international strategy has not achieved its intended goals. The Jordan Anti-Cyber Crime Unit of the Public Security Department reported 1,039 cybercrime cases in 2012. By 2014, this number had risen to 1,865, and by 2022, it had surged to 16,027. These crimes were categorized as follows: 1,285 cases of cyber-blackmail, 3,769 cases of cyber defamation, 1,000 cases of data theft, 2,115 cases of hacking, 16 cases of cyber theft, and 3,466 cases of cyber threats (Maghaireh, 2024, p.17).

Furthermore, the Jordanian National Cybersecurity Center regularly issues four security reports per year, detailing the state of cybersecurity and cyberattacks in the country. The latest reports for 2023 and 2024 clarified that more than 55% of cyberattacks aim to commit cybercrimes, around 15% are related to hacktivism, and about 30% involve cyberespionage (National Cyber Security Center, 2025). It is evident that cybercrimes represent the most significant cyber risk to the country, surpassing other threats. However, neither the Cybersecurity Center nor the Anti Cybercrime Unit specifies the percentage of cybercrimes targeting the country or its citizens

from outside its borders. Global reports estimate that cross-border cyberattacks outnumber national ones (World Economic Forum, 2024). Therefore, cybersecurity threats are mostly cross-border in nature.

In 2019, experts conducted an interdisciplinary review of cybercrimes, a category that included some of the 7,427 computer-related crimes reported, indicating that cross-border cybercrimes are evolving rapidly and may double within a few years (Buçaj & Idrizaj, 2024, p. 3). Although Jordan is considered more technologically advanced compared to its neighboring countries, it is expected that cross-border cybercrimes targeting the country and its citizens will pose one of the most significant challenges in the future.

To this extent, the wide array of advanced cybercrimes that cross continents highlights the need for enhancing international collaboration in combating cybercrimes in the Arab region. Therefore, Morocco signed and ratified the Budapest Convention on Cybercrime in 2018 (Council of Europe, 2018), despite having already signed the Arab Convention on Combating Information Technology Crime (League of Arab States, 2010). Furthermore, in 2021, Morocco signed the Second Additional Protocol to the Budapest Convention (Hespress English, 2022). The convention and its protocol establish international legal standards for dealing with cybercrime and facilitate cooperation between member states on issues such as electronic evidence gathering and mutual legal assistance.

Unlike Morocco, no other Arab state has signed the Budapest Convention, even though it is the first binding multilateral treaty designed to regulate cybercrime. It is widely recognized as the most effective framework for harmonizing cybercrime laws not only regionally but also globally. Consequently, it is considered one of the most significant international efforts to combat cybercrime (Clough, 2014, p. 698).

In 2020, experts published a report titled “The Budapest Convention on Cybercrime: Benefits and Impact in Practice.” (Cybercrime Convention Committee, 2020). The report sought to evaluate the treaty’s impact on its member states. Its conclusions were optimistic, highlighting the treaty’s positive impact on national legislation, particularly in improving collaboration between public and private entities to combat cybercrime. Additionally, the report noted that international cooperation in addressing cybercrime had been significantly strengthened (Bejan, 2022, p.6).

Jordan has not ratified or signed the Budapest Convention or its protocols. Instead, international efforts in Jordan have been focused on the Arab Convention on Combating Information Technology Crime, bilateral agreements, and initiatives such as the CyberSouth Initiative (Council of Europe, 2017).

Despite the growing importance of cybercrime regulation, scholarly engagement with the doctrinal implications of Jordan's legislative framework remains underdeveloped. Much of the existing literature offers descriptive accounts of legal developments, critical analysis of cybercrime rules (Al-Zoubi, 2023) rather than critical evaluations of regional treaty implementation. This study seeks to fill that gap by offering a comparative legal analysis of Jordan's cybercrime approach within the frameworks of the Budapest Convention, the Arab Convention, and the UN Draft Convention. This analysis highlights the unique challenges and opportunities facing Jordan as it navigates the intersection of domestic laws and international treaties. Ultimately, it provides practical insights for policymakers and legal scholars interested in enhancing the global response to cybercrime in the Arab world.

3. Research Method

This study adopts a normative comparative legal research methodology to examine Jordan's role in international cooperation to combat cybercrime. The normative method focuses on the analysis and evaluation of legal rules, principles, and standards embedded within international and regional legal frameworks. It allows for a thorough examination of the legal content and its applicability to real-world issues, particularly in the field of cybercrime.

By incorporating a comparative approach, the research explores and contrasts three major legal instruments: the Arab Convention on Combating Information Technology Offences, the Budapest Convention on Cybercrime, and the United Nations Convention against Transnational Organized Crime.

This comparison is designed to assess the degree of alignment and divergence between regional and international legal frameworks. It also evaluates how these differences influence Jordan's legislative efforts and its engagement in cross-border legal cooperation. The rationale behind selecting these specific conventions lies in their relevance to Jordan's legal obligations and the challenges of harmonizing domestic laws with multiple international and regional standards. The comparative analysis helps highlight both areas of compliance and opportunities for legal reform.

The study relies on both primary and secondary data sources. Primary sources include the full texts of the selected international and regional conventions, along with relevant Jordanian legislation. These legal documents provide the foundation for normative analysis. Secondary sources—such as scholarly journal articles, academic books, institutional reports, and credible online resources—

offer valuable insights into the practical implementation of these legal instruments and present broader perspectives on international cooperation in combating cybercrime

4. Discussions and Results

While the Jordanian authorities have undertaken various bilateral and multilateral efforts to combat cybercrime, there is a growing need to develop a more comprehensive framework for international collaboration on this issue. This can be achieved by examining the implementation of international cooperation standards as outlined in the Arab Convention on Combating Information Technology Crime, the Budapest Convention on Cybercrime, and the United Nations Draft Convention on Cybercrime.

4.1 Scope of Application

The Arab Convention on Combating Information Technology Crime, as a regional collaboration agreement, is limited in scope to 22 Arab countries. Only four countries—Lebanon, Somalia, Comoros, and Mauritania —have not signed the convention due to political and security-related reasons (League of Arab States, 2010). In contrast, the Budapest Convention has emerged as one of the most significant international initiatives in combating cybercrime. It currently includes 76 member states, with an additional 20 states having either signed or been invited to accede (Council of Europe, 2001).

As for the United Nations Draft Convention on Cybercrime, if enacted, it will be open to all 193 UN member states, thus ensuring broad participation (United Nations, 2024). However, despite its wide potential reach, the UN Convention is not legally binding, as it lacks compulsory enforcement mechanisms. While it plays an important role in promoting the harmonization of international

cooperation efforts (Mittal & Sharma, 2017, p.1372), it also grants states the flexibility to amend their national legislation. This flexibility may create barriers and significant challenges to effective collaboration among UN member states in combating cybercrime.

In this context, joining the Budapest Convention represents the most effective path toward achieving broad and binding international collaboration in the prevention of cybercrime, given its enforceable nature and extensive global membership. In contrast, reliance on regional agreements such as the Arab Convention limits cooperation to a narrow regional scope. Similarly, non-binding frameworks like the UN Convention leave room for political and self-interest considerations to undermine effective international cooperation.

4.2 Mutual Legal Assistance

Mutual legal assistance is crucial in international collaboration to prevent potential violations

of another state's sovereignty. Additionally, it ensures due process, safeguards individual rights such as privacy and protection from self-incrimination, and fosters trust through reciprocity (Osula, 2015, p. 9). Bilateral or international agreements with other states can effectively facilitate the provision of such assistance.

In this context, the scope, urgency, and practicality of mutual assistance under the UN and Budapest Conventions, compared to the Arab Convention, differ significantly. Both the Budapest and UN Conventions establish broad procedural frameworks for mutual legal assistance in cybercrime cases that are applicable to all member states. However, they also provide a flexible approach by allowing urgent requests to be sent directly between judicial authorities, with a copy forwarded to central authorities and, if necessary, transmitted through Interpol. While this approach allows for swifter processing of requests, its practical implementation can be challenging due to variations in national legal systems (Council of Europe, 2001, article 27).

In contrast, the Arab Convention offers a more structured and regionally tailored procedure. It emphasizes direct communication between central authorities within the Arab region and supports faster response times through clearly defined emergency protocols. The practicality of this approach is enhanced by shared legal traditions and cultural similarities among member states

(League Arab States, 2010, article 34).

The Budapest Convention, however, presents clear advantages in the area of mutual legal assistance. It introduced a dedicated mechanism to facilitate international cooperation in cybercrime cases: the establishment of a 24/7 Network of Contact Points(Council of Europe, 2001, article 35). This network enables countries to respond rapidly to cybercrime incidents by ensuring direct and immediate communication between law enforcement agencies. For instance, if a country detects a ransomware attack originating from another jurisdiction, the 24/7 contact point can promptly alert the relevant country, preserve digital evidence, and coordinate law enforcement actions. This real-time responsiveness gives the Budapest Convention a clear edge over other frameworks, as formal legal assistance procedures in most other conventions tend to be slow and bureaucratic.

Accordingly, Jordan would benefit significantly from joining the Budapest Convention, which offers a more efficient and responsive framework for mutual legal assistance in cybercrime cases. The 24/7 Network of Contact Points ensures swift coordination, which is crucial for addressing

cyber threats in real time. Adopting this mechanism would substantially strengthen Jordan's capacity for cooperation with over 76 member states.

4.3 Cross Border Access stored Data and electronic evidence Collection

Electronic evidence stored in foreign jurisdictions has become a critical component in investigating and prosecuting cybercriminals (Hossain, 2023, p. 143). However, accessing such data across borders presents significant legal, technical, and ethical challenges. To address these issues, cybercrime conventions have established standards for the exchange and access of digital evidence.

The Arab Convention on Combating Information Technology Crime imposes obligations on preserving digital data within national borders. Article 30 of the convention mandates that State Parties adopt procedures enabling competent authorities to issue orders for the expedited custody of digital information, including data used to trace users on information technology systems. Furthermore, according to article 25 of the Convention each State Party must implement procedures that allow authorities to access specific information, such as by compelling individuals to provide data stored on their devices or obligating service providers to disclose user-related data under their control. However, while these measures support domestic data preservation, the Convention's effectiveness is limited to actors within a state's territory. It does not explicitly permit cross-border data access or authorize direct investigative orders to entities outside national jurisdictions.

In contrast, the Second Additional Protocol to the Budapest Convention offers a more comprehensive and practical approach to cross-border access to digital evidence. According to article 7 of the protocol, state parties have direct access to data stored abroad and streamlines the process for obtaining subscriber information, reducing dependency on traditional Mutual Legal Assistance (MLA) mechanisms (Council of Europe, 2022). The protocol also allows competent authorities to issue direct orders to service providers in another jurisdiction for subscriber data, going beyond the domestic scope of the Arab Convention. Moreover, it includes compliance mechanisms, such as penalties for failure to respond to requests and provisions for intergovernmental notification and consultation when necessary (Council of Europe, 2022, articles 12 and14).

While the Second Additional Protocol to the Budapest Convention, aimed at enhancing access to electronic evidence and facilitating international cooperation, has reignited concerns over national sovereignty among several non-signatory states, Article 7 could potentially undermine state control over data flows and legal procedures. These mechanisms may conflict with national privacy laws and constitutional guarantees (Azmi & Shabrina, 2023). Indeed, the protocol must ensure that cooperation mechanisms do not conflict with domestic judicial oversight or expose the country to external political pressures. Thus, this could be a limitation for Jordan's

engagement in the Budapest Convention.

The UN Draft Convention on Cybercrime, by contrast, adopts a more restrictive approach. Its scope is limited to offenses that meet a "serious crime" threshold—defined as offenses punishable by at least four years of imprisonment—thereby excluding lower-level cyber offenses from its e evidence exchange provisions (Digital Watch Observatory, 2024). Furthermore, the UN Convention relies heavily on traditional MLA procedures for sharing digital evidence, which are

typically slower and more cumbersome compared to the streamlined processes outlined in the Budapest Convention's second protocol (Council of Europe, 2022).

Given these differences, it would be strategically beneficial for Jordan to accede to the Budapest Convention and its Second Protocol, thereby enhancing its capacity for international cooperation in cybercrime investigations. This move would allow Jordanian authorities to more efficiently access cross-border digital evidence and reduce dependency on slow and bureaucratic MLA channels. By doing so, Jordan would strengthen its legal and procedural infrastructure to better address the complex and transnational nature of cybercrime.

4.4 Jurisdiction

As cybercrimes can originate in one state and cause harm in another—or even in multiple jurisdictions—a uniform approach to jurisdiction is essential to ensure consistency in legal outcomes across similar cases. In contrast, jurisdictional conflicts and inconsistent judicial approaches can hinder the development of coherent cyber laws and impede effective international cooperation. Recognizing these challenges, the Budapest Convention, Arab Convention, and UN Draft Convention each address the complexities of jurisdiction in cyberspace, seeking to reduce legal fragmentation that could disrupt regional and international cybercrime investigations (Hasan, 2018, p.162).

According to article 30 of the Arab convention (League of Arab States, 2010)) and article 22 of the Budapest Conventions (Council of Europe, 2001), jurisdictional principles rooted in territoriality and nationality, state partiesin both conventions are authorized to exercise jurisdiction over cybercrimes that take place within their national borders, on ships bearing their flag, or aboard aircraft registered under their authority. Additionally, they may claim jurisdiction over offenses committed by their nationals, as long as the act is also considered a crime in the location where it was carried out, or if the crime occurs in territories not governed by any single nation. Notably, the Arab Convention introduces an additional jurisdictional principle, allowing a state to assert jurisdiction if the cybercrime affects a vital interest of that

state. While this expansion enhances flexibility, the term "overriding interest of the state" remains vague and open to broad interpretation.

The UN Draft Convention similarly bases jurisdiction on the principles of territoriality and nationality but expands the criteria further. It grants jurisdiction over offenses committed by stateless persons with habitual residence in the territory of a state party, and uniquely extends jurisdiction to crimes committed against a national of a state party. This contrasts with the Arab and Budapest Conventions, which focus more on the perpetrator's nationality. Furthermore, the UN Convention under article 22 includes jurisdiction over crimes—such as illegal access—intended to be committed within a state party's territory, even if the act originates outside its borders. This introduces intent to commit a crime against the state as a novel basis for jurisdiction

(United Nations, 2024).

When it comes to positive jurisdictional conflicts—situations where multiple states claim jurisdiction over the same offense—each convention takes a different approach. The Budapest Convention under article 27/5 encourages consultations between states to determine the most appropriate forum for prosecution but does not specify whether these discussions should occur before or during the initiation of proceedings (Council of Europe, 2001). This lack of clarity could delay coordination efforts.

This ambiguity in the Budapest Convention's handling of jurisdictional overlaps has drawn criticism, particularly from states outside its framework, who question the Convention's ability to balance coordination with respect for state sovereignty. For instance, Russia and China, argue that to jurisdictional conflicts lacks sufficient respect for national sovereignty in cyberspace because it reflects a Western-centric legal framework. They contend that cyberspace should be treated similarly to sovereign airspace, where states maintain full jurisdiction over digital activity that intersects with their territorial boundaries (Eichensehr, 2015, p.336). From this perspective, engaging in consultations without firm jurisdictional rules, are seen as inadequate and potentially intrusive. Indeed, this perspective reflects geopolitical concerns, particularly the fear that internet governance could be dominated by the EU, alongside apprehensions about the militarization of cyberspace.

In contrast, the UN Convention clarifies in article number 22/5 that if a state party exercising jurisdiction is notified or becomes aware that another state party is conducting an investigation, prosecution, or judicial proceeding regarding the same conduct, the competent authorities of those states must consult to coordinate their actions (United Nations, 2024). This implies that consultation on jurisdiction is to begin only after one state has already exercised its jurisdiction over the crime. This approach in the UN Convention contradicts the principle of fostering international collaboration to combat cybercrime. Such delayed engagement can result in

duplicated efforts and procedural inefficiencies.

Moreover, the Convention has faced criticism for incorporating the passive personality jurisdiction doctrine (United Nations, 2024, article 22/5), which allows a state party to assert jurisdiction over crimes committed abroad against its nationals. In extreme cases, this could enable a State to claim that an individual committed a serious offence against one of its citizens and request extradition, even if the offence occurred outside its territory. Critics argue that this provision could be misused to target political dissidents under the pretext of enforcing cybercrime laws. While some view this inclusion as a drafting oversight, a closer look at the convention's negotiation history tells a different story. During the drafting process, some states pushed for the criminalization of broadly defined cyber activities that raised concerns about freedom of expression and due process (Nguyen, 2025).

The Arab Convention offers a more structured hierarchy for resolving jurisdictional disputes. According to 30/3 of the convention, priority is first given to the state whose security or interests are most affected, followed by the state where the crime occurred, and finally to the nationality of the offender. If competing claims remain, priority is granted to the state that first requested extradition (League of Arab States,2010). While this framework is more rigid and clear than those in the other conventions, the concept of "state interests" is subjective and potentially overbroad, creating opportunities for abuse or overreach. It also fails to sufficiently consider the rights of individuals, which are protected under international human rights law (Zając,2019, p.8).

In reality, rigid adherence to traditional jurisdictional bases—such as territory or nationality—is increasingly insufficient for addressing cybercrime, which transcends physical borders. Jurisdictional claims based on vague notions of state interest or delayed consultations risk undermining efficiency and fairness. Therefore, if Jordan were to accede to the Budapest Convention, it would benefit from a more flexible and cooperative framework for jurisdictional coordination. Although the convention does not provide a strict hierarchy for resolving positive conflicts, it remains more balanced and comprehensive than both the Arab and UN Conventions in navigating the complexities of cybercrime jurisdiction.

4.5 Extradition

Enforcing extradition laws presents a significant challenge when the legal authority of a state is obstructed by the physical absence of the accused, particularly in cybercrime cases where an individual's location may be unknown or obscured by technological means. The inherently transnational nature of cybercrime complicates the enforcement of criminal justice

and necessitates a clear, cooperative extradition framework among states (Sekati, 2022, p. 18).

Both the Arab Convention on Combating Information Technology Crimes and the Budapest Convention on Cybercrime address the issue of extradition. Article 24 of the Budapest Convention and Article 31 of the Arab Convention establish that extradition is permitted for offenses punishable by at least one year of imprisonment under the laws of both parties. These provisions also account for situations in which different minimum penalties may apply under other relevant reciprocal agreements, uniform legislation, or bilateral/multilateral extradition treaties, in which case the standards outlined in those instruments would prevail.

In the context of the Arab region, this study finds that drafting separate and specific extradition provisions within the Arab Convention is unnecessary, as all Arab League member states have already ratified the Riyadh Arab Agreement for Judicial Cooperation (Riyadh Arab Agreement for Judicial Cooperation,1983). Thistreaty contains conditions for extradition that closely mirror those in the Arab Convention. The overlap raises an important question: Which regional convention should take precedence in cases of conflict?

Although the Arab Convention includes a general clause stating that the provision better suited to combating cybercrime shall apply in the event of contradiction with earlier conventions, the mechanism for determining which provision is “better suited” remains vague and lacks procedural clarity. In practice, the Riyadh Convention has proven more effective and frequently utilized for extradition and broader judicial cooperation among Arab states than the Arab Convention on Cybercrime. Nevertheless, the absence of a clear conflict-resolution procedure between overlapping regional agreements continues to pose legal uncertainties.

Conversely, the United Nations Draft Convention on Cybercrime offers a more comprehensive and structured extradition framework. Article 37 not only reinforces the principle of dual criminality but also introduces flexibility for offenses not yet criminalized under the domestic law of the requested state. Importantly, it embeds human rights protections into all stages of the extradition process, including safeguards against politically motivated or discriminatory extradition requests. Furthermore, the Convention under article 37 promotes international cooperation by encouraging consultation prior to denying an extradition request, thereby supporting dialogue and coordination in resolving complex or overlapping jurisdictional and legal issues.

5. Conclusion and Recommendations

The rapid pace of the technological revolution has given rise to unforeseen developments in cybercrimes targeting individuals, states, and critical information systems (Alramamneh

& Abuanzeh, 2023, p.331). These crimes have posed significant challenges to Jordan's infrastructure,

economy, and national security. As cybercrime transcends borders, addressing it effectively requires robust international cooperation.

This study analyzed the frameworks for international cooperation set out in the Arab Convention on Combating Information Technology Crimes, the Budapest Convention on Cybercrime, and the United Nations Draft Convention on Cybercrime, with the aim of identifying the most suitable model to enhance Jordan's role in the global fight against cybercrime. While these conventions seek to harmonize national legal systems and promote collective action, each varies in scope, binding power, and effectiveness (Doneva, 2022, p. 169).

The Arab Convention provides a foundational regional framework but lacks consistency and global outreach, which limits Jordan's capacity to engage with non-Arab states in investigations, intelligence sharing, and joint enforcement efforts. Meanwhile, although the UN Convention addresses several pressing cybercrime issues at the international level, its non-binding nature reduces its enforceability. In contrast, the Budapest Convention stands out as the most effective and practical international instrument due to its binding provisions and comprehensive mechanisms for international cooperation.

Based on the analysis, the study recommends the following to enhance Jordan's capabilities in combating cybercrime:

1-Strengthening International Cooperation

Jordan should accede to the Budapest Convention and its Second Protocol to benefit from tools like the 24/7 Network of Contact Points, enabling faster international coordination. In parallel, Jordan can advocate for the UN Cybercrime Convention to become binding, reinforcing international cooperation and human rights safeguards. A careful assessment is needed to prioritize between overlapping frameworks to ensure alignment with national interests.

2- Advancing Legal and Jurisdictional Reforms

Jordan must revise its legal framework to clearly define jurisdictional authority and enable joint investigations. The laws should also support faster digital evidence exchange. Furthermore, Jordan should promote improvements to the Budapest Convention by supporting the creation of binding mechanisms for resolving jurisdictional conflicts, guided by a competent international body.

3. Building Institutional and Digital Capacity

Creating a national research department on cybercrime would help identify legal gaps and support policy-making. In addition, digitizing MLA procedures would speed up international legal cooperation and reduce bureaucratic delays. These steps would enhance Jordan's ability to manage cyber threats efficiently and align with global best practices.

6. Limits and Future researches

This study has several limitations. It primarily focuses on existing legal frameworks for international collaboration in combating cybercrime as reflected in Jordanian national legislation, as well as in Arab and European regional conventions and United Nations international instruments. However, it does not consider other regional or bilateral agreements, such as the Shanghai Cooperation Organization (SCO) Agreements or the African Union Convention on Cybersecurity and Personal Data Protection (Malabo Convention).

Moreover, since the study centers on Jordan's international collaboration efforts, it does not analyze similar initiatives undertaken by other states, particularly within the Arab region. Given that effective international cooperation requires both regional and global engagement, future research could yield valuable insights by examining the broader efforts of Arab states in combating cybercrime. Such investigations could lead to recommendations for reforming the Arab Convention on Combating Information Technology Crimes, with the aim of fostering more comprehensive and effective regional collaboration.

Additionally, future studies might explore the implications of the UN Convention on Cybercrime for human rights, particularly in developing countries, which often grapple with systemic challenges related to human rights protection. Understanding the convention's impact in these contexts could help balance the need for cybercrime enforcement with the preservation of fundamental rights.

References

Al-Kasassbeh, F. Y., Abu Ghazleh, A. M., Kareem, M. J. M., & Breizat, M. O. (2023). International and national efforts to protect cybersecurity: Jordan case study. International Journal of Cyber Criminology, 17(2), 350–364. https://www.cybercrimejournal.com/

Alramamneh, I. M., & Abuanzeh, A. (2023). International and national procedural framework for combating cybercrime. International Journal of Cyber Criminology, 17(2), 330–349.

Al-Zoubi, M. (2023). Crimes of electronic defamation, libel, and slander under Jordanian cybercrimes law. Al-Majallah Al-Duwaliyya lil-Qanun wa-l-Huquq (The International Journal for Law and Rights), 2(1), 267–284.

Azmi, A. N., & Shabrina, S. (2023). Challenges of universal adoption of the Budapest Convention on Cybercrime. In The 5th International Conference on Technology, Education, and Social Science 1(1), 1-7.

Bejan, E. (2022). Cybersecurity and cybercrime: Challenges of an invisible space. Perspectives of Law and Public Administration, 11(1), 5–10.

Buçaj, E., & Idrizaj, K. (2024). The need for cybercrime regulation on a global scale by international law and cyber convention. Multidisciplinary Reviews, 8(1), 1–10. https://doi.org/10.31893/multirev.2025024

Clough, J. (2014). A world of difference: The Budapest Convention on Cybercrime and the challenges of harmonisation. Monash University Law Review, 40(3), 698–736. https://ssrn.com/abstract=2615789.

Council of Europe. (2001). Convention on Cybercrime (Budapest Convention) (ETS No. 185). https://www.coe.int/en/web/conventions/full-list?module=treaty-detail&treatynum=185 (Last visit 14 April 2025)

Council of Europe. (2017). CyberSouth. https://www.coe.int/en/web/cybercrime/cybersouth. (Last visit 11 April 2025)

Council of Europe. (2018). Morocco joins the Budapest Convention on Cybercrime and its Protocol on Xenophobia and Racism. https://www.coe.int/en/web/cybercrime/t-cy- (Last visit 14 April 2025).

Council of Europe. (2022). The second additional protocol to the Budapest Convention on Cybercrime on enhanced cooperation and disclosure of electronic evidence (ETS No. 224). https://www.coe.int/en/web/cybercrime/second-additional-protocol.

Cybercrime Convention Committee. (2020). The Budapest Convention on Cybercrime: Benefits and impact in practice (T-CY(2020)16). Council of Europe. https://rm.coe.int/t-cy-

2020-16-bc benefits-rep-. (Last visit 14 April 2025).

Digital Watch Observatory. (2024, October 22). Comparative analysis: The Budapest Convention vs the UN Convention Against Cybercrime. Digital Watch Observatory. https://dig.watch/updates/comparative-analysis-the-budapest-convention-vs-the-un-convention against-cybercrime (Last visit 13 April 2025)

Doneva, N. (2022). Cybercrime regulations: Need for a new international approach? Optime, 13(2), 167–180. https://doi.org/10.55312/op.v13i2.377.

Eichensehr, K. (2015). The cyber-law of nations. Georgetown Law Journal, 103(2), 317–352. https://ssrn.com/abstract=2447683.

Hasan, G. M. (2018). Laws on cyber jurisdiction in international perspectives. Dhaka University Studies, Part F, 29, 141-163.

Hossain, B. (2023). Digital evidence in foreign jurisdiction and quality of justice. ELCOP Journal on Human Rights, 1(1), 143-159. https://doi.org/10.59871//SFGB7594.

Hespress English. (2022). Morocco strengthens cybercrime laws to protect citizens and privacy. https://en.hespress.com/106929-morocco-strengthens-cybercrime-laws-to-protect-citizens-and privacy.html (Last visit 13 April 2025)

Jordanian Criminal Procedure Law No. 9 of 1961. (1961). Published in Official Gazette No. 1539 on March 16, 1961, page 311.

League of Arab States. (2010). Arab Convention on Combating Information Technology Crime.DOI:

https://www.asianlaws.org/gcld/cyberlawdb/GCC/Arab%20Convention%20on%20Combating% 20Information%20Technology%20Offences.pdf.

Maghaireh, A. M. (2024). Cybercrime laws in Jordan and freedom of expression: A critical examination of the Electronic Crimes Act 2023. International Journal of Cyber Criminology, 18(1), 15–36.

Mittal, S., & Sharma, P. (2017). A review of the international legal framework to combat cybercrime. International Journal of Advanced Research in Computer Science, 8(5), 1372-1374. https://doi.org/10.2139/ssrn.2978744.

National Cyber Security Center. International cooperation. Available at https://ncsc.jo/Ar/List/intl_cooperation (Last visit at 12 April 2025).

National Cyber Security Center. Security reports. https://ncsc.jo/Ar/List/Reports_AR. (Last visit at 12 April 2025).

Nguyen, T. T. (2025). Addressing the criticisms against the United Nations Convention against Cybercrime. Centre for International Law. https://cil.nus.edu.sg/blogs/addressing-the-criticisms against-the-united-nations-convention-against-cybercrime/ . (Last visit 14 April 2025).

Nuroni, I., Sumartono, E., Darmawan, D., Asykur, M., & Koynja, J. J. (2024). The impact of cybercrime on global security. JOIN: Journal of Social Science, 1(5), 199–214.

Osula, A.-M. (2015). Mutual legal assistance & other mechanisms for accessing extraterritorially located data. Masaryk University Journal of Law and Technology, 9(1), 43–64. https://doi.org/10.5817/MUJLT2015-1-4

Razmetaeva, Y., Ponomarova, H., & Bylya-Sabadash, I. (2021). Jurisdictional issues in the digital age [Cuestiones jurisdiccionales en la era digital]. Revista de Derecho, 10(1), 167–183. https://doi.org/10.31207/ih.v10i1.240

Riyadh Arab Agreement for Judicial Cooperation. (1983). https://www.refworld.org/legal/agreements/las/1983/en/39231. (Last visit 14 April 2025)

Sekati, P. (2022). Assessing the effectiveness of extradition and the enforcement of extra territorial jurisdiction in addressing transnational cybercrimes. Comparative and International Law Journal of Southern Africa, 55(1), 1–36. https://doi.org/10.25159/2522-3062/10476.

Sviatun, O. V., Goncharuk, O. V., Roman, C., Kuzmenko, O., & Kozych, I. V. (2021). Combating cybercrime: Economic and legal aspects. WSEAS Transactions on Business and Economics, 18, 751–762. https://doi.org/10.37394/23207.2021.18.72.

United Nations. (2024). Draft United Nations Convention against Cybercrime. https://www.unodc.org/unodc/en/cybercrime/ad_hoc_committee/ahc_draft_convention.html.

World Economic Forum. (2024). Global cybersecurity outlook 2024. https://www3.weforum.org/docs/WEF_Global_Cybersecurity_Outlook_2024.pdf (Last visit 13 April 2025)

Zając, D. (2019). Criminal jurisdiction over the internet: Jurisdictional links in the cyber era. Cambridge Law Review, IV(ii), 1–28 https://ssrn.com/abstract=3824751.