THE INTERNATIONAL JOURNAL OF HUMANITIES & SOCIAL STUDIES

The Role of International Efforts in Combating Cybercrimes

Hamzah Suleiman Aldoghmi
Assistant Professor, Department of Public Law,
Al al-Bayt University, Jordan

Abstract:
Cybercrimes have become a modern type of crime pattern. They are characterised by the fact that they transcend the borders of states. This led to the direction of the international community to cooperate to confront cybercrimes, as they have a great impact on the national security of states. Therefore, states and international organisations have sought to take joint measures to protect individuals, societies and companies from cybercrimes by concluding international and regional agreements. The most important of these agreements is the Budapest Convention on Combating Cybercrime, the latest of which is the Paris Call for Confidence and Security in Cyberspace. The increase in the use of the internet results in an increase in exposure to the risk of cybercrime. Moreover, the increasing involvement of individuals and organised criminal groups with the internet can harm states, individuals and companies. This invites regional and international organisations to play an important role in concluding international agreements that consolidate international efforts in cybersecurity. However, although there are important international steps in combating cybercrimes, this effort faces several challenges. In addition, the implementation of international agreements approved by states in combating cybercrime is still problematic. Cybercrime is a global challenge, and any effective response requires coordination between the public and private sectors, including law enforcement agencies across many international jurisdictions. This paper discusses the role of international efforts in combating cybercrime in terms of international legal instruments and the role of international organisations in this context. The paper also presents the most important challenges facing the enforcement of these efforts to achieve international co-operation in confronting this type of emerging crime. The paper uses descriptive and interpretive approaches with analytical methods. It concludes with several recommendations for ways to improve international efforts in combating cybercrimes, including the establishment of an international system for responsibility sharing among states to combat cybercrimes.

Keywords: *Cybercrimes, cyber security, international treaty law, international organisations*

1. Introduction

Recently, there have been many aspects driven by technological development. This includes communication through technology and the use of social media between people. Also, buying online has become a phenomenon that many people use. This is also due to the banks' reliance on electronic purchases and the increased lack of reliance on cash. In addition, there is a pattern of transferring money between states, whether because of work, trade, study, tourism or other reasons. All this may result in many problems, most notably cybercrimes. This is because financial crimes increase steadily with the increase in electronic business transactions.

There is a need for states to cooperate in the area of cybercrimes. This need derives from the need for international co-operation and reflects this effort in national laws. This is because cybercrimes are transnational, and no state can protect itself without the help of the international community. States can cooperate in a number of aspects. The first is the signing of international agreements related to cybercrimes. Second, states need to enact laws to combat cybercrimes. Third, states should attach importance to judicial co-operation in the field of cybercrimes.

Although there is an international effort to combat cybercrimes, states face major challenges in doing so. These challenges impede criminal justice, extradition, and compensation for those affected by cybercrimes. Therefore, states need international co-operation to confront this type of crime. These efforts begin by looking at international conventions on cybercrimes, investigating the role of international organisations in combating cybercrimes, as well as reviewing related national laws.

By reviewing previous studies that dealt with international co-operation towards cybercrimes, most of these studies dealt with combating cybercrime from one angle. Therefore, this paper targets the methods of different subjects. However, it flows in one direction: finding legal mechanisms that limit cybercrimes through international co-operation and the reflection of international legal principles in national laws. The paper also differs from previous studies in identifying international efforts with international agreements and organisations. The paper also aims to reflect these international mechanisms in domestic law to protect against cybercrimes as a culmination of international efforts in this context.

1.1. Study Problem

Cybercrimes have become an evolving pattern in states. As an international crime, states alone cannot combat its forms. There is a need, therefore, for international action to address this cybercrime and protect people from its effects. This raises the question: What is the role of international efforts in combating cybercrime? Therefore, this paper will answer the following questions:

- What is the role of international treaty law in the protection from cybercrimes?
- What is the role of international organisations in combating cybercrimes?
- What are the challenges facing states in combating cybercrimes?

1.2. Study Objectives

The study addresses the following objectives:

- Evaluating international efforts in the protection from cybercrimes.
- Identifying international legal mechanisms to combat cybercrimes.
- Establishing an international institutional basis for preventing cybercrimes.
- Ensuring international standards for states to combat cybercrimes.
- Highlighting the challenges that hinder the protection from cybercrimes.

1.3. The Importance of the Study

The importance of this paper lies in building on previous research in addressing international efforts to combat cybercrimes. In addition, the paper clarifies the legal tools and policies agreed upon by states in reducing this type of transnational crime. It sheds light on how states apply the rules of international law related to cybercrimes and enforce them in their national legal systems. The paper also proposes several legal mechanisms and effective policies aimed at reducing the emergence of cybercrimes.

1.4. Literature Review

After the study by Wu (1997), which discussed the linkage between regulating the internet and the international system, there has been various research on international co-operation relating to cybercrimes. This section focuses on studies that examined international efforts to combat cybercrimes. It focuses on the most important and recent studies highlighting protection from cybercrimes. The section presents chronologically previous studies and argues that these studies examined cybercrimes from different points of view. However, they do not highlight the international effort in combating cybercrimes and their impact on national measures aiming to prevent and protect populations from their consequences.

First, Mittal and Sharma (2017) reviewed cyberspace as an aspect under threat from state and non-state actors. They argued that international co-operation is insufficient to protect states from cybercrimes. Their paper suggested that there is a need for an international convention to put forward the legal rules for the protection from cybercrimes. However, their study focused on international conventions and used a theoretical approach in doing so.

Second, Reitano et al. (2015) highlighted initiatives that have been set to enforce international and national law related to cybercrimes. They explained the importance of carrying out tasks to govern administrative and policy frameworks in the protection from cybercrimes. Their paper showed several forms of cybercrimes, highlighting the most heinous crimes, such as online sexual exploitation, identity theft, and vicious botnets. Nevertheless, their study examined how to encourage states to apply measures related to the protection from cybercrimes, focusing on the forms of this transnational crime.

Third, Cerezo et al. (2007) focused on cybercrimes in the context of criminal law. They drew attention to international relations in a set of international guidelines to fight cybercrimes. Their study also discussed many challenges to international co-operation in cybercrime prevention. Therefore, their study is limited to addressing cybercrimes from the point of view of criminal law.

1.5. Study Methodology

The research design for this paper is descriptive and interpretive through qualitative methods. The paper uses an analysis approach for each part. It starts with reviewing the international norms and identifying their legal basis by using descriptive methods. The paper then tests the enforcement of these norms in the national system by analysing challenges facing states. It finally demonstrates its arguments and draws the main findings to put forward recommendations for avoiding the seriousness of cybercrimes.

1.6. Scope and Limitations of the Study

This paper is based on theoretical and conceptual underpinnings. It does not make empirical research nor rely on data. The paper is limited to international instruments and the role of international and regional actors. Thus, national laws are not the focus of its discussions. The paper also examines cybercrimes from the point of view of international law. Therefore, it does not discuss cybercrimes in the context of criminal law or civil law.

2. International and Regional Instruments on Cybercrimes

This section discusses international and regional instruments on cybercrime. These instruments can be divided into two parts.

- First, global instruments to which any state can be a party.
- Second, regional instruments are limited to states in a specific region of the world.

The section argues that international treaty law on cybercrimes is limited in many areas, both in terms of its effectiveness and implementation.

2.1. The Council of Europe's Convention on Cybercrime (2001) and Its Protocol

Also known as the Budapest Convention, this is the first international agreement aimed at reducing computer-related crime by harmonising national laws, improving investigative techniques, and increasing international co-operation. The Committee of Ministers of the Council of Europe adopted the Budapest Convention at its 109th Session on 8 November 2001. It was opened for signature in Budapest on 23 November 2001 and entered into force on 1 July 2004. As of April 2023, 68 states have ratified the convention (Council of Europe, 2023).

The second European instrument was the Additional Protocol to the Convention on Cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems on 28 January 2003. The main reason to issue an amendment to the Convention on Cyber Crime is to integrate provisions on racist and xenophobic expressions through computer systems. However, the protocol is only binding to the signatory states of the protocol itself, which does not include all signatory states to the Convention.

The primary objective of the Convention is to create a 'common criminal policy' to improve the fight against computer crimes around the world by harmonising national laws, improving the capacity of law enforcement and the judicial system, and enhancing international co-operation (Budapest Convention, 2001). The Convention obliges signatories to:

- Define criminal offences and penalties under national law for four types of computer crimes: fraud, counterfeiting, child pornography, copyright infringement, hacking, and security breaches, such as data interception, network integrity, and system interferences.
- Develop national guidelines for the detection, investigation, and prosecution of computer crimes and the collection of electronic evidence for any criminal offence.
- Provide a quick and efficient framework for global co-operation. According to the convention, cybercrimes are extraditable offences, and law enforcement agencies in one nation may gather computer-based evidence on behalf of individuals in another.

2.2. Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse (2007)

The Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse, the Lanzarote Convention, is a multilateral agreement wherein governments consent to make specific types of sexual abuse against minors illegal. It is the first international convention that tackles domestic or family-based child sexual abuse. States that ratify the Convention commit to making sexual conduct with minors under the legal age of consent illegal, regardless of the circumstances; it also makes child prostitution and pornography illegal. The Convention puts forward several steps to stop the exploitation and abuse of children for sexual purposes, such as teaching and training young people, monitoring offenders, and screening and training those who interact with children. According to the Lanzarote Convention, it is illegal to obtain, disseminate, or approach minors for sex using information and computer technology.

2.3. The Arab Convention on Combating Information Technology Offences (2010)

The Arab Convention on Combating Information Technology Offences was enacted in 2010. The Arab Ministers of Interior and Justice approved the Convention in their joint meeting held at the headquarters of the General Secretariat of the League of Arab States in Cairo on 21 December 2010. The agreement entered into force as of the date of deposit of the documents of ratification, acceptance or approval by seven Arab states pursuant to paragraph 3 of the final provisions of the agreement. As of April 2023, all Arab states have signed the Convention (LAS, 2023).

To enhance the co-operation between Arab states, the aim of the Convention is 'to combat information technology offences threatening their security, interests and the safety of their communities' and enable parties to 'adopt a common criminal policy aimed at protecting the Arab society against information technology offences' (ACCITO, 2010). Moreover, the Convention aims to improve co-operation between the Arab States in the area of combating information technology offences to protect the security and interests of the Arab States and the safety of their communities and individuals. The Convention stipulates the offences of information technology, procedural provisions, and mechanisms of legal and judicial co-operation between State Parties.

2.4. The Shanghai Co-operation Organization's Agreement on Co-operation in the Field of International Information Security (2010)

The Shanghai Co-operation Organization adopted the Agreement on Co-operation in the Field of International Information Security on 16 June 2009. The Agreement establishes the institutional and legal framework for the parties' collaboration in global information security (Gastorn, 2017). Its goal is to coordinate and carry out the required cooperative measures to ensure global information security. The Agreement also intends to establish a cooperative monitoring and response system for new threats in this domain. Its main legal objective is to develop cooperative measures for the adoption of international law provisions restricting the proliferation and use of information weapons that endanger public safety, national security, and defence capabilities (Ad Hoc Committee, 2022).

The scope of this agreement went beyond cybercrime and cybersecurity to encompass the information security of member nations as a fundamental goal, as well as national sovereignty over networks and content. The Shanghai Co-operation Organization Agreement defines 'information offences' as 'the use of information resources and (or) the impact on them in the informational sphere for illegal purposes.' (Shanghai Agreement, 2010).

2.5. African Union Convention on Cyber Security and Personal Data Protection (2014)

The Malabo Convention on Cybersecurity and Personal Data Protection, which is a Convention of the African Union, covered several aspects of cybercrime. Despite being enacted on 27 June 2014, it has not yet gone into effect since the necessary number of ratifications has not been reached. Only 13 states had ratified the Convention as of April 2023, whereas Article 36 of the Convention calls for 15 instruments of ratification (AU, 2023).

This Convention includes, *inter alia*, a call to African states to create and/or amend national laws to adequately combat cybercrime, harmonise national laws, create mutual legal assistance treaties (MLATs), facilitate information sharing between states, facilitate regional, intergovernmental, and international co-operation and utilise existing means available to cooperate with other states, and even the private sector. The AU Convention establishes a 'credible framework for cybersecurity in Africa through the organisation of electronic transactions, protection of personal data, promotion of cyber security, e-governance and combatting cybercrime' (CCDCOE, 2023). The three primary topics covered by the Convention are cybersecurity and cybercrime, personal data protection, and electronic transactions.

2.6. The Paris Call for Trust and Security in Cyberspace (2018)

Launched on 12 November 2018 during the Paris Peace Forum, the Paris Call for Trust and Security in Cyberspace seeks to advance efforts on unregulated topics. To this end, it collaborates with a range of stakeholders, including governments, corporations, trade groups, and civil society organisations (Paris Call, 2023). The Call outlines a vision for cyberspace governance and the underpinning key principles. These principles include the applicability of international law, the responsibility of states, the monopoly of the use of violence for lawful purposes, and the acknowledgment of the obligations of the private sector. The Call is the first significant global endeavour that is unwaveringly a component of a multi-stakeholder strategy, including governments, businesses, and civil society groups to combat cybercrimes.

The Paris Call encourages nations to collaborate with academics, civil society, and commercial sector partners, and it extends an invitation to all entities operating in cyberspace to collaborate. The 1,200 signatories to the Paris Call, including 80 nations, over 700 businesses, and 350 civil society groups, pledge to cooperate in promoting ethical behaviour and putting into practice the core values that govern the real world in cyberspace (Paris Call, 2023). It is an appeal for co-operation in the face of emerging dangers that put infrastructure and populations at risk.

3. The Role of International and Regional Organizations

Cybercrimes have been the focus of international actors. Mainly, international and regional organisations play an important role in combating cybercrimes. Their role is to assist in mobilising states around action on issues related to cybercrimes. At the international level, international organisations started their work on cybercrimes by building networks and making treaty law available for states to cooperate. At the regional level, regional organisations have been the main players in the protection against cybercrimes. This section examines the role of international and regional organisations in combating cybercrimes. The section argues that this role has been weak so far due to a lack of legal mechanisms and the nature of decisions and resolutions on the protection from cybercrimes.

3.1. The United Nations

The United Nations' action on the issue of cyber-security has been limited. The United Nations General Assembly has passed several resolutions on cybercrimes. These resolutions have been based on the agenda item: 'Developments in information and telecommunications in the context of international security' (UN, 2023). Nevertheless, several binding and non-binding instruments cover, *inter alia*, issues governing the protection from cybercrime. These instruments include the United Nations Convention against Corruption (UNCAC) 2003, the United Nations Convention against Transnational Organized Crime (UNTOC) 2000, the 2021 GGE (Group of Governmental Experts) and OEWG (Open-ended Working Group) reports, and the IEG (Independent Evaluation Group (IEG)) Recommendations (Ad Hoc Committee, 2022).

For a better understanding of the security implications of developing information technologies, the United Nations organised an international conference of specialists in Geneva in August 1999. In addition, an investigation into global information security concerns was mandated by the resolution. The World Summit on the Information Society was a two-phase event sponsored by the UN in 2003 and 2005, although it produced few tangible outcomes. In addition, as 'an initial step toward building the international framework' for security and stability, government cybersecurity professionals from fifteen countries, including key cyberpower states, such as the United States, China, and Russia, submitted a set of recommendations to the UN Secretary-General in July 2010, marking a significant advancement for the UN (UNGA, 2010).

3.2. The Council of Europe

The Council of Europe has adopted the clearest and most practical strategy to control cybersecurity and cybercrime. The 2001 Council of Europe Convention on Cybercrime, also called the Cybercrime Convention, established the first international convention on crimes perpetrated over the Internet and other computer networks. Its main goals are to safeguard society from cybercrime by means of legislation and collaboration (Council of Europe, 2001). The

Convention is the most sophisticated international legal framework that directly regulates cyberattacks. Its regional membership and inability to control most state-party attacks are its main limitations. Nevertheless, it offers a place to start when creating an all-encompassing global framework to control unlawful cyberattacks.

In 2014, the European Cybercrime Centre (EC3) launched an important initiative, the Joint Cybercrime Action Task Force (J-CAT). This is the first project of its sort, arising out of dissatisfaction with standard law enforcement techniques. The J-CAT has demonstrated the need to establish a task force located in a single physical site, regulated by a flexible administrative structure, and worthy of Member States' trust. The J-CAT has focused on cooperative investigations into some of the most egregious Internet-enabled crimes, including online sexual exploitation, nasty botnets, and identity theft rings (Reitano et al., 2015).

3.3. Organisation of American States

In April 2004, the Organization of American States (OAS) endorsed a resolution directing member states to 'evaluate the desirability of adopting the principles of the Council of Europe's Convention on Cybercrime (2001)' and 'explore the feasibility of acceding to that convention' (OAS, 2004). The OAS also adopted 'cybercrime rules and principles that will safeguard Internet users and prevent and discourage illegal exploitation of computers and computer networks, while respecting privacy and rights' (OAS, 2004). The OAS also adopted a 'Comprehensive Pan-American Cybersecurity Strategy' to address challenges caused by cyber threats and protect individual users of the Internet (Hathaway et al., 2012).

The OAS Working Group on Cybercrime advised in 2010 that members should create government agencies to investigate and punish cybercrimes, pass laws making them illegal, and allow for international collaboration in the investigation and prosecution of cybercrime offences (Hathaway et al., 2012). The Working Group also committed to reviewing the status of putting these measures into practice. Thus, the OAS has not yet created a more active program to combat cyberattacks. However, it has started a helpful regional conversation on cooperative ways to combat cyberattacks that constitute cybercrimes (Hathaway et al., 2012).

3.4. The League of Arab States

As mentioned above, the objective of the League of Arab States Convention is to increase and improve collaboration between the Arab States. In addition, there has been an increasing discourse on the protection of Arab States from Cybercrimes. However, the steps taken to prevent these states from the threat of cybercrimes are limited to three non-binding mechanisms. Therefore, this section reviews these steps and clarifies that without legally binding means, Arab states cannot cooperate to fight cybercrimes and their effects on the protection from Internet-related crimes. Although these steps are not sufficiently effective in combating cybercrimes in the Arab world, they advance cooperative and participatory efforts between Arab states to protect from and deal with the effects of cybercrimes.

3.4.1. The League of Arab States Model Law (2003)

The Council of Arab Ministers of Justice approved the League of Arab States Model Law on Combating Information Technology Offenses in their joint meeting on 22 May 2003. The Model Law proposed a draft law that attempted to enable parties to establish a common criminal policy aimed at protecting Arab society from information technology crimes. It includes criminal provisions for using a computer system for forgery, threats, blackmail, stealing moveable property, illegally collecting credit card information, illegally benefitting from communication services, and building an internet site with the intention of trafficking narcotic drugs or psychotropic substances. The Model Law allows for enhanced penalties for unlawful access conducted in conjunction with several online crimes, for illegal access committed by the offender in the course of or as a result of the fulfilment of his responsibilities, or for having enabled the commission of offences by a third party.

3.4.2 Arab Association for Cyber Security (2021)

In 2021, Qatar launched the Arab Association for Cyber Security to promote joint Arab action to discuss future challenges in the field of cybersecurity, in addition to discussing co-operation mechanisms to establish joint research and programs on cybersecurity. Arab Association for Cyber Security is one of the most important associations, as it includes specialists in the field of cybersecurity, and it is interested in establishing a link of communication and co-operation between Arab researchers. In addition, its objective is to create opportunities for capacity building and development and encourage the establishment of specialised and joint centres in Arab states. The Arab Association for Cybersecurity seeks to support Arab research in the field of cybersecurity, raise awareness of its risks, enhance the level of security, and keep abreast of technology and modern technologies. This will make electronic systems more secure, coherent, and capable of facing challenges that threaten cybersecurity to address transnational crimes and limit cyber-attacks.

3.4.3 Arab International Summit on Cybersecurity (2022)

The Arab International Summit on Cybersecurity served as the largest convention in the region for government regulators, industry professionals and solution providers to discuss and devise strategies to secure their cyber and information technology infrastructure. With the central theme of Empowering Global Co-operation in Cybersecurity, the summit offered a global overview of all aspects of the cybersecurity and information security hierarchy in any organisation. The Summit is the region's largest gathering of government regulators, industry professionals and solution providers to explore and develop strategies to protect their cyberinfrastructure. It provides an overview of all areas of

cybersecurity and the hierarchy of information security in any company, focusing on the main theme of enabling global co-operation in cybersecurity.

4. Challenges of the International Governance of Cybercrimes

International co-operation to combat cybercrimes has been not immune to challenges. These challenges highlight the significance of launching an international conversation to explain current principles in this context. It also demonstrates that international law cannot address the new issues created by cyberattacks on its own. This section discusses the challenges facing international co-operation in combating cybercrimes. It shows that without international co-operation, states cannot deal with cybercrimes as one form of transnational organised crime.

4.1. The Domestic Enforcement of Instruments on Cybercrimes

Each state experienced a different kind of cyberattack or cybercrimes. This would have an impact on states in dealing with these new crimes. It would require all states to cooperate and consider their contributions to the implementation of international and regional instruments on cybercrimes. Furthermore, protection from cyber-attacks cannot happen without the co-operation and involvement of international, regional, and national actors, including public and private sectors.

Cybercrimes and cyber-attacks have been a new trend of crimes crossing state borders. However, individual governments operating alone will not be able to solve this global crisis effectively. The first obstacle is determining how domestic and international law might be utilised to counter cyberattacks and the nature of the problem confronted by governments. The domestic enforcement of international rules governing cybercrimes and cybersecurity has been the main challenge facing states (Kleijssen & Perri, 2016).

Several measures can address certain aspects of the problem. However, addressing the core cause of the global cyber-attack threat would necessitate international co-operation. As a result, there is a need for a worldwide electronic convention with two major goals. First, a new agreement should incorporate provisions for international collaboration. Second, such a convention should define cyberattacks and cyberwarfare and limit the types of assaults to which nations may react with force. This means that governments would play a key role in developing and accepting a new cybercrime convention.

4.2. Criminal Prosecution and Criminal Justice

The second challenge facing states in combating cybercrimes is the criminal prosecutions among states and the problem of how states can achieve criminal justice considering different jurisdictions. Perhaps the reason behind the lack of 'transnational cybercrime law' is the different legal regimes of states signatories to international instruments (Guarda, 2015). In addition, the complicated kind of cybercrimes worsens when it comes to preventing, detecting, investigating, prosecuting, and adjudicating cases of cybercrimes and cyberattacks (Kleijssen & Perri, 2016). However, a major improvement in extradition links may not be achievable immediately because extradition treaties, discussed on a bilateral basis, need a significant amount of effort and time to negotiate and pass (Arnell & Faturoti, 2023). These agreements can significantly affect the prosecution of numerous crimes caused by greater globalisation, such as narcotics, weapons, human trafficking, and transnational white-collar crime (Arnell & Faturoti, 2023).

One approach to dealing with such a problem is to create a new instrument that allows states to collaborate in the collection of evidence and criminal prosecution of those participating in international cyberattacks. Once governments have agreed on a uniform definition of cyberattacks, cybercrime, and cyberwarfare, the next stage is for states to work more closely together on information sharing, evidence collecting, and criminal prosecution of those involved in cyberattacks.

4.3. International Solidarity, Transparency and Global Governance

International and regional instruments that directly regulate cybercrimes and cyberattacks address only part of the overall challenge. These instruments are limited to managing most state-party attacks because of their geographical membership. However, they serve as a foundation for creating a comprehensive international framework for controlling unlawful cyberattacks.

The principle of international solidarity has a fundamental role to play in encouraging states to combat cybercrimes. It is essential for the implementation of international rules governing the confrontation of cybercrimes (Budapest Convention, 2001). This would strengthen the commitment of all states to promote international solidarity in support of the victims of cybercrimes. It also can promote the involvement of civil society in a global campaign against cybercrimes. There is also a need to promote international debate on cybercrimes to establish practical mechanisms of international solidarity and promote the exchange of best practices among states.

In addition, consistent with state legal commitments relating to cybercrime prevention, the most technologically advanced states should be encouraged to assist the least developed states in responding to common cyber threats. Furthermore, inter-governmental co-operation should be advanced in the framework of regional co-operation, and cybersecurity capacity building should have a permanent place on the policy agenda of states. In the absence of a global consensus on norms of behaviour in cyberspace, the huge number of cyberattacks and state defence probing exercises have led different coalitions of states to design their own set of rules (Deibert & Crete-Nishihata, 2012). Efforts by governments and international organisations to define governance standards are regularly paralleled by civil society and

business actions aimed at modelling behaviour, exchanges, and responsibilities on a global level (Deibert & Crete-Nishihata, 2012).

An essential solution in preventing cybercrime is redefining the notion of 'universal' jurisdiction. This contains incidents of current cybercrimes that have international dimensions, at least when their repercussions are severe. The notion of universal jurisdiction is intended to grant sovereignty to every state in the world, regardless of whether the criminal or victim has a connection to its territory or citizenship (Ruelens, 2015). The goal of such a measure is to foster worldwide solidarity among governments and to keep specific parts of the world from becoming safe havens for international criminals. It refers to each state's right to pursue offences against the fundamental ideals of the international community (Ruelens, 2015).

5. Conclusion

The existence of co-operation between states which is the establishment of legal system in combating cross-border crimes is an important step. In addition, international and regional organisations have played an essential role in confronting cybercrimes and cyberattacks. States sought to conclude international conventions to combat cybercrimes through the conclusion of Budapest Convention to combat cybercrime.

However, states are still far from implementing international rules and legal norms in their national systems. Therefore, there is a need for cooperative action between states through international judicial co-operation and the exchange of information and documents required by judicial authorities in connection with cybercrimes. Despite the existence of many international instruments, the lack of a common approach, including within these multilateral instruments to cybercrime, means that states should cooperate to take further actions in dealing with cybercrimes.

This paper examined the problem of cybercrime from the perspective of international law and global governance. Given the current trend towards increasing cybercrimes and cyber-attacks, states have an important role to play in combating such a new trend of transnational crimes. The paper also discussed the role of international and regional organisations in preventing and protecting cybercrimes. It also examined the challenges facing states in combating cybercrimes and cyberattacks. The paper finally recommends taking the following measures at both international and national levels:

- Establishing an international system for responsibility sharing among states in combating cybercrimes.
- Prioritising the protection mechanisms of cybercrimes to avoid contradiction with free international trade.
- Reforming national legal and judicial systems in states in alignment with international legal rules in combating cybercrimes.
- Mobilising international support and advocacy to combat cybercrime by taking international actions and debate.
- Providing financial and technological support to states that are unable to combat cybercrime.

6. References

i. Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes, Overview of Existing Instruments, Recommendations and other Documents on Countering the Use of Information and Communications Technologies for Criminal Purposes, (A/AC.291/CRP.10), Second session, 20 April 2022.
ii. Ana Cerezo, Javier Lopez, and Ahmed Patel, International Co-operation to Fight Transnational Cybercrime, Second international workshop on digital forensics and incident analysis, 2007, 13–27.
iii. Chart of signatures and ratifications of the Convention on Cybercrime (ETS No. 185), Council of Europe. <https://www.coe.int/en/web/conventions/full-list?module=signatures-by-treaty&treatynum=185>.
iv. Council of Europe - Convention on Cybercrime (ETS No. 185).
v. Council of Europe, Economic Crime Division, the functioning of 24/7 points of contact for cybercrime (discussion paper prepared by the Project on Cybercrime), 2009.
vi. Guettaf Suleiman and Bouqrin Abdelhalim, Confronting Cyber Crimes in the Light of International Conventions, *The Journal of Legal and Economic Research*, Centre Universitaire Aflou, 5(2), 2022, 62–87.
vii. Henrik Kaspersen, Cybercrime and Internet jurisdiction, Project on Cybercrime, 2009.
viii. Jake Ruelens, Universal Jurisdiction: An Analysis from a Comparative and International Law Perspective. A Future of Universal Jurisdiction over Serious Crimes under International Law, University of Ghent, 2015.
ix. Jan Kleijssen and Pierluigi Perri, Cybercrime, Evidence and Territoriality: Issues and Options, in Netherlands Yearbook of International Law 2016, The Changing Nature of Territoriality in International Law, The Hague, TMC Asser Press, 2017, 147–173.
x. Jan Spoenle, Cloud Computing and Cybercrime Investigations: Territoriality vs. the Power of Disposal, Council of Europe Project on Cybercrime Discussion Paper, 2010.
xi. Joseph Schwerha, Law Enforcement Challenges in Transborder Acquisition of Electronic Evidence from "Cloud Computing Providers", Council of Europe, 2010.
xii. Kennedy Gastorn, Relevance of International Law in Combating Cybercrimes: Current Issues and Aalco's Approach, Presentation at the 4th World Internet Conference, Wuzhen Summit, on the Session on 'International Co-operation in Countering the Use of Cyberspace for Criminal and Terrorist Purposes', 2017.
xiii. Kristin Archick, and Foreign Affairs, Defense, and Trade Division, Cybercrime: The Council of Europe Convention, Congressional Research Service, Library of Congress, 2005.
xiv. League of Arab States. <http://www.lasportal.org/ar/legalnetwork/Pages/agreements_treaties.aspx>.

xv. NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE). <https://ccdcoe.org/organisations/au/>.
xvi. Nermin Alazraq, Criminal Liability Determinants of Hacking, Interception & Plagiarism and Ways of Regulation and Deterrence in Arab Legislations in the Digital Age: Analytical comparative study, *Journal of Mass Communication Research*, 56(3), 2021, 1041–1080.
xvii. Nicola Dalla Guarda, Governing the Ungovernable: International Relations, Transnational Cybercrime Law, and the Post-Westphalian Regulatory State, *Transnational Legal Theory*, 6(1), 2015, 211–249.
xviii. Oona A. Hathaway, et al., The Law of Cyber-attack, *California Law Review*, 2012, 817, 864–865.
xix. Paul Arnell and Bukola Faturoti, The Prosecution of Cybercrime–Why Transnational and Extraterritorial Jurisdiction Should Be Resisted, *International Review of Law, Computers & Technology*, 37(1), 2023, 29–51.
xx. Pedro Verdelho, The Effectiveness of International Co-operation against Cybercrime: Examples of Good Practice, Council of Europe, 2008.
xxi. Ronald J. Deibert and Masashi Crete-Nishihata, Global governance and the Spread of Cyberspace Controls, *Global Governance*, 18, 2012, 339.
xxii. Sandeep Mittal and Priyanka Sharma, A Review of International Legal Framework to Combat Cybercrime, International Journal of Advanced Research in Computer Science, 2017, 1372–1374.
xxiii. Shaikha Alzahrani, International Co-operation in Combating Cyber Attacks, *University of Sharjah Journal of Law Sciences*, 14(1), 2017, 740–772.
xxiv. Shanghai Co-operation Organization Agreement, Annex 1.
xxv. The African Union (AU). <https://au.int/en/treaties>.
xxvi. The United Nations. <https://www.un.org/disarmament/ict-security/>.
xxvii. Timothy S. Wu, Cyberspace Sovereignty - the Internet and the International System, *Harvard Journal of Law & Technology*, 10, 1996, 647.
xxviii. Tuesday Reitano, Troels Oerting, and Marcena Hunter, Innovations in International Co-operation to Counter Cybercrime: The Joint Cybercrime Action Taskforce, The European Review of Organised Crime, 2(2), 2015, 142–154.
xxix. United Nations Office on Drugs and Crime, Comprehensive Study on Cybercrime, 2013.