ITJ | The International Tax Journal

Inclusion of Cybercrimes within the Subject-Matter Jurisdiction of the International Criminal Court: Limits of Possibility

Samsar Aissa [1]

[1] Specialisation: International Criminal Law, University of Ghardaia, Algeria,
Email: samsar.aissa@univ-ghardaia.dz

Abstract---Cybercrime is one of the most dangerous emerging crimes threatening the international community. Its ability to evolve and spread rapidly, infiltrating various aspects of life, heightens its danger. However, the means available to combat these crimes are insufficient to address the issue effectively. This necessitates including cybercrimes within the International Criminal Court's subject-matter jurisdiction. However, there are several obstacles that limit the feasibility of this inclusion. This study will elaborate on the most significant of these obstacles.

Keywords---State Criminal Court, cybercrimes, obstacles, limits of possibility.

Introduction

There is no doubt that including cybercrime within the International Criminal Court's jurisdiction is important and urgent for the international community. This crime poses significant risks to both its own existence and the higher interests that the established international system aims to protect. However, several practical obstacles stand in the way of achieving this. This study will attempt to highlight the most significant of these obstacles. To this end, we have devised a two-section plan: the first section addresses subjective obstacles related to cybercrime, and the second section discusses objective obstacles related to cybercrime.

How to Cite:
Aissa, S. (2025). Inclusion of cybercrimes within the subject-matter jurisdiction of the International Criminal Court: Limits of possibility. *The International Tax Journal*, *52*(4), 1661–1671. Retrieved from https://internationaltaxjournal.online/index.php/itj/article/view/269

The International tax journal ISSN: 0097-7314 E-ISSN: 3066-2370 © 2025

Submitted: 20 November 2024| Revised: 19 March 2025| Accepted: 20 April 2025

Section One addresses the limits of possibility due to subjective obstacles related to the nature of cybercrime

Inclusion of cybercrime within the subject-matter jurisdiction of the International Criminal Court requires the definition of its characteristics and the determination of its elements in order to establish responsibility for it. Here, the subjective obstacles multiply, hindering this process. These obstacles stem from the nature of cybercrime, making it challenging, if not impossible, to achieve this goal. In this section of the study, we will briefly touch upon the most significant of these obstacles, as the scope does not allow for an exhaustive list. This will be explored through two subsections: first, we will address the obstacles arising from the crime's characteristics (Subsection One); then, we will illustrate the crime's broad scope (Subsection Two).

Subsection One: The Limits of Possibility Due to the Characteristics of Cybercrime

The characteristics of cybercrime make it exceedingly difficult to define its parameters and place it within a legal context that would permit its inclusion within the International Criminal Court's subject-matter jurisdiction. These characteristics render cybercrime an emerging crime, as well as a means of creating new crimes. Additionally, they create a criminal landscape that is challenging to trace and address. Among these characteristics, the following can be mentioned by way of example:

1. Cybercrime as an emerging crime

Cybercrime is a crime that has emerged as a result of the significant technological advancements witnessed in the modern world. It evolves and changes according to time, place and human needs. It is relatively modern in the sense that it was not known in the past, and it remains largely unknown in countries that are lagging behind in the cyber domain. Its continuous renewal makes it difficult to control and manage, particularly with regard to including it in the Statute of the International Criminal Court.

2. Cybercrime in a Virtual Realm

The virtual nature of cybercrime complicates legal jurisdiction and enforcement. This environment allows for anonymity and distance, which can obscure the identities of perpetrators and victims alike.

3. Difficulty in proving cybercrime

The evidence required to prove cybercrime is often intangible and difficult to collect, which makes legal prosecution complex.

4. Challenges in detecting and combating cybercrime

The rapidly evolving techniques used by cybercriminals pose significant challenges for detection and response efforts. Law enforcement agencies often struggle to keep pace with these methods.

Subsection Two: Cybercrime in a Virtual Realm

Following significant technological advancements experienced by the international community, a new world has emerged: the virtual world. This has become a lived reality and is rapidly and forcefully competing with the physical world. People around the world are eager to access it, and nations are competing to demonstrate their level of immersion in this realm. However, this invisible world has undefined boundaries, making the crimes that occur within it or originate from it difficult to address, regulate and define legally for the purpose of criminalising them and including them within the International Criminal Court's subject-matter jurisdiction.

Subsection Three: Difficulty in Proving Cybercrime

Since the advent of the internet in the 1960s, the world has witnessed astonishing developments in communication, accompanied by the alarming rise of cybercrime both nationally and internationally. Those attempting to combat cybercrime face a fundamental issue in the fight against it: the collection of forensic evidence, which is crucial for proving the occurrence of the crime and for imposing penalties on the perpetrator.

The difficulty lies in the nature of electronic forensic evidence, which is challenging to locate and collect. Such evidence can be quickly destroyed, enabling criminals to evade punishment. This presents another obstacle to including cybercrime within the Statute of the International Criminal Court.

Subsection Four: Difficulties in Detecting and Combating Cybercrime

Cybercrime primarily occurs through smart electronic devices, which originally stemmed from computers. Computers are electronic machines designed to receive, store and process data[1], enabling simple and complex operations to be conducted quickly and accurately with automatic results. Tracing cybercrime requires digital forensic analysis, which combines the criminal sciences used by investigative bodies with knowledge of the electronic devices involved in committing cybercrimes. The aim is to extract digital evidence[2].

Conducting such investigations demands substantial scientific and technical resources, which are often kept confidential and monopolised by states. This hinders the execution of these investigations, leaving crimes unprosecuted and untraced. This presents a significant obstacle to including cybercrime within the International Criminal Court's subject-matter jurisdiction.

Section Two: The Broad Scope of Cybercrime

The virtual world, the domain of cybercrime, exceeds the physical world in terms of both quantity and scope. It is an expansive realm, and as modern humans have succumbed to it, all traditional fields are transitioning from reality to virtuality. In fact, cybercrime infiltrates every aspect of human life, indicating that the domain of crime is vast and making it challenging to establish the necessary legal frameworks for addressing and punishing offenders.

Every conceivable area must be reviewed and updated to align with the Statute of the International Criminal Court, which would require tremendous effort. Below, we will mention several important fields in this context by way of example:

1. Invasion of personal space (subsection one).
2. Invasion of financial space (subsection two).
3. Invasion of security space (subsection three).

Subsection One: Invasion of Personal Space by Cybercrime

Cybercrime violates the privacy and dignity of individuals — one of the most important human rights — by disseminating pornographic content. This includes any act of sending, publishing, preparing, storing, processing, displaying, printing, promoting or facilitating pornographic material or activities related to prostitution[3].

Such violations occur online and spread quickly, particularly affecting children, who are a vulnerable segment of society that is often exploited in this context. Although the international community has established legal protections for children, these laws are largely ineffective in practice. This creates a significant obstacle to including this crime within the International Criminal Court's subject-matter jurisdiction, given the immense resources required to combat it.

Subsection Two: The Invasion of the Financial Space of Individuals and States

Cybercrime has successfully penetrated the financial realm of individuals and states alike, impacting their financial integrity. We will discuss this in more detail below.

1. Invasion of the financial space of individuals

---

[1]- Diab, Salima and Boutrara, Bilal. Cybercrime: Foundations and Concepts', Journal of Social Science Development, University of Oued Souf, 13 January 2020, p. 10.

[2]- Bassem, Saad Ghaleb. Database Management Systems, Dar Al-Yazuri Scientific Publishing and Distribution, Amman, 2009, p. 21.

[3]- Moussa, Amr. Computer Crimes (Cyber Crimes in Egypt and the Arab Countries), University Press, Alexandria, Egypt, 2006, p. 102.

Cybercrime can manifest in various ways that affect individuals' finances. The internet enables people to communicate with the outside world and conduct buying and selling transactions online, as well as manage their businesses.
Some examples of cybercrimes that individuals may encounter and which can have an adverse effect on their financial situation include:
- Identity theft: Unauthorised use of personal information to impersonate someone else.
- Credit card fraud: Misuse of an individual's credit card information for unauthorised purchases.
- Extortion and threats: Cybercriminals may threaten to release sensitive information unless a ransom is paid.
- Bank transfer fraud: Deceptive practices used to illegally transfer funds from an individual's bank account.
- Stock Ownership Transfer: Illegal transfer of ownership of stocks to the perpetrator.
- Bill inflation: Criminals may manipulate billing systems to increase charges to the victim[4].

The following sections will provide examples of the most common of these crimes.

1. Credit cards

Various types of credit card serve as a significant tool for cybercriminals. Cybercrime occurs when the perpetrator obtains passwords stored in the victim's computer systems. This access enables the cybercriminal to infiltrate the information system, either by being present online during a transaction or by entering data into the device's memory[5].

2. Electronic fraud

Victims are often deceived into believing in lucrative projects advertised via electronic flyers across different parts of the internet. In reality, these projects are fictitious and are aimed at unlawfully seizing funds.

Invasion of the financial space of states:

Similar to individuals, cybercrime has significantly infiltrated the financial realm of states, leading to the emergence of various crimes in this context, including:
- State fund embezzlement: Cybercriminals can gain unauthorised access to state financial systems, resulting in substantial financial losses.
- Cyber espionage: Stealing sensitive financial information or data related to national security can undermine a state's financial stability.
- Disruption of financial services: Attacks on banking institutions can disrupt services, affecting the economy and public trust.
- Tax fraud: Manipulating online tax systems to unlawfully claim refunds or evade taxes.

These crimes present significant challenges to states in protecting their financial resources and maintaining economic integrity.

1. Corporate Espionage

As the term 'espionage' itself is multifaceted and cannot be confined to a single definition, there is no specific definition for electronic espionage[6]. However, electronic espionage can be identified as a form of cyber terrorism involving the use of harmful technology to cause significant damage and disruption to control stations, computer systems and communication networks, driven by political, ethnic or religious motives.
Espionage against companies can lead to various crimes, including:

---

[4]- Siraj, Karima and Daqish, Jamal. 'Economic Dimensions of Cybercrime', Journal of Marketing Studies and Business Administration, Vol. 2, No. 1, January 2018, p. 43.

[5]- Boucef, Sghir. 'Crimes Committed Online', Master's thesis, Faculty of Law and Political Science, Mouloud Mammeri University, Tizi Ouzou, Algeria, 2013, p. 4.

[6]- Najari, Faiza Ben Haj Ali. 'Cyber Espionage', article published in the journal: Strategy, No. 11, First Semester 2019, Algeria, p. 66.

- Accessing confidential information: Gaining insights into sensitive information related to bids, marketing strategies or proprietary deals for personal gain.
- Tampering with company data: Deleting, altering or disabling access to company information storage systems.
- Stealing funds: Illegally transferring funds from the company's bank accounts.
- Fraudulent electronic transactions: Manipulating sales figures or engaging in other deceptive practices.
- Threats and extortion: Using sensitive information to blackmail the company.
- Hacking company websites: Breaching the company's online presence.

These actions can result in substantial financial losses for companies[7], often amounting to billions of pounds.

2. Bank theft

Banks are vulnerable to crimes that ultimately result in the theft of their funds. Some of the most significant crimes include:

- Cybercrimes targeting banks: Various electronic crimes aimed at compromising banking operations.
- Electronic robbery: Illegally accessing financial assets through cyber means.
- Tampering with bank data: - Deleting, modifying or disabling access to critical information storage systems.
- System disruption: Causing operational shutdowns that hinder the bank's ability to function normally.
- Stock Ownership Transfers: Illegally transferring ownership of stocks.
- Hacking bank websites: Breaching the bank's online platforms to steal sensitive information or funds.

These criminal activities compromise the financial stability of banks and undermine public trust in financial institutions[8].

3. Money laundering encouraged by corruption crimes:

Billions of dollars are laundered within the framework of the corruption that plagues the global economy. This is primarily due to the environment being conducive to such crimes, which are facilitated by cybercrime. Money laundering is one of the most prominent activities carried out by organised crime networks, requiring a high degree of coordination, planning and global reach.

According to statistics from the United Nations and the International Monetary Fund, approximately $30 billion in illicit funds are laundered annually through electronic networks, crossing the borders of around 76 countries worldwide[9].

Section Three: Invasion of the Security Space by Cybercrime

As in other fields, cybercrime has infiltrated the security domain of states and consequently the international community. This is evident in several areas, including:

1. Cyberterrorism

Cyberterrorism is one of the crimes that has troubled the international community, leading to significant debates among legal scholars regarding its definition and how to respond to it. Those in control of the international system often use this term flexibly to serve their interests, adapting the definition to fit the context of the time.

A concerning aspect of cyberterrorism is its integration with cybercrime, which gives it the ability to execute attacks quickly and precisely, making it a particularly dangerous threat to international peace and security.

2. Cyber Aggression

Cyber aggression involves hostile actions taken by one state against another through cyber means, which can undermine the sovereignty and security of nations.

---

[7]- Siraj, Karima and Daqish, Jamal. Previous reference, same topic.

[8]- Siraj, Karima and Daqish, Jamal. Previous reference, same topic.

[9]- Hegazi, Mohammed. Computer and Internet Crimes (Cyber Crimes), Egyptian Centre for Intellectual Property, Cairo, Egypt, 2005, p. 8.

3. Fueling transnational organised crime
Cybercrime contributes to the growth of transnational organised crime by facilitating illegal activities that cross national borders, which complicates enforcement and legal responses.

Second: cyber aggression crimes
A review of the international community's efforts to protect international peace and security reveals that 'aggression is a key concern in the United Nations Charter, as the primary objective of establishing the United Nations is to maintain international peace and security, and aggression poses the greatest threat to this goal'. The emergence of cybercrime has complicated matters, making this crime more aggressive and difficult to confront. This necessitates its inclusion within the International Criminal Court's subject-matter jurisdiction[10], along with the significant resources and efforts that this would require.

Third: Fueling Transnational Organised Crime
Transnational organised crime encompasses a range of traditional crimes that have long been recognised by the international community. However, cybercrime has transformed these offences into new crimes that pose an existential threat to the international community. This requires responses that may exceed the international system's capacity to include them in the Statute of the International Criminal Court.

Chapter Two: The Limits of Possibility Due to Objective Obstacles Related to Cybercrime
In addition to subjective obstacles related to the nature of cybercrime that limit its inclusion within the International Criminal Court's subject-matter jurisdiction, there are equally important objective obstacles related to the crime itself. These will be addressed in two sections. In the first section, we will outline the limits of possibility due to obstacles related to the structure of international institutions. In the second section, we will discuss the limits of possibility due to obstacles related to the international approach.

First section: Limits of Possibility Due to Obstacles Related to the Structure of International Institutions
Undoubtedly, tracing the effects of international crimes and pursuing their perpetrators for the purpose of bringing them to international criminal justice requires the existence of institutions. In this study, we explore the possibility of including cybercrime within the International Criminal Court's subject-matter jurisdiction, given that it is an international institution specialising in this area. However, this institution also requires coordination with other institutions, such as the United Nations Security Council, in order to fulfil its responsibilities. However, these institutions can hinder the achievement of international criminal justice, either by complicating the legal context — as is the case in our study — or by creating barriers to the application of established rules.
Below, we outline the obstacles related to the Security Council hindering the inclusion of cybercrime within the International Criminal Court's subject-matter jurisdiction (first subsection), followed by the obstacles related to the International Criminal Court's legal framework (second subsection), and finally, the obstacles related to the relationship between the International Criminal Court and the Security Council (third subsection).

First Subsection: Obstacles Related to the United Nations Security Council
The Security Council is the United Nations' executive body, and according to the United Nations Charter[11], it plays a fundamental role in maintaining international peace and security — two of the organisation's most important objectives. Therefore, the Security Council is a vital institution; without

[10]- Kheir Al-Din, Shamama. 'The Role of the International Criminal Court in Punishing the Crime of Aggression in Light of the Kampala Amendments', article published in the Journal of Arab Policies, Doha, Qatar, no. 6, January 2014, p. 119.
[11]- Ndiaye, Sidy Alpha. The Security Council and International Criminal Jurisdictions, Doctoral Thesis, Doctoral School of Human and Social Sciences, University of Orléans, France, 2011, p. 77.

it, legal texts would be meaningless. However, the Security Council can sometimes impede the pursuit of international criminal justice. In the context of our study, for instance, the Security Council may present an obstacle because of its legal framework: the permanent members of the Security Council have the right of veto. They can block any decision or proposal brought before the Council, leading to criticism and undermining international confidence in it.

Dr Omar Mahmoud Omar states: 'The use of the veto right, the Council's procedures, the non-participation of other United Nations members in its decisions, the lack of transparency in its actions and the unfair representation of permanent member states have led to a wave of criticism against the Council.[12]'

If any of the five permanent members decided to exercise the veto, either deliberately or because it does not align with their interests, the veto right would be an obstacle to including cybercrime within the subject-matter jurisdiction of the International Criminal Court.

Second Subsection: Obstacles Related to the Nature of the International Criminal Court

The nature of the ICC may pose an obstacle to the inclusion of cybercrime and the tracking of its perpetrators. The ICC is considered a new, permanent, independent international organisation with jurisdiction only over crimes committed after 1 July 2002. It complements national criminal jurisdictions and was established by an international treaty to prosecute individuals suspected of being responsible for serious violations of international humanitarian law[13].

As it is established by a treaty, it is considered a 'treaty-based court' that is only binding on its member states (Article 26 of the 1969 Vienna Convention on the Law of Treaties)[14], rather than a supranational entity. It is similar to other existing entities and is not a substitute for national criminal justice, but rather complements it[15]. More precisely, the ICC cannot prosecute individuals who commit cybercrime if their state is not a member of the ICC Statute or has not issued a declaration accepting its jurisdiction. This is a challenging prospect and therefore the Statute of the Court must be amended to overcome this obstacle, which is difficult to achieve.

Third Subsection: Obstacles Related to the Relationship Between the International Criminal Court and the Security Council

As previously mentioned, the Security Council is the executive body of the United Nations and has the power to enforce rulings issued by the International Court of Justice. Similarly, the Security Council has a close relationship with the International Criminal Court. However, this relationship has faced significant criticism, particularly in cases of 'referral' and 'deferral'.

First: Referral Authority:

Regarding referral authority, this "consists of a request directed to a judicial body without infringing upon its jurisdictional boundaries. The council exercises this authority when it submits a request to the International Criminal Court to investigate international crimes relating to the maintenance of international peace and security, and to prosecute their perpetrators[16]. This is stipulated in paragraph (b) of Article 13: 'The Court may exercise its jurisdiction regarding a crime referred to in Article 5 in

---

[12]- Omar, Omar Mahmoud. 'Towards Reforming the United Nations Security Council (Its Necessity and Dimensions)', article published in the Jordanian Journal of Applied Sciences, Humanities Series, Vol. 16, No. 2, 2014, p. 205.

[13]- Saadallah, Omar. International Judiciary and International Humanitarian Law in the Age of Extremism, Dar Houma for Printing, Publishing and Distribution, Algeria, 2015, p. 257.

[14]- The Vienna Convention on the Law of Treaties, adopted by the United Nations Conference on the Law of Treaties, held under General Assembly Resolutions No. 2166, dated 5 December 1966, and No. 2287, dated 6 December 1967. The conference took place in two sessions in Vienna, from 26 March to 24 May 1968 and from 9 April to 22 May 1969. It was adopted on 22 May 1969, opened for signature on 23 May 1969, and entered into force on 27 January 1980.

[15]- Ashnan, Al-Moktar. The Principle of Complementarity Between the International Criminal Court and National Criminal Jurisdiction, Doctoral Thesis in Public Law, Doctoral School 'Human Sciences and Society', François Rabelais University of Tours, France, 2015, pp. 74–75. Thesis available at: http://www.theses.fr/2015TOUR1004 (accessed 19 September 2025, 09:33).

[16]- Abdelwahab, Shitar. 'The Powers of the Security Council in Light of the Statute of the International Criminal Court', Thesis for a Doctorate in Law, Faculty of Law and Science, University of Tizi Ouzou, 2014, p. 18.

accordance with the provisions of this Statute in the following situations: if the Security Council refers a situation to the Prosecutor acting under Chapter VII of the United Nations Charter, indicating that one or more of these crimes may have been committed.[17]'

Secondly, the deferral authority is defined as follows:
As for the deferral authority, after granting the Security Council exclusive rights to refer crimes to the Court in Article 13(b) of the Rome Statute, Article 16 then stipulates that the Security Council has exclusive superior authority or guardianship over the Court and its institutions under the title of deferring investigation or prosecution[18]. Consequently, Article 16 imposes absolute and fundamental powers on the Security Council without restrictions, and their use will inevitably prevent the Court and its institutions from fulfilling their role[19]. Moreover, this provision contradicts the concept of the relationship between the two bodies and results in negative legal consequences[20]. These two authorities hinder efforts to include cybercrime in the Statute of the International Criminal Court, either by preventing referral altogether or by deferring investigation if referral occurs.

Second Section: Limits of Possibility Due to Obstacles Related to the International Approach
Alongside the structural obstacles faced by international institutions, there are other equally significant obstacles related to the international approach. More precisely, these obstacles arise from clashing international interests. This evident role of the concept of interest within the realm of public international law is acceptable given that the international community consists of sovereign states that lack a genuine intention to establish effective legislative representation reflecting conflicting interests and capable of achieving alignment and consensus. Therefore, states pursue their interests without restraint[21].
The pursuit of interests is thus an active practice of states, which often causes paralysis within international institutions. These interests can be categorised into three types: obstacles related to the economic interests of states (first subsection), obstacles related to the political interests of states (second subsection), and obstacles related to hidden imperial interests (third subsection).

First Subsection: Obstacles Related to the Economic Interests of States
Economic interests are one of the most significant reasons for the competitive and intense atmosphere between states. This competition often drives some states to engage in illegal activities to achieve their objectives, including cybercrime in the economic domain. This highlights the necessity of including cybercrimes within the International Criminal Court's subject-matter jurisdiction. Economic interests are diverse and varied, including those related to energy resources, arms sales and the activation of global media institutions, which we will outline below.

First Subsection: Interests Related to Energy Resources
It could be argued that energy resources are the primary cause of most global conflicts throughout history. They have shaped the geopolitical landscape and created alliances throughout time and space. This phenomenon has become increasingly evident in the present day. In this context, the interests of certain states, particularly major powers, may coincide with cybercrime, raising the question of whether cybercrime should fall within the International Criminal Court's subject-matter jurisdiction.

Second Subsection: Interests Related to Arms Sales
Interest in arms sales is as significant as interest in energy resources because selling arms generates substantial revenue for states. Some nations are so eager to sell arms that they fabricate wars and

---

17- See Article 13 of the Statute of the International Criminal Court.
18- Al-Majdoub, Mohammed. International Criminal Justice and Criminal Courts, Dar Al-Manhal, Beirut, Lebanon, 2010, p. 514.
19- Sur, Serge. 'International Criminal Law Between the State and International Society', Current Events and International Law, October 2001, p. 5. Article available at: http://www.ridi.org/adi/200110sur.htm (accessed 11 September 2025, 20:26).
20- Al-Majdoub, Mohammed. 'Previous Reference', p. 515.
21- Hussein, Mustafa Salama. Dual Treatment in Public International Law, Dar Al-Jami'a Al-Jadida, Azbatia, 2007, p. 20.

exacerbate existing conflicts to facilitate sales. Once again, the interests of certain influential states may align with cybercrime in this context, which poses a significant obstacle to including such crimes within the International Criminal Court's subject-matter jurisdiction.

Third subsection: Obstacles Related to the Political Interests of States

Alongside energy-related interests, there are political interests primarily concerned with global leadership. To achieve dominance and control, states that aspire to this often use straightforward and complex methods. In this context, they engage in numerous cybercrimes against their rivals and competitors. One of the most notable of these crimes is 'espionage', which is defined as 'the act of an unauthorised individual unlawfully accessing operating systems in various communication devices for improper purposes, allowing the spy to transfer, delete or add files or programs'. They can also control the operating system by issuing commands such as printing, scanning or storing. This can be carried out through organised or individual espionage against individuals, states, organisations or international or national institutions, using the informational resources and electronic systems brought about by technological advancements in the information age.

Types of cyber espionage crimes[22].

Cyber espionage crimes can take various forms, including:

1. Political and security espionage crimes:

This type of crime involves spying on or threatening to assassinate political figures, as well as infiltrating vital public institutions of the state. Several incidents have involved attacks on military centres through cyber piracy to access and acquire information stored in their computer systems. Notable examples include the theft of military information relating to NATO member states' warships through the French Navy's computer systems in the summer of 1994[23].

2. Social and Political Espionage Crimes:

These crimes affect the lives and well-being of civilians, as well as their culture. They target communities through media messages that terrorise and intimidate. This includes gaining illicit access to individuals' electronic identities, such as email accounts and passwords. This can lead to identity theft and the extraction of important files and images from individuals' devices. The aim is to force individuals to comply with demands, thereby disrupting social relationships and damaging the moral fabric of society, particularly within family dynamics. The various outcomes of cybercrime, such as defamation, the spreading of false news and rumours, and cases of kidnapping and assassination (even after ransom payments have been made), can have a severe impact on social structures[24].

These crimes may be of interest to powerful states, which could further hinder the inclusion of cybercrime in the Statute of the International Criminal Court.

Third subsection: Discriminatory Obstacles Related to Hidden Imperial Interests

There are other hidden obstacles that may not be immediately visible, but which manifest as practical actions in the field. These obstacles stem from several premises, including:

First: Double standards in handling

'States and international organisations often resort to double standards to achieve specific goals. The double standard in treatment is not an end in itself, but rather a means to achieve various objectives that actors of international law strive to attain. These objectives can be both visible and apparent, as well as hidden and imperceptible[25].

Secondly, there are hidden differences regarding the concept of international justice.

While the term 'international justice' may seem clear in United Nations documents, it is in fact vague and ambiguous, as it is related to the values from which it is established. For example, one person may

---

[22]- Salami, Nadia. 'Mechanisms for Combating Cyber Espionage', thesis submitted for the Doctorate in Sciences, University of Arab Tebessa, Faculty of Law and Political Science, Department of Law, Academic Year 2018–19, p. 25.

[23]- Kziz, Sabah and Qat, Samir. 'The Impact of Cyber Crimes on the Security and Stability of States': The Example of the Hacking of the Qatari News Agency's Website', Journal of Political Studies Critique, No. 3, October 2014, p. 127.

[24]- Same reference and topic.

[25]- Hussein, Mustafa Salama. Previous reference, p. 16.

see someone as a victim, while another may see them as a terrorist. This raises serious issues that require the international community to regulate terminology away from discriminatory foundations, similar to the term 'terrorism', as discussed in the first section of this study. Such ambiguity can result in injustice and double standards permeating international relations.

These hidden, discriminatory, imperialist interests represent a significant barrier to incorporating cybercrime within the International Criminal Court's subject-matter jurisdiction. Those with these interests find that this type of crime creates a grey area that allows them to evade accountability, enabling them to pursue their interests without facing justice before the ICC.

Conclusion

The aim of this study was to shed light on the limits of possibility for including cybercrimes within the International Criminal Court's subject-matter jurisdiction. We reached the following conclusions and made the following suggestions:

First: Results:

1. Serious threat: cybercrimes are among the most dangerous threats facing the international community. They evolve rapidly in line with changes in time, space and human needs. The measures taken by the international community to combat cybercrime are insufficient; they are either isolated and inadequate, or non-existent for those lagging behind in technological advancement.

2. Necessity for inclusion

Given the ineffectiveness and inadequacy of the measures taken by the international community to address cybercrime, it has become essential to include this crime within the International Criminal Court's subject-matter jurisdiction to bring its perpetrators to international criminal justice. This inclusion aims to limit or at least constrain the spread of such crimes.

3. Existing obstacles

The inclusion of cybercrime within the International Criminal Court's subject-matter jurisdiction faces several obstacles, including subjective ones related to the nature of the crime, as well as others concerning the subject matter. We have discussed these in some detail, as permitted by the context.

Second: suggestions

1. Urgent action is required to remove the obstacles hindering the inclusion of cybercrime within the International Criminal Court's subject-matter jurisdiction. The rapid evolution of cybercrime poses a significant threat to international order and public safety, necessitating a swift response.

2. Re-evaluation of existing systems

The international community should reconsider the existing Security Council and International Criminal Court frameworks to facilitate the inclusion of cybercrime in the Statute of the International Criminal Court. This would enable effective responses to this growing challenge.

References:

Books:

1. Omar Moussa, Cyber Crimes: Computer Crimes in Egypt and Arab Countries, University Office, Alexandria, Egypt, 2006.
2. Mohamed Hegazy, Computer and Internet Crimes (Cyber Crimes), Egyptian Centre for Intellectual Property, Cairo, Egypt, 2005.
3. Mohamed Al-Majdoub, International Criminal Justice: Criminal Courts, Dar Al-Manhal, Beirut, Lebanon, 2010.
4. Mostafa Salama Hussein, Double Standards in International Public Law, Dar Al-Jamiah Al-Jadida, Al-Zabtiya, 2007.
5. Saad Ghaleb Yassin, Database Management Systems, Al-Yazouri Scientific Publishing and Distribution, Amman, 2009.

6. Saad Allah Omar, International Justice and Humanitarian Law in the Age of Extremism, Homa Publishing and Distribution, Algeria, 2015.

Articles

1. Salima Diab and Bilal Boutarrah, 'Cybercrime: Foundations and Concepts', Journal of Social Science Development, University of Oued Souf, 13 January 2020.
2. Khaireddine Chamama, 'The Role of the International Criminal Court in Punishing the Crime of Aggression in Light of the Kampala Amendments', Arab Policies Magazine, Doha, Qatar, Issue 6, January 2014.
3. Omar Mahmoud Omar, 'Towards Reforming the United Nations Security Council (Necessity and Dimensions)', Jordanian Journal of Applied Sciences: Humanities Series, Vol. 16, No. 2, 2014.
4. Faiza Najari Ben Hajj Ali, 'The Crime of Electronic Espionage', *Strategia Magazine*, Issue 11, First Half, Algeria, 2019.
5. Karima Sira and Jamal Daqish, 'The Economic Dimensions of Cybercrime', Journal of Marketing Studies and Business Administration, Vol. 2, No. 1, January 2018.
6. Bouchef, S. (2013). 'The crime committed via the internet'. Master's thesis. Faculty of Law and Political Science, Mouloud Mammeri University, Tizi Ouzou, Algeria.
7. Sabah Kziz and Samir Qat: 'The Impact of Cyber Crimes on the Security and Stability of States: The Case of the Qatari News Agency Hack', Al-Naqid Journal of Political Studies, Issue 3, October 2014.

Doctoral theses

1. Nadia Salami, 'Mechanisms for Combating Electronic Espionage', thesis submitted for a Doctorate in Sciences, Faculty of Law and Political Science, University of Arab Tebessa, Tebessa, Academic Year: 2018–19.
2. Chiter, Abdelwahab. 'The Powers of the Security Council in Light of the Statute of the International Criminal Court'. Thesis submitted for a Doctorate in Law. Faculty of Law and Political Science, University of Tizi Ouzou. Academic Year: 2014–15.

International Documents

1. Rome Statute, adopted by the United Nations Conference on the Establishment of an International Criminal Court on 17 July 1998 and entered into force on 1 June 2001.
2. Vienna Convention on the Law of Treaties, adopted by the United Nations Conference on the Law of Treaties in Vienna on 22 May 1969, entered into force on 27 January 1980.

Foreign References

References for Doctoral Theses

1. Sidy Alpha Ndiane, 'The Security Council and International Criminal Jurisdictions', Doctoral Thesis, Doctoral School of Human and Social Sciences, University of Orléans, France, 2011, p. 77.
2. Almoktar Ashnan, 'The Principle of Complementarity Between the International Criminal Court and National Criminal Jurisdiction', Doctoral Thesis in Public Law, Doctoral School 'Science of Man and Society', François Rabelais University of Tours, France, 2015, pp. 74–75. Thesis available at: http://www.theses.fr/2015TOUR1004 (accessed 19 September 2025 at 09:33).

Articles

1. Serge Sur, 'International Criminal Law Between the State and International Society', Current Affairs and International Law, October 2001, p. 5. Article available at: http://www.ridi.org/adi/200110sur.htm (accessed 11 September 2025, 20:26).