Criteria of Relative Gravity for determining cyber-attacks as a Serious violation

Luma Fadel Nayef
Student at Al-Alamain Institute for Postgraduate Studies - Department of Public Law, Najaf, Iraq.
luma95fadel@gmail.com

Prof. Dr. Ahmed Aubais Alfatlawi
Department of Public Law, Faculty of Law, University of Kufa, Najaf, Iraq
Lecturer at Al-Alamain Institute for Postgraduate Studies, Najaf, Iraq.
ahmeda.alfatlawi@uokufa.edu.iq

تاريخ استلام البحث 2024/7/1 تاريخ ارجاع البحث 2024/7/19 تاريخ قبول البحث 2024/8/4

Cyber-attacks have become one of the means to commit crimes without losses, whether material or human; if military force costs countries a lot of losses at all levels, cyber-attacks have enabled countries to implement their plans and hit another country's systems with the push of a button. The effects of their destruction may exceed t he impact of traditional grave violations, whether infrastructure destruction or human losses. In this area, the information space is seen as the fifth area of war by the military, as the US Department of Defense states that "although information space is a man-made field, it is as important for military operations as land, sea, air, and space." The application of quantitative and qualitative relative gravity standards to information behavior (cyber-attacks) that may fall within the jurisdiction of the ICC, as well as how crimes are committed, instigated, or facilitated in the "cyber" information space.

Keywords: Cyber-attacks, Relative Gravity, Quantitative and qualitative criteria, Serious violations.

Introduction

If we assume that a cyber-attack may constitute, incite, or facilitate an international crime, it is essential to clarify, as previously noted, that for a case to be admissible before the ICC, it must meet the criterion of sufficient gravity. Under the Rome Statute, gravity is a fundamental element of a crime's admissibility before the Court and serves as the primary threshold before other elements are considered. The Statute includes multiple explicit references to the relative gravity and seriousness of international crimes, as reflected in the definitions provided in Articles (6, 7, 8, and 8 bis).

For instance, Article (8 bis/1) specifies that an act of aggression must (by its character, gravity and scale, constitutes a manifest violation of the Charter of the United Nations), Article (7) requires that crimes

against humanity be (committed as part of a widespread or systematic attack directed against any civilian population). Regarding war crimes, Article (8/1) states (The Court shall have jurisdiction in respect of war crimes in particular when committed as part of a plan or policy or as part of a large-scale commission of such crimes).

1. The Significance of the Research

Cyber-attacks may be one of the most serious threats to international peace and security, as the nature of offensive operations in the information space represents unique challenges to the international criminal system. Therefore, there is a debate in legal academic circles about classifying cyber-attacks as basic crimes under ICL, in the sense of linking cyber-attacks to war crimes, genocide, crimes against humanity, and crimes of aggression.

Does the Rome Statute of the ICC require amendment and increase cyber-attacks to the core crimes stipulated in Article 5?

2. Problem Statement

For a case to be admissible before the International Criminal Court (ICC), it must meet a threshold of relative gravity, indicating a substantial level of seriousness that raises concern within the international community. According to Article 17(1)(d) of the Rome Statute, a case cannot be deemed admissible if it lacks sufficient gravity to warrant further action by the Court. Furthermore, Article 53(2)(b) of the Statute states that if an investigation does not reveal adequate grounds for prosecution, the case may be ruled inadmissible under Article 17. This ensures that only cases of significant gravity are pursued in line with the Court's mandate.

Cyber-attacks pose complex challenges to the international community due to three main factors: the absence of territorial jurisdictions in cyberspace, the lack of uniform laws on such attacks worldwide, and the rapid and continuous development of such attacks. The perpetrators of these attacks will continue to evolve, surpassing the efforts of law enforcement agencies unless States address all these interrelated factors cooperatively.

3. Research Method

We will follow the inductive approach by indicating the relative gravity criteria and their relationship to serious violations and cyberattacks. In addition, we will follow the analytical approach by analyzing the relationship between relative gravity and the most serious crimes at the international level, which are known as serious violations, and their relationship to cyberattacks.

4. Structure of Research

We will address this in three parts: first, we will identify the key individuals responsible; second, we will explore the quantitative and qualitative criteria for determining the relative gravity of cyber-attacks; and third, we will examine the legal framework governing cyber-attacks.

1. The most responsible persons

Concerning the first criterion for assessing relative gravity in the context of cyberattacks, a divergence of opinion emerged between the Prosecutor and PTC I in the Mavi Marmara case regarding the identification of those most responsible or bearing the greatest responsibility for the alleged crimes (Roscini, 2019).

The OTP decided not to initiate an investigation, citing, among other reasons (Saxon, 2016), the lack of a reasonable basis to believe that senior IDF commanders and Israeli officials were responsible as perpetrators or planners. The OTP interpreted the term "most responsible" to refer to senior individuals. Applying this reasoning to the context of cyberspace, a case against a high-ranking military commander who plans and orders multiple harmful and unlawful cyberattacks would carry greater gravity than a case against an independent hacker acting on instructions to execute such attacks. (Al-Momeni, 2001).

A distinguishing feature of cyberattacks is the involvement of multiple individuals—the multiplicity of perpetrators—working together to harm the victim. These attacks typically involve a person skilled in computer technologies who executes the technical aspects, alongside another individual who oversees the manipulation process and manages the transfer of illicit gains. Participation can also take a negative form, such as the silence or inaction of individuals aware of the attack, which facilitates its completion. Alternatively, participation may be positive, involving the provision of technical or material assistance to support the attack. Determining rank and seniority presents a significant challenge in the context of cyberspace operations, as actors in this domain often function within horizontal structures rather than hierarchical frameworks.

These dynamics prioritize cyber skills and the exploitation of an opponent's vulnerabilities over traditional command-and-control authority. (Saxon, 2016, pp. 570-571)

The most significant opinion concerning relative gravity, and notably the only one rendered by the Appeals Chamber, arose in the Tribunal's first case involving the situation in the Democratic Republic of the Congo. In this case, the Prosecutor submitted a request to PTC I to issue arrest warrants for Thomas Lubanga and

Bosco Ntaganda, both accused of war crimes. Although the Prosecutor did not address the issue of admissibility, PTC I determined that, before issuing an arrest warrant, it was necessary to first assess the admissibility of the proposed case. The Chamber, on its own initiative, proceeded to evaluate the relative gravity of the matter (DeGuzman, 2013).

PTC I observed that the ICC's jurisdiction is already restricted to crimes of significant gravity and seriousness. Relative gravity, therefore, constitutes an additional layer of evaluation in the classification of crimes. PTC I referred to this concept as an "additional threshold." According to PTC I, relative gravity comprises three components. First, the conduct in question must be either systematic or widespread. In this regard, the Chamber emphasized that "due consideration" should be given to the "social alarm" triggered by such behavior. Second, the accused must hold a senior command position in the case under investigation. Third, the accused should be among those most responsible for the alleged crimes. To support these second and third components of the relative gravity test, the judges emphasized the importance of concentrating the Court's efforts on senior commanders most responsible for such crimes. This focus, they argued, aligns with the ICC's central purpose of deterring the commission of serious crimes (DeGuzman, 2013, p. 478).

The Chamber issued an arrest warrant for Lubanga but declined to issue one for Ntaganda, arguing that he was not among the senior commanders responsible for the crimes in question. However, the Appeals Chamber disagreed with PTC I on all points, including the limitation of admissibility to the most responsible senior commanders. The Appeals Chamber argued that such a limitation would undermine deterrence, as it would leave all perpetrators of international crimes beyond the ICC's reach. PTC I revised its position, contradicting the logic of the OTP by limiting the ICC's jurisdiction to certain categories, which was contrary to the Statute. (However, the OTP argued that the designation of "most responsible persons" should not be based on calculations of seniority or the hierarchical position of those responsible for the alleged crimes (Marco Roscini., 2019).

In the context of PTC I, the term "most responsible" refers to individuals who played the most significant role in committing the crime, regardless of their position or rank. It is important to clarify that the term "hacker" refers to individuals who carry out hacking, sabotage, and espionage operations in cyberspace. The term "cracker," which is the plural of "cracker," is used to describe individuals who specialize in deciphering or cracking programs or

passwords, without necessarily engaging in network sabotage (Al-Rawi, 2021).

Based on this identification, the perpetrator of the attack is classified as belonging to one of two types. The individual carrying out the attack can be defined (as that person who has technical knowledge and skills in the field of computers and information security that enable him to carry out hacking, sabotage and espionage operations through cyberspace, or decipher or break programs or passwords to change or disable information, or to imitate and exploit programs, or to transfer and seize the accounts of others, or to control the computer or operate it unlawfully, by using a specific information system) (Al-Husseinawi, 2009).

Accordingly, we can identify several characteristics of the perpetrator of a cyber-attack as follows (Al-Rawi, 2021, p. 11):

1. The individual possesses advanced knowledge and technical expertise in computers and information security, which enables them to infiltrate cyberspace and electronic networks, bypass passwords, and circumvent security measures. This skill set allows them to penetrate systems designed to protect sensitive data, such as those used by banks and military institutions, and specialize in cyber-attacks without relying on traditional or conventional means of aggression.
2. The perpetrator is often highly intelligent, equipped with the skills to modify or develop security systems that prevent tracking or detection of their activities. They are capable of manipulating data storage, controlling network systems, and accessing computers at unauthorized times. Typically, the cyber attacker carries out multiple attacks rather than a single one, driven by motives such as quick financial gain and immediate wealth. This often involves theft, fraud, and the seizure of credit card numbers or account details, which they exploit for illicit purposes via the Internet.

Individuals involved in cyber operations assume various roles, not only executing attacks but also participating as co-perpetrators in activities such as developing and designing malware, recruiting and training hackers, gathering information about the target system necessary for the attack, and ensuring access to the required devices for carrying out the operation.

Actions in cyberspace may also facilitate or contribute to the commission of conventional international crimes. For instance, individuals may hack into systems to obtain confidential information essential for enabling an international crime, or they may use the Internet to spread warnings encouraging further violence, such as inciting the continued targeting of civilians from a specific religious group during an armed conflict (Roscini, 2019, p. 257).

The challenge in applying the "most responsible" criterion lies in the difficulty of obtaining sufficient evidence to attribute conduct, particularly during the initial screening stage, as anonymity is a defining feature of cyberspace. Cyber-attacks pose unique challenges due to two key characteristics of cyberspace: the anonymity of the perpetrator and the ambiguous territorial boundaries that complicate jurisdictional issues (Roscini, 2019, p. 258).

The Internet, specifically, is a decentralized system where communication protocols and transmitted data are broken into multiple packets. These packets take various, unpredictable paths to reach their destination, where they are then reassembled (Brenner, 2011).

The IP address identifies the origin and destination of data in collaboration with the Internet Service Provider (ISP), linking the relevant system to the IP address on the Internet. While it can be associated with an individual, group, or country, the IP address may be subject to "spoofing," or the system corresponding to the IP address may serve as a "starting point" for an attacker located elsewhere (Andres, 2011) (Shackelford, 2009)

Attribution of a cyber-attack refers to the ability to identify the perpetrator of the attack and the location from which it originated. This process is arguably one of the most difficult challenges in cybersecurity. First, tracing an attack from the IP address to the end user is complicated, as IP addresses are often linked to multiple end users. Second, hackers can obscure their identities, as the Internet is designed for rapid communication and lacks clear geographical boundaries (Greco, 2020).

Providing sufficient evidence to identify the hacker and determine whether they are the most responsible person may pose a significant challenge for the prosecutor. This process will likely require the cooperation of the countries from which the cyber operation originated. Additionally, another challenge is that most cyber-attacks are not conducted by states; rather, they are carried out by non-state actors, often facilitated by individuals or groups acting independently. Although cyber weapons can cause significant damage due to their high destructive potential, they are relatively inexpensive and easily created by highly skilled hackers. However, ICL does not apply to these categories of actors (Greco, 2020, p. 41).

In 2013, the OTP appointed a digital forensic expert to the Scientific Response Unit to enhance its ability to collect and analyze digital evidence (Macauley, 2013) (Warden, 2014).

Assessing the admissibility of a case, including its relative gravity, becomes more challenging at the post-investigation stage. The lack of

sufficient evidence can be a significant obstacle to identifying and prosecuting those most responsible for crimes involving cyberspace conduct (Longobardo, 2016).

Following this analysis, it is clear that PTC I explained the concept of relative gravity, emphasizing the accountability of those most responsible and focusing on widespread and systematic attacks that cause social alarm. This approach aligns with the ICC's objective of holding individuals accountable for the most serious crimes of concern to the international community. Therefore, it is unnecessary to assert that cases not involving grave violations will fall within its jurisdiction, including certain forms of cyberattacks. Addressing such serious attacks requires genuine international cooperation and their inclusion under the provisions of the Rome Statute.

2. Quantitative and qualitative criteria for the relative gravity of cyber-attacks

We have previously outlined the quantitative and qualitative criteria used by the OTP of the ICC to assess the gravity of situations and cases within its jurisdiction. In this regard, we will now examine how these criteria impact the evaluation of the gravity of situations and cases involving cyber conduct that constitutes, incites, or facilitates international crimes under the ICC's jurisdiction, as assessed in the context of each individual case (Schabas, 2008).

Therefore, we will break this down into several parts to illustrate the application of these quantitative and qualitative criteria to cyber behavior, and assess whether such behavior, if of significant gravity, can constitute a grave violation that falls within the jurisdiction of the ICC.

2.1 Number of direct and indirect victims of cyber behavior

The number of victims, particularly fatalities, is a key factor in "quantitative gravity," which reflects the seriousness and extent of the offense. Therefore, the OTP decided not to open an investigation into the "Mavi Marmara" attack, as the number of victims was relatively low compared to other cases under investigation by the prosecutor. Similarly, the "Counter-Terrorism Committee" also emphasized the importance of victim numbers, which played a role in initiating investigations into the situations in "Kenya" and "Georgia" (Marco Roscini., 2019, p. 261).

When applied to cyber systems, cyber-attacks can cause substantial physical damage to people and property. For instance, cyber behavior could lead to the shutdown of an electricity plant during winter, resulting in civilian deaths due to freezing temperatures. Similarly, a cyber-attack could disable computers controlling water stations and dams, causing flooding in populated areas, or compromise the air

traffic control system, potentially causing the downing of a civilian aircraft.

2.2 Temporal and Territorial Dimension of Cyber Attacks

Cyber-attacks can have a wide geographic impact while resulting in limited physical damage. For example, the malicious "Stuxnet worm" spread across computers in several countries, including Iran, Indonesia, India, Azerbaijan, the United States, and Pakistan. However, it is reported to have caused significant damage only to Iran's uranium enrichment facility in Natanz, with minimal effects on other computers lacking specific vulnerabilities (William A. Owens, 2009).

Similarly, millions of botnets operating across multiple countries can cause temporary disruptions, such as brief service outages, but these typically do not result in material harm to people or property. Consequently, even if such attacks were deemed crimes under the jurisdiction of the court, operations like the 2007 DDoS attacks on Estonia, which disrupted banking and communications, would be considered serious only in a broad sense, unless they caused loss of life or destruction of physical property (Klanter, 2016).

2.3 The Qualitative Gravity of Cyber Attacks

A situation or case does not necessarily require a large number of victims to justify an investigation and prosecution. Qualitative criteria must also be considered. For instance, crimes such as murder, rape, and other forms of sexual violence, crimes against children, persecution, or the imposition of living conditions intended to destroy a group, are inherently more serious than other crimes. This means that some crimes are, by their nature, more severe than others. National and international sources, for example, consistently recognize murder as the most serious crime. Similarly, crimes involving sexual violence, torture, and physical or psychological suffering are considered highly serious, whereas, as noted by the ICC Trial Chamber, crimes against property are relatively less severe (Heller, 2010).

However, if accepted, cases involving cyberattacks that result solely in damage to physical property, such as the "Stuxnet" case, may not be considered sufficiently serious in nature, especially when compared to cases involving murder or physical suffering. This indicates that relative gravity plays a role in the selection of cases for investigation, as explained above.

2.4 Other Criteria for Relative Gravity

Other criteria for assessing relative gravity include the means used to carry out the crime, the degree of involvement of the perpetrator, the perpetrator's intent, the extent to which the crimes were systematic,

whether the crimes were part of an organized plan or policy, the abuse of authority or official capacity, and elements of special cruelty. These elements may include the vulnerability of the victims, any discriminatory motives, or the use of rape and sexual violence as a means of destroying groups (Marco Roscini., 2019, p. 266).

The various degrees of involvement in cyber operations have already been outlined, including the means used to commit the crime. In this context, malware and cyber infrastructure such as computers and servers are unlikely to be considered aggravating factors, unlike more traditional means of harm, such as the use of electric shocks, machetes, or prohibited weapons. Additionally, distinguishing "criminal intent" in a cyber context is challenging, as malware may operate unpredictably due to technical errors or insufficient knowledge of the target systems. Nevertheless, cyber-attacks can be considered cruel, as exemplified by an attack that alters patients' medical data, leading to incorrect, painful, or unnecessary treatments (Marco Roscini., 2019, p. 266).

Among other criteria, the degree of suffering experienced by the victims, their heightened vulnerability, and the social, economic, and environmental damage inflicted on the affected communities are crucial factors. The impact, therefore, has two dimensions: the direct effect on the victims and the broader societal consequences.

Including this "impact" criterion in the assessment of relative gravity means that even situations where the number of victims meets quantitative thresholds may still be considered serious from a qualitative standpoint if they cause significant societal impact.

For instance, cyberattacks that result in the deaths of peacekeepers and humanitarian workers can have a profound impact, given the importance of peacekeeping and humanitarian missions and the potential deterrent effect on such efforts. Similarly, cyberattacks aimed at influencing political elections can significantly affect society as a whole (Heller, 2010, pp. 236-237).

Cyberattacks aimed at influencing political elections can have a significant impact on society. For instance, in August 2017, the Kenyan opposition claimed that hackers manipulated the results of the recent election by breaching the Kenya Electoral Commission's database to access voter data and develop a targeted campaign strategy (Dias, 4 April 2018).

The ICC did not classify the incident as an international crime, but the violence that followed the president's re-election in Kenya resulted in at least 24 deaths (Dias, 4 April 2018).

Some cyberattacks can have significant economic repercussions, as seen in the 2007 DDoS attacks against Estonia. More generally,

cyberattacks targeting critical national infrastructures that disrupt essential services can have a profound societal impact, especially if their effects are prolonged. In such cases, it is important to consider not only the social and economic damage but also the potential harm to the natural environment. For example, a cyber-attack on a chemical plant could aim to release hazardous substances into the environment during an armed conflict (Roscini, 2019, p. 269).

3. Legal Regulation of Cyber Attacks

The application of ICL to cyberattacks and the prosecution of perpetrators in the international arena presents several practical challenges. These include issues of national sovereignty, the need for multinational cooperation between states to combat cyberattacks, and the lack of legislative frameworks and their implementation. Cyberattacks create unique challenges for law enforcement due to three main factors: first, the absence of territorial judicial boundaries in cyberspace; second, the lack of uniform laws governing these attacks globally; and third, the rapid and ongoing evolution of cyber threats. If countries do not address these interrelated factors, cybercriminals are likely to continue outpacing law enforcement efforts (Cade, 2012).

In this regard, we will examine three approaches to addressing cyberattacks at the international level by proposing distinct methods for their regulation. The first approach advocates for the application of universal jurisdiction over cyberattacks. The second approach calls for states to ratify national laws specifically targeting these attacks. The third and most realistic approach proposes the establishment of ICL for cyberattacks, enforced by an international court and supported by multinational task forces. Additionally, we will explore the legal regulation of cyberattacks, along with international and national efforts to address and respond to these threats.

3.1 Universal Jurisdiction over Cyber Attacks

Expanding the scope of universal jurisdiction to cover cyberspace is an appealing idea, but it presents several challenges. While it is crucial to focus on major crimes that are central to universal jurisdiction, extending this jurisdiction to include cyberattacks is particularly important. These attacks can reach a level of severity and heinousness comparable to other crimes that hold unique international significance, such as genocide and crimes against humanity (Kontorovich, 2004), Acts of extreme cyberterrorism could involve the complete dismantling of national financial security systems.

Even if universal jurisdiction permits a country to prosecute a defendant under a specific set of cybercrime laws, domestic court

systems may not be adequately equipped to manage the unique scale and complexity of such cases (Abu-Odeh., 2007).

A cybercriminal could launch an attack on a global network using a self-replicating virus that adapts to various computer systems and programs, making it challenging to pinpoint the exact nature and duration of the damage. Such an attack could result in millions of victims within the prosecuting country, as well as a continuous global impact.

This would strain a state's judicial resources, and there are few procedural mechanisms capable of effectively managing the scope and complexity of these legal proceeding (Rho, 2007).

Overall, granting states universal jurisdiction as the sole solution to combat cyberattacks is impractical, although this approach acknowledges several important considerations. It highlights the significance of deterrence in preventing attacks by potential cybercriminals and rightly suggests that universal jurisdiction has a role in broader efforts to address cyberattacks.

3.2 National Compliance with International Cybercrime Treaties

The establishment of broad, multinational treaties grounded in traditional concepts of territorial sovereignty offers a solution for addressing cyberattacks at the international level. These treaties can lay the foundation for setting standards and developing customary international law (Weber, 2003).

For instance, both State (A) and State (B) may criminalize the same cyber activity under a cyber-attack treaty to which they are parties, yet they may differ in their approaches to addressing such an attack (Miquelon-Weismann, 2005).

State (A) may swiftly implement universally agreed legal standards, but the effectiveness of its efforts could be hindered by the delays in State (B)'s legislative process (Weber, 2003, p. 428).

In such instances, cooperation between Member States would continue to face challenges, particularly in areas such as evidence exchange, extradition, or the enforcement of sentences (Lentz).

Ultimately, for such treaties to be effective, they must ensure universal participation and include binding provisions outlining the rules and procedures that states must follow when enacting their legislation (Cade, An Adaptive Approach for an Evolving Crime: The Case for an International Cyber Court and Penal Law, 2012).

However, states would likely reject such a stringent treaty, and even if they agreed to sign and ratify it, they might undermine its value by including numerous reservations that exempt them from stricter provisions. As a result, while the multinational treaty could serve as an important first step in mobilizing international efforts to combat

cybercrime, it would ultimately fail if it relied entirely on local procedures for enforcement.

3.3 Jurisdiction at the International Tribunal

The most promising approach to preventing and prosecuting cybercrime combines the use of universal jurisdiction with multinational treaties, while also taking the further step of assigning jurisdiction over international cybercrime law to an international judicial body. By granting jurisdiction over cybercrime to an institution such as the ICC, the international community can ensure that the authority to define and establish criteria will rest with a single entity capable of adapting to the continuously evolving nature of cybercrime (Cade, An Adaptive Approach for an Evolving Crime: The Case for an International Cyber Court and Penal Law, 2012).

The Cybercrime Convention, with its effort to establish a set of global definitions and its expanding list of member parties, serves as a crucial starting point for drafting an international penal law for cybercrime and cyberattacks. As explained by Amalie M. Weber in her article "Council of Europe Convention on Cybercrime," the value of creating such a law lies in its adaptability: (It can be more easily amended as technology evolves, allowing states to better maintain consistency between their legislative schemes and statutes) (Weber, 2003, p. 445).

Finally, the development of such a model law could offer better solutions to the judicial challenges posed by legislation related to cybercrime. A detailed and specific penal law for cybercrime would also help address many of the definitional inconsistencies currently present in existing legal systems (Chibueze, 2006).

The structure of the ICC provides an ideal model for an international court or body with jurisdiction over cybercrime for at least four compelling reasons. First, the ICC's ability to engage with various criminal actors is already supported by international (though not universal) sanctions. Therefore, as long as either the cybercriminal or the victims are nationals of a state party to the Rome Statute, the ICC may have jurisdiction over the case. The historic creation of the ICC by the international community, with its novel scope and judicial structure, suggests that establishing a similar court focused on cyberattacks is a feasible possibility. Second, the principle of complementarity and the focus on only the most serious international crimes, as exemplified by the ICC, would allow States to maintain jurisdiction over less severe cybercrimes or those affecting only domestic actors. This would apply to cases involving large populations spread across multiple countries, as well as heinous crimes, terrorist acts, or cyberattacks that occur exclusively within

national borders (Cade, An Adaptive Approach for an Evolving Crime: The Case for an International Cyber Court and Penal Law, 2012, pp. 1171-1172).

Third, an international cybercrime court, similar to the U.S. Supreme Court, would have the authority to offer formal, definitive interpretations of international penal law, enabling it to quickly adapt to technological advancements.

If a cybercriminal exploits new technology to commit an unlawful act in a previously unimaginable manner, the court would play a pivotal role in interpreting international cyber sanctions laws to determine whether the offender's actions align with the international community's definitions of criminal conduct (Harding, 1999).

Fourth, the provisions of such a court would be enhanced by the pre-existing multinational cybercrime task forces, which could serve as the enforcement mechanism that the court itself lacks (Cade, An Adaptive Approach for an Evolving Crime: The Case for an International Cyber Court and Penal Law, 2012, p. 1172).

However, the implementation of this proposal faces at least three major obstacles: (Cade, An Adaptive Approach for an Evolving Crime: The Case for an International Cyber Court and Penal Law, 2012, p. 1173) First, states are likely to be reluctant to surrender their sovereignty to an international body. While some may argue that placing authority over cybercrimes in an international court may not be an extreme step—given the increasing involvement of non-state and multi-state entities, as well as the development of transnational public law, which has already blurred traditional jurisdictional boundaries—granting full regulatory authority to an international cybercrime court would represent an unprecedented shift in international law.

This change may prove difficult for many sovereign states to accept. Second, significant efforts will be required to draft an international penal law and establish a treaty for an international court with specific authority to adjudicate cybercrime cases. As discussed earlier, the lack of uniformity in definitions of cybercrime and the slow pace of treaty development will make the creation of such legal instruments a challenging process. Third, the new international tribunal will depend on independent states for enforcement and funding, necessitating the establishment of a mechanism to ensure cooperation between states (Posner, 1996).

3.4 International and National Initiatives for Addressing Cyber Attacks

At the international level, several efforts have been made to address cyberattacks, including the "Arab Convention on Combating

Information Technology Offences" of 2010. This initiative is part of the ongoing efforts by the League of Arab States to enhance security measures and combat information technology-related crimes, in alignment with legal foundations and the broader legal environment. One of the most significant international efforts to combat cyberattacks is the Council of Europe's "Budapest Convention on Combating Cybercrime," which entered into force on July 1, 2004 .

At the national level, several countries have enacted laws to address cyberattacks. Sweden was the first country to introduce legislation on computer and internet crimes with the enactment of the Swedish Data Law in 1973, which focused on addressing computer-mediated fraud. Following this, the United States implemented laws related to the protection of computer systems between 1976 and 1985. In 2000, the U.S. Department of Justice also introduced a classification of computer crimes (Al-Mutairi, 2020).

In 1988, France incorporated computer crimes into its internal criminal laws, further advancing this in 1994 with the introduction of a new Penal Law that addressed the regulation of automatic data processing in Article 323, which consisted of four paragraphs. In the same year, the authority to investigate, take witness statements, and conduct inquiries into information-related crimes was granted to the Public Prosecution. In the UK, similar steps were taken, with the introduction of laws in 1982 aimed at combating forgery and counterfeiting through electronic and information technologies, followed by the Computer Abuse Law in 1990 (Taha, 2018).

Regarding legislation in Arab countries, Egypt, in response to the evolving internet landscape and transnational information crimes, took significant steps. In 2014, the President of Egypt issued Decree No. 276, approving the country's accession to the Arab Convention on Combating Information Technology Crimes, signed in Cairo on December 21, 2010.

Furthermore, the Prime Minister issued three key decisions: Decision No. 2259 of 2014, which established the Supreme Council for the Security of Communications and Information Technology Infrastructure ;Decision No. 1453 of 2015, which created the Higher Council for the Digital Society and defined its competencies; and Decision No. 994 of 2017, which relates to the implementation of decisions and recommendations by the Supreme Council for Cybersecurity .

In 2018, the Egyptian legislator enacted Law No. (175) to combat information technology crimes. Saudi Arabia has faced a significant number of cyberattacks, with information violations against the

country accounting for an average of 2.27 percent of total attacks (Abdul Rahman Hammouda, 2009).

The Prime Minister's Decree No. 79, dated 3/7/1428 AH, related to the Anti-Cybercrime Law, was issued and ratified by Royal Decree No. (M/17) on 8/3/1428 AH, corresponding to 8/3/2007, which established a system to combat information crimes (Al-Enezi, 2017).

The UAE, a leading nation in adopting technological advancements in line with its digital government strategy, introduced the UAE Cybercrime Law through Federal Legal Decree No. (34) of 2021. This law, aimed at combating rumors and cybercrime, came into effect on January 2, 2022 .

In Iraq, the draft "Anti-Cybercrime Law" is still pending approval by the Iraqi Council of Representatives. Consequently, Iraqi courts continue to address information crimes, such as electronic blackmail, under the provisions of the Iraqi Penal Law No. (111) of 1969.

Conclusion:

In our research titled "Criteria of Relative Gravity for Determining Cyber-Attacks as Serious Violations," we identified key findings and recommendations to enhance international law and combat cybercrime.

We emphasize that assessing relative gravity involves both quantitative and qualitative criteria, including the intent behind crimes, the extent of damage caused, and the perpetrator's identity. This comprehensive approach helps identify the most serious violations and classify them as international crimes.

We highlight the necessity for clear criteria regarding cyber-attacks, which present unique challenges due to the lack of territorial boundaries and the evolving nature of threats. Collaboration between national and international legal systems is essential to address behaviors that threaten fundamental rights. The concept of "universal jurisdiction" is vital in preventing safe havens for perpetrators and enforcing international law. We recommend amending national laws, such as Article 13 of the Iraqi Penal Law, to classify cyber-attacks as serious crimes. This would ensure accountability for perpetrators at both national and international levels.

Finally, establishing an international court for cybercrimes, akin to the International Criminal Court, is crucial. This court would standardize definitions and criteria, fostering a unified international penal law for cybercrimes and addressing inconsistencies in national legal systems.

Bibliography

5. Abdul Rahman Hammouda. (2009). *Combating Information Crimes (Analytical Study).* Riyadh.

6. Abu-Odeh., L. (2007). A Radical Rejection of Universal Jurisdiction. *116 YALE L.J. (Pocket Part)*, 715.
7. Al-Enezi, K. A. (2017). *Cybercrime and its Impact on the National Economy (A Comparative Study).* Faculty of Law Cairo University.
8. Al-Husseinawi, A. J. (2009). *Computer and Internet Crimes.* Amman: Al-Yazuri Scientific Publishing House.
9. Al-Momeni, N. A. (2001). *Information Crimes.* (2. Edition, Ed.) Lebanon: Dar Al-Thaqafa for Publishing and Distribution.
10. Al-Mutairi, K. Z.-S. (2020). *Confronting Information Crimes in the Light of Contemporary Criminal Legislation and International Conventions.*
11. Al-Rawi, R. F. (2021). Legislative Shortcomings in Confronting Cyber Attacks. *Published Research Journal of the College of Law Legal and Political Sciences, 10*(39), 195.
12. Andres, S. J. (2011). State Responsibility for Cyber Attacks: Competing Standards for a Growing Problem. 982.
13. Brenner, J. (2011). *America The Vulner-able: Inside the New Threat Matrix of Digital Espionage, Crime, and Warfare.* New York: Penguin Press.
14. Cade, N. W. (2012). An Adaptive Approach for an Evolving Crime: The Case for an International Cyber Court and Penal Law. *Brooklyn Journal of International Law, 37*(3), 1147.
15. Cade, N. W. (2012). An Adaptive Approach for an Evolving Crime: The Case for an International Cyber Court and Penal Law. *Brooklyn Journal of International Law, 37*(3), 1170.
16. Chibueze, R. O. (2006). *The ICC: Bottlenecks to individual criminal liability in the Rome statute.*
17. DeGuzman, M. M. (2013). The ICC's Gravity Jurisprudence AT Ten. *WASHINGTON UNIVERSITY GLOBAL STUDIES LAW REVIEW, 12:475*, 478.
18. Dias, T. D. (4 April 2018). *"Propaganda and Accountability for International Crimes in the Age of Social Media: Revisiting Accomplice Liability in International Criminal Law.* Opinio Juris.
19. Greco, G. (2020). CYBER-ATTACKS AS AGGRESSION CRIMES IN CYBERSPACE IN THE CONTEXT OF INTERNATIONAL CRIMINAL LAW. *European Journal of Political Science Studies, 4*(1), 41.
20. Harding, C. (1999). *The international and European control of crime.* in Renegotiating Westphalia.
21. Heller, K. J. (2010). *Situational Gravity Under the Rome Statute in Carsten Stahn and Larissa van den Herik (eds.) Future Perspectives in International Criminal Justice.* The Hague T.M.C. Asser Press.
22. Klanter, Z. E. (2016). *International Responsibility Arising from Cyber Attacks.* Master's Thesis Faculty of Law University of Kufa.
23. Kontorovich, E. (2004). The Piracy Analogy: Modern Universal Jurisdiction's Hollow Foundation. *45 HARV. INT'L L.J. 183*, 205-206.
24. Lentz, C. E. (n.d.). *A State's Duty to Prevent and Respond to Cyberterrorist Acts.* 10 CHI. J. INT'L L.

25. Longobardo, M. (2016). *Factors relevant for theAssessment of sufficient gravity in the ICC proceeding and elements of international crimes Longobardo.* University of forward thinking Westminster.
26. Macauley, E. D. (2013). *The Use of EO Technologies in Court by the Office of the Prosecutor of the ICC in Ray Purdy and Denise Leung (eds.).* (E. f. Satellites, Ed.) Leiden, Nijhoff.
27. Marco Roscini., M. (2019). Gravity in the statute of the international criminal court and cyber conduct that constitutes instigates or facilitates international crimes. *criminal law forum*, 257.
28. Miquelon-Weismann, M. F. (2005). *The Convention on Cybercrime: A Harmonized Implementation of International Penal Law: What Prospects for Procedural Due Process?* 23 J. MARSHALL J. COMPUTER & INFO. L.
29. Posner, R. A. (1996). *The federal courts: challenge and reform.*
30. Rho, J. J. (2007). Comment lackbeards of the Twenty-First Century: Holding Cybercriminals Liable under the Alien Tort Statute. *B, 7 CHI. J. INT'L L*, 715.
31. Roscini, M. (2019). Gravity in the statute of the international criminal court and cyber conduct that constitutes. 256.
32. Saxon, D. (2016). Violations of International Humanitarian Law by Non-State Actors during Cyberwarfare: Challenges for Investigations and Prosecutions. *21 Journal of Conflict and Security Law*, 564.
33. Schabas, W. A. (2008). Prosecutorial Discretion v. Judicial Activism at the ICC. *Journal of International Criminal Justice*, 740.
34. Shackelford, S. J. (2009). From Nuclear War to Net War: Analogizing Cyber Attacks in International Law. *Berkeley Journal of International Law*, 204.
35. Taha, A. F. (2018). *Crimes Committed Online.* Faculty of Law Cairo University.
36. Warden, A. A. (2014). *The 2013 Salzburg Workshop on Cyber Investigations: An Overview of the Use of Digital Evidence in ICCs.* Digital Evidence and Electronic Signature Law Review.
37. Weber, A. M. (2003). *The Council of Europe's Convention on Cybercrime,.* 18 BERKELEY Tech. L.J.
38. William A. Owens, K. W. (2009). *Technology, Policy. Law, and Ethics Regarding U.S Acquisition and Use of Cyberattack Capabilities.* Washington: The National Academies Press.