ISSN (Online) 3134-884X

Advanced Research Journal of Computer Science

Received: March 07, 2025 | Accepted: June 14, 2025 | Published: June 30, 2025
Volume 02, Issue 01, Pages 05-13

DOI https://doi.org/10.66590/arjcs2025020102

Reviewing Organized Cybercrime: A Global Perspective on Cybersecurity Challenges

Muna Radhi[1*], Abdul Hussien[2] and Yasmin Hussain Mohialden[3]
[1-3]Department of Computer Science, College of Science, Mustansiriyah University, Baghdad, Iraq

Author Designation: [1]Professor, [2,3]Assistant professor

*Corresponding author: Muna Radhi (e-mail: muna.ali@uomustansiriyah.edu.iq).

How to Cite the Article:
Radhi, Muna, *et al*. "Reviewing Organized Cybercrime: A Global Perspective on Cybersecurity Challenges." Advanced Research Journal of Computer Science, vol. 2, no. 1, 2025, pp. 05-13. https://doi.org/10.66590/arjcs2025020102

Abstract | Despite the difficulty in defining crimes such as cybercrime and organized crime, the international community has not determined a simple method for measuring these new offenses. This is due to their inability to limit and control the characteristics of these new crimes to acquire comprehensive data. This could be due to the different perspectives on crime held by wealthy and developing nations, each with distinct economic and financial interests. The advancement of technology has resulted in the development of new instruments, inventions and services in various fields. Due to technological transformation, a new type of transaction has emerged: electronic transactions. In terms of occurrence and operation, they differ from traditional commerce. As nations conduct more business with one another and their economies become more globalized, culture and crime have also become more globalized. This has resulted in the emergence of dangerous organizations that operate on a global and organized scale, cross international borders and extend across multiple nations. They employ specific plans and partnerships between criminal groups from various nations to gain control of other countries. Cybercrime has become a natural phenomenon due to the increasing prevalence of electronic and third-generation services. The number of crimes has increased from a smattering to thousands. Most of these crimes involve intimate matters, making individuals more susceptible. Under the guise of technology, fraud, defamation, identity theft and extortion are among the offenses that have entered Iraqi society. These are brand-new crimes with fictitious motives, but their victims are genuine individuals who have suffered financial losses. Therefore, we have chosen to compose this paper to explain the nature and implications of electronic crime. It seeks to draw the attention of law enforcement officials to this new social phenomenon in the field of crime, highlight its risks and losses and increase public awareness of this form of corruption so that individuals can be cautious. This research will examine the significant obstacles nations confront in this field. Despite the difficulty of defining crimes such as electronic and organized crime, the international community has not arrived at a precise method for measuring these new offenses. They could not restrict and control the characteristics of these new crimes to compile them exhaustively. This research paper will examine organized electronic.

Key Words Organized Crime, Social Media, Emerging Crime, Cybercrime, Cyber Extortion, Cybersecurity, Cybercriminal Networks, Cybersecurity Challenges

INTRODUCTION

The world has become more economically, socially and technologically advanced, which has led to a considerable rise in wealth and changes in the global system. This has changed how crimes are planned, carried out and committed and who commits them. Corruption is no longer limited to one area or country; it has spread to many countries, making it easier for criminals to operate. These actions include committing crimes in unusual ways because of better organization and planning, the vast profits these organized groups make and the harmful effects on countries where these crimes happen, which spread to most parts of the world.

Studying organized crime is important because it threatens nations and the world needs to join against it. It is no longer possible for a single country to fight crimes that affect its sovereignty and powers alone. As a result, governments worldwide have developed a set of rules and

procedures to fight organized crime by having conferences and making international agreements. This study will look into organized crime, cybercrime and the definition of organized crime in Arab law. Several stories have been shared. Dr. Mohammed Farouk Al-Nibhan says organized crime is "created by material civilization to help criminals reach their criminal goals in a way that the law cannot follow because of its surroundings" [1,2].

In Western law, Dr. Grisi explains what organized crime is. R. Donald says organized crime is committed by "a person who holds a position in a work based on division and is dedicated to committing the crime." Some people think that this definition means that organized crime comes from two things: the existence of a criminal group and the intent to commit a crime.

Organized crime started long ago, but it was not illegal until recently. This is because economic and technological changes have made committing crimes easier, not just in one place or country. Organized crime started when criminal gangs tried to take control of the city through their illegal activities.

Some examples of organized crime include:

- Italian Mafia: It started in Italy and its actions have slowed
- In Japan, Yakuza gangs mainly dealt with guns, drugs and money laundering. Colombian gangs were involved in drug trafficking
- Alcohol-smuggling gangs in the U.S., Nigerian crime organizations and Chinese triad groups

These gangs quickly started doing more and more illegal things at a faster pace. This happened during the communications and transportation revolutions and the growth of the global economy. It let them move their actions to other countries or gave them a legal front, such as money laundering. It is well known that most organized crimes can be punished locally under the criminal and penal laws of the country where they were committed. For example, drug trafficking, helping minors get involved in prostitution, human and arms trafficking and laundering money were all crimes that could be punished locally before the idea of organized crime came about, even before these crimes moved from a local framework to an international and global one [3]. Since the fall, man has been linked to crime and criminality. Cybercrime is characterized as crimes performed online using a computer as a tool or a specific target. It is highly challenging to categorize crimes into discrete groups because many offenses change every day. Crimes like rape, murder and theft don't always have to be committed in isolation, even in the real world. It just depends on which of the two is the primary target whether the victim is the computer or the person operating it. Therefore, for the purpose of simplicity, the computer will be viewed as either a target or a tool. For instance, hacking entails assaulting the data and other resources on the computer. It is crucial to remember that overlap happens frequently, making it hard to establish a precise classification system [3-5]. In the age of globalization, the word "crime" is one that we frequently hear. Crimes include any infraction of the law or the performance of an unlawful act. Cybercrime has generated a great deal of discussion over the past 20 years in a variety of contexts. It is obvious that the internet's explosive growth has given rise to unheard-of new avenues for offense. It is defined as crimes carried out online that either use a computer as a tool or a sapecific victim [6,7].

The Concept of Organized Crime

Organized crime refers to crimes committed by groups of people in a hierarchy. Their goal is to make money through legal and illegal violent and intimidating actions beyond the state's borders. This type of crime has happened worldwide, making people worried about the risks and effects it could have on countries.

It is a dangerous organization with a significant impact and a wide range of people engaged. High coordination, flexibility in operations, planning crimes ahead of time, adaptability in carrying them out, continuity, secrecy, use of violence and bribes, involvement in illegal activities, making fake profits and recruiting and gathering members are all signs of a well-managed organization. They have a strong and authoritative leader and this group needs help from people who know about management, economics and sometimes politics.

Regarding the quality and nature of its activities, namely organization, it shows signs of skill, continuity and the use of violence to achieve organized crime goals beyond a single state's borders. One of its main goals is to make money, get benefits and build alliances with other groups through promises and agreements. The effects of this crime are significant and insufficient on national, foreign and even personal levels. The results can be economic, social, or financial. This crime includes money laundering, which is banned because of a United Nations Convention from 1990 and the Palermo Convention from 2000. Article 6 of the latter clarified that this was a global crime, as was human trafficking, which made the third-most money after drug and gun trafficking. The openness of the economy, the speed of transportation and the ease of contact have all made it easier for this crime to happen and attracted many people to join criminal gangs. To make this crime less dangerous, get rid of it and make it harder for people to join, it is essential to find and arrest gang leaders, give money to people who report crimes, protect people who leave criminal gangs and work with specialized security agencies on investigations. Also, reducing punishment is essential so that they can use knowledge and make the most of modern communication and the Internet to stop this crime. The United Nations Security Council has passed many decisions to support global and local cooperation against terrorism and transnational organized crime. Two

keys (2462 and 2482 of 2019) said international organized crime could help terrorist groups raise money.

Lastly, through Legislative Act No. 20 of 2007, Iraq signed the United Nations Convention against Transnational Organized Crime and its related protocols. This is an essential tool for fighting international crime [8].

Elements of Organized Crime

According to general principles of crime, for a crime to occur, whether it is material or moral corruption, there must be two essential elements: the material and the righteous.

These elements are necessary to hold the person responsible for their actions that violated an interest or right protected by the law.

Material Element

The material part of a crime is what makes it happen in the real world rather than being just an idea in someone's mind. This means that a crime, in general, is the behavior of a person or a specific action that harms legal rights and interests. The material part of a crime is how it appears from the outside, so every crime must involve material things that embody the criminal intent of the perpetrators.

To prove the material element of a crime, the offender must commit a specific criminal act. For some crimes, this act may be sufficient to satisfy the law. For other crimes, the law may also require a harmful, illegal result and there must be a link between the criminal act and the criminal development [9].

Moral Element

This refers to general and specific criminal intent, so the offender must intend to commit the material criminal act. Actions must be taken by sane, responsible adult who is aware of what they are doing, excluding youth, the insane and those who commit crimes in good faith.

Organized crime is intentionally committed because the general criminal intent is based on knowledge and will.

This is evident when a criminal organization is established to commit a serious crime.

Knowledge: Every member of a criminal organization must know what the organization is and that it was established to commit a specific crime. They must also know that unlawful activity or severe crime is illegal and can get them into trouble.

As for the will, the member's choice must focus on being part of the criminal organization, which should focus on committing the crime in question. As for specific criminal intentions, the purpose of starting a criminal organization is to make money, so the reason for starting a profitable organization is organized crime.

Specific criminal intent is fundamental to distinguishing between terrorist, political, racial, religious and organized crimes across nations.

Types of Organized Cybercrime Groups

In 2012, it was reported that about 80% of cybercrimes could be attributed to some form of organized activity. Scientists have identified six basic organizational patterns of cybercrime. However, they noted that the classification of organized cybercrime groups will likely change as the digital environment evolves [10-15].

Type 1: Groups operate exclusively online and are predominantly "virtual," while trust is evaluated through reputation in illicit online activities. This category includes two subtypes: Swarms: Swarms appear as "leaderless, loosely organized entities with a common goal." They are types of networks with minimal leadership chains, primarily acting online. Swarms may operate in viral forms reminiscent of previous "hacktivist" groups. They are more active in ideologically driven online activities (such as hate crimes and political resistance). An example of an anonymous group is a typical swarm.

Hubs: Hubs are also primarily active online but have a higher degree of organization than swarms. They involve a central point (intersection) where core criminals gather, surrounded by associates. Their activities are highly diverse, including phishing attacks, botnets, online sexual crimes, etc., all happening online. An example of a hub-type cybercriminal group is Silk Road 2.0, an online marketplace for illicit goods like drugs.

Type 2: Groups operate online and offline and are described as "hybrid." This category can also be divided into two subtypes: clustered hybrids and extended hybrids.

Clustered hybrids are criminal activities a small group commits using specific activities or methods. Clustered hybrids resemble hubs in their structure but fluctuate between online and offline criminal activities. Their activities are profit-driven. An example of an evolved hub/internet criminal hybrid organization was presented by Chabinsky, a representative of the Internet Department of the U.S. Federal Bureau of Investigation, in his speech. He mentioned programmers creating malware, exploits and other tools necessary for committing crimes. Distributors trade or sell stolen data and credentials provided by other specialties. Technicians maintain the criminal infrastructure and supporting technologies. Hackers search for security vulnerabilities in applications, systems and networks and exploit them to gain administrator access or disclose payroll. Fraud specialists develop and employ social engineering schemes, including phishing, spamming and domain crowding. Hosts provide "safe" facilities for illicit content servers and websites. Cashiers control escape accounts and provide these names and accounts to other criminals for a fee. They also typically manage individual cash mules, or "money mules," who transfer the proceeds from their committed fraud operations to a third party for further laundering into financial instruments. Cashiers assist in the conversion and laundering illicit proceeds

through digital currency services and between different national currencies. Executive managers set goals, recruit members, assign them to the abovementioned tasks and manage the distribution of crime proceeds.

Extended hybrids operate similarly to clustered hybrids but are less centralized. They usually involve multiple affiliates and subgroups and engage in a variety of criminal activities while still maintaining a sufficient level of coordination to ensure the success of their operations. The level of coordination depends on the complexity of the operation. Their activities are also profit-driven.

Type 3: Groups operate offline but utilize internet technology and cyberspace to facilitate offline activities. They increasingly contribute to digital crime and can be divided into "hierarchical sequences" and "aggregates" based on their level of organization and cohesion.

Hierarchical sequences are organized criminal groups that export some of their activities online, using the Internet to support or expand their offline activities. Examples include online gambling, extortion and the online transmission of prostitution (such as pornography, webcam services, etc.).

Aggregates are loosely structured, temporary groups, often with unclear objectives. They utilize specialized digital techniques. For example, the use of BlackBerry Messenger to coordinate public disorder during the 2011 U.K. riots and the Sydney riots in September 2012, where 18 similar incidents occurred. Additionally, the organized cybercrime group can be further classified, concerning purpose criteria, into two other subtypes.

Online Crime Activities and Their Impact on Society

Below are some crime activities and their impact on society [16-18]:

Online Drug Trade

E-commerce has evolved as a significant marketing process between Businesses (B2B), Business-To-Customer (B2C) and sales approaches. It offers several advantages compared to traditional retail sales, such as overcoming geographical limitations, low cost, speed in reaching the market, direct customer targeting and a broader customer reach. With the digital shift, pharmaceutical companies are taking a step back and reevaluating everything they do, from internal systems to online and in-person customer interactions. E-commerce is available in various formats, including branded websites, mobile applications, marketplaces like Amazon and eBay and social media platforms like Facebook Marketplace, Instagram Shoppable Ads and Pinterest Buyable. Most social media platforms have their marketplace where traders can directly sell products to customers without following the necessary guidelines and permissions. These underlying systems lack adequate mechanisms to verify the source and authenticity of the products. Criminals and counterfeiters see it as an opportunity to sell fake drugs to customers by offering attractive prices and dispensing without a prescription. Drug counterfeiters use online tools to identify customers' locations based on internet search records, trends and health conditions. There is a need for strong regulation of drug sales on social media and the dark web, which can impose severe penalties on criminals and counterfeiters [19].

Online Money Laundering

Online Social Networks with virtual currencies (OSNs) have become increasingly important in facilitating various financial activities, such as money exchange, online shopping and earning money through gaming.

Often, users purchase virtual currency using real money. Attackers want to do this because they can create many accounts to collect money (virtual currency) through illicit or unlawful means with minimal investment, launder the obtained funds and then use the virtual cash to earn significant profits.

Such attacks result in significant financial losses for the victims and harm the business ecosystem. For this reason, it is crucial to identify malicious OSN accounts engaged in activities like online money laundering.

To do so, closely examine how each behaves based on operational information gathered from Tencent Q.Q., one of the world's largest Online Social Network (OSN) platforms. Multiple features are created to identify accounts from three perspectives: feasibility, transaction sequencing and spatial linkage between stories [20].

Human Trafficking and Slavery via the Internet

Most anti-trafficking policies discuss it in terms of the crime itself, "illegal" migration, being a victim and assisting individuals. This narrow focus is ineffective in addressing how technology and trafficking interact and combat trafficking. There is a need for an in-depth analysis of the levels of interaction between technology and human trafficking and an understanding of how they work together [21].

New legal and regulatory challenges arise as technology globally permeates every public and private life aspect. The increasing dominance of unregulated global technology companies and social media platforms raises significant concerns for lawmakers and international and national regulators dealing with health, safety and security issues such as online exploitation, digital harassment and violence, online human trafficking and sexual exploitation, particularly affecting vulnerable populations living in conflict areas.

Additional issues revolve around biases and programmed discrimination in artificial intelligence and how global technology companies and social media platforms utilize powerful algorithms to expand their international audience without possessing the necessary technological linguistic proficiency to enforce their community standards that prohibit hate speech, illegal content and illicit activities on their platforms.

While social media has its benefits, it can also facilitate crimes such as cyber exploitation, sexual terrorism and online human trafficking, which harm socially marginalized and economically disadvantaged individuals, especially women and children. This article in the field of law focuses on the relationship between cyber exploitation, slavery, sexual torture and online human trafficking on global technology platforms and social media and its connection to terrorist financing, with a detailed discussion of what has happened to Yazidi women, children and other religious and ethnic minorities during the rise of the Islamic State in Iraq and Syria (ISIS).

This legal article also explores the legal frameworks in the United States, Europe and Iraq that may allow victims of cyber exploitation to pursue criminal and civil accountability against corporate entities [22].

What are Computer-Based Crimes?

"Pure" cybercrimes can only be committed through the Internet. Using a computer, computer network, or any other form of Information and Communication Technology (ICT), examples of such actions include hacking and distributed Denial-of-Service (DDoS) attacks. Here are some explanations of what these terms mean:

These activities target computer devices or network resources but can also have various other effects. For example, information gathered through email account breaches can later be used for fraud. This chapter focuses solely on electronic crimes in their simplest forms: crimes "against" computers and networks.

The most common types of crimes that computers are subjected to include:\Malware: Malicious software is a general term for harmful programs that can spread from one computer to another, hindering the operation of computer devices. Malware can be destructive, such as deleting files or causing system "crashes," but it can also be helpful, as it is used for stealing personal data. Malware comes in various forms, with viruses being one of the most well-known. Viruses can cause minor issues on computers, but they can also have more severe effects on devices, software, or files by either breaking or deleting them. They can achieve more by spreading from one computer to another. They need a place to reside (like a file, disk, or spreadsheet) to act as a carrier on the computer, but they cannot infect a computer unless someone runs or opens the virus-infected file.

Worms: Worms are also self-replicating programs, but they can spread themselves among computers and within them without any action taken by a person or host. For this reason, worms can cause more significant damage than viruses and destroy networks. Worms can also deliver Trojan horses into the network system.

Trojan Horses: Trojan horses are malware that appears to be genuine software but is harmful and enables unauthorized access to a computer. They can steal information without the user's knowledge and deceive users by performing legitimate actions while carrying out hidden and unauthorized activities.

Spyware: Spyware is a program that violates user privacy by collecting private or personal information from infected systems and monitoring visited websites. The collected data can then be sent to other individuals. Spyware is sometimes hidden within adware (free programs that sometimes require you to view ads to use them) or unwanted software.

These are Just a Few Common Types of Electronic Crimes

Keylogging: Keylogging software records and sends keystrokes performed on a computer, making obtaining sensitive information such as passwords or banking account details possible. One type of spyware takes screenshots of the victim's computer. Spyware is one of the most dangerous types of malware, as its sole objective is to invade privacy.

Hacking: Hacking is a method of unlawfully accessing or gaining unauthorized entry to computer systems or network resources by taking advantage of security vulnerabilities. Through hacking, you can: Obtain information about individuals that criminals can exploit.

Deface Websites: Be used in Denial of Service (DoS) or distributed denial of service (DDoS) attacks. Distributed Denial of Service (DoS and DDoS) attacks involve sending many requests to Internet servers, overwhelming them and preventing them from responding quickly enough. This can lead to significant server overload, freezing, or disruption.

Spam: Spam refers to unsolicited or "junk" email that is typically sent in large quantities to many individuals. It occurs worldwide and is often associated with drugs or pornography. (Random email messages can also be used to send phishing emails or malicious software, increasing the potential return for criminals).

Botnets: Botnets refer to groups of computer devices infected with malware. They are used to automatically and repeatedly send spam, deceptive, or malicious traffic to specific targets. They are often called "zombies" because a "botmaster" or "controller" manipulates the networks from a single location.

Electronic Extortion Crime against Women

The variety and increased use of social media in various aspects of life have contributed to the rise of electronic crimes, especially electronic extortion, which has become a dangerous threat to Iraqi families, leading to numerous family problems. Notably, no legislation has been enacted in Iraq to regulate this type of crime, despite its prevalence and the weak performance of responsible authorities in disclosure and investigation. The Iraqi legislature had proposed including provisions related to information crimes in the Information Crimes Law Bill of 2011, but it has not been enacted. This issue must be

addressed and the Iraqi courts continue to apply the provisions of the Iraqi Penal Code No. 1 and the Code of Criminal Procedure No. 1 concerning extortion crimes.

As a result, Iraqi judges still have jurisdiction over cases involving perpetrators of extortion crimes. The legislator needs to expedite the enactment of the Information Crimes Law and distinguish it from the existing provisions that address crimes related to it.

Previous Studies on Electronic Extortion in Iraqi Society

A study by Al-Anzi *et al*. [16] demonstrates the effectiveness of public relations with electronic extortion and the impact of extortion on public relations. It highlights the dangerous nature of this crime due to its implications for human pride, leaving individuals vulnerable to attack. Electronic extortion is a new crime that threatens the security and safety of society by placing individuals in psychological and social conflicts, pressures and threats. This implies that the public needs social and legal awareness about dealing with virtual means and regulating online relationships, especially among college students who are likely to be victims.

The researcher utilized survey methods and various scientific tools such as questionnaires, participant observation and interviews. The sample consisted of 100 male and female students randomly selected from an Iraqi university. The study revealed that the Iraqi Ministry of Interior could utilize public relations to address the issue of electronic extortion and that there are various types of public relations activities, including direct actions such as workshops, seminars and lectures, as well as indirect activities such as posters, advertisements and campaigns. Many had not been subjected to extortion when discussing electronic extortion with young people because they knew how to deal with it. This is because the youth have sufficient knowledge to prevent them from falling victim to this Kareem *et al*. [17].

The world has become a small village where everyone can buy, sell and access information and data in a fraction of a second. This has happened due to the speed at which technology has advanced.

Some people use this technology negatively to achieve cheap and evil goals that affect both the financial and ethical aspects. Extortion damages the unity and stability of society because it harms all social, economic and ethical aspects.

Given the importance of the subject in our Iraqi society, where extortion has become more common, the study addressed the nature of extortion, how it spreads, the psychological and social effects of extortion and how to deal with it.

We will also discuss the role of the family and the government in Iraqi society. Several interviews were conducted with individuals who resisted extortion. They were informed about actual cases and how to overcome them. The research concludes with a discussion of the results and some suggestions.

Reza *et al*. [18] discussed how to punish electronic extortion in Islamic and Iraqi law. It showed that electronic extortion is one of the newest crimes in our modern world, emerging after the advent of technology. However, it is not a crime that corrupts morals in society because it involves attacks on money and honor and seriously affects individuals and society.

But because Islamic law is a complete way of life, it has not left anything. Instead, it has gathered everything for the benefit of humanity in all aspects of life and protected the interests of individuals, society and what is in people's best interest. This includes maintaining order, establishing justice and fairness, combating corruption and punishing criminals and wrongdoers. For this reason, Islamic law has not left this crime unpunished and the law has also not escaped punishment [19].

In a letter sent to the Parliament in Baghdad on March 2, 2019, several Iraqi and international human rights and media groups strongly urged the Parliament either to eliminate the controversial Internet Law project or make significant changes. They stated, "We understand that there is a need for legislation on cybercrimes, but if this law is passed in its current form, it will be a serious setback for freedom of expression in Iraq and create an atmosphere of self-censorship in the country."

The groups that signed this letter were the Iraqi Journalists' Rights Defense Association, the Iraqi Network for Social Media, the Iraqi Observatory for Human Rights, the International Press Institute, Amnesty International and Human Rights Watch. In the joint letter, they said that the Information Technology Crimes Law, which was first read in Parliament in January 2019 and was similar to a draft law from 2011 that was "paralyzed" and later withdrawn, was particularly concerned about Articles 3, 4 and 6, which punish vague and imprecise actions that could fall under the right to freedom of expression with life imprisonment and hefty fines.

The letter states that the law defines crimes with vague or self-defined phrases that the government can use to persecute individuals exercising their rights under the Iraqi Constitution. The Iraqi Media and Communications Commission has recently been trying to pass the law. This comes after months of the Iraqi government shutting down the Internet in response to recent protests in Iraq's central and southern provinces. The world has become a small village where everyone can buy, sell and access information and data in a fraction of a second. This has happened due to the speed at which technology has advanced. Some people use this technology negatively to achieve cheap and evil goals that affect both the financial and ethical aspects. Extortion damages the unity and stability of society because it harms all social, economic and ethical aspects.

Given the importance of the subject in our Iraqi society, where extortion has become more common, the study addressed the nature of extortion, how it spreads, the psychological and social effects of extortion and how to deal with it.

Reza *et al*. [18] discussed how to punish electronic extortion in Islamic and Iraqi law. It showed that electronic extortion is one of the newest crimes in our modern world, emerging after the advent of technology. However, it is not a crime that corrupts morals in society because it involves attacks on money and honor and seriously affects individuals and society.

But because Islamic law is a complete way of life, it has not left anything. Instead, it has gathered everything for the benefit of humanity in all aspects of life and protected the interests of individuals, society and what is in people's best interest. This includes maintaining order, establishing justice and fairness, combating corruption and punishing criminals and wrongdoers. For this reason, Islamic law has not left this crime unpunished and the law has also not escaped punishment [19].

In a letter sent to the Parliament in Baghdad on March 2, 2019, several Iraqi and international human rights and media groups strongly urged the Parliament either to eliminate the controversial Internet Law project or make significant changes. They stated, "We understand that there is a need for legislation on cybercrimes, but if this law is passed in its current form, it will be a serious setback for freedom of expression in Iraq and create an atmosphere of self-censorship in the country."

The groups that signed this letter were the Iraqi Journalists' Rights Defense Association, the Iraqi Network for Social Media, the Iraqi Observatory for Human Rights, the International Press Institute, Amnesty International and Human Rights Watch. In the joint letter, they said that the Information Technology Crimes Law, which was first read in Parliament in January 2019 and was similar to a draft law from 2011 that was "paralyzed" and later withdrawn, was particularly concerned about Articles 3, 4 and 6, which punish vague and imprecise actions that could fall under the right to freedom of expression with life imprisonment and hefty fines.

The letter states that the law defines crimes with vague or self-defined phrases that the government can use to persecute individuals exercising their rights under the Iraqi Constitution. The Iraqi Media and Communications Commission has recently been trying to pass the law. This comes after months of the Iraqi government shutting down the Internet in response to recent protests in Iraq's central and southern provinces.

Characteristics of Cybercrime

Cybercrime consists of several elements, including:

- Crimes committed on or through the Internet
- The computer is the tool used to commit the crime
- Cybercrimes are indifferent to their location (domestic, international, or transnational)
- Cybercrimes are challenging to detect and prove (use of aliases, internet cafes, etc.) and do not leave a physical trace, as they can disappear within seconds [23]

Criminal Liability for Electronic Extortion on Social Media Platforms

Criminal liability for electronic extortion through social media platforms is a grave crime that affects individuals and society. Recent scientific advancements have led to the development of human communication methods, which have shortened time and effort and transformed the world into a small village. These communication methods are characterized by high quality and immense digital capabilities that have facilitated communication at all levels and brought dynamism and progress to human interactions. Social media platforms are a modern method that has brought about positive changes and significant advancements in human communication worldwide. Despite the numerous advantages of social media and its revolution to communities, some segments of society have not refrained from using these technologies to harm others, including through various crimes such as electronic extortion. The openness, lack of restrictions and widespread use of social media platforms have contributed to the proliferation of these crimes, turning electronic extortion into a phenomenon that penetrates Arab and Iraqi societies in particular, threatening their foundations and causing harm. One of the primary goals of any civilized society is to ensure the security of its individuals and make them feel safe in their lives. Due to the gravity of this crime, the Iraqi criminal justice system has attempted to keep up with developments in the criminal field, despite the absence of legislation explicitly criminalizing this type of emerging crime. It relies on general principles in Iraqi Penal Code No. 111, amended in 1969, to criminalize electronic extortion, consider it an explicit threat, impose criminal liability on the perpetrator and subsequently impose penalties [24-31]. The motivations behind internet-based crimes primarily revolve around personal profit or financial gain (e.g., using malware to access a bank account). Still, they can also take the form of protest and criminal damage (e.g., hacking and defacing a website). The functionality of the software or tools can mostly be used to deduce the motivations. Additional non-traditional motivations may also exist, according to some study, including sated curiosities or challenges, general hatred, retaliation, building respect and influence within online communities, or simply boredom.

Internet-based crimes can either target specific victims or are more randomly committed. For instance, viruses may disseminate widely and haphazardly infect numerous individuals. As shown in incidents like Stuxnet

and Flame2, advanced persistent threats and highly organized, sophisticated and lengthy attacks have a definite objective in mind, such as the destruction of infrastructure or the acquisition of comprehensive information about a person or group involved in cyberattacks. Overall, the landscape of cybercrime is still changing and as technology develops, new types of criminal behavior are probably going to appear. To address and deter cybercriminal actions, people, companies and governments must exercise vigilance, implement strong cybersecurity measures and implement suitable legislative frameworks.

CONCLUSION

We reviewed emerging organized cybercrime, stressing its nature, problems and ramifications. We examined the challenges of categorizing cybercrime and organized crime, emphasizing the lack of an easy way to measure these new acts. The international community struggles to manage these crimes, resulting in a lack of comprehensive data. The differing views on crime between wealthy and poor nations, driven by economic and financial concerns, make assessing these offenses more difficult. Due to technology, electronic transactions differ from traditional commerce in terms of occurrence and functioning. The globalization of culture and crime has led to the rise of organized and deadly multinational groups. These organizations work together to take over other nations.

Electronic and third-generation services have made fraud, defamation, identity theft and extortion more common. These crimes affect personal lives and expose victims to financial damage. The victims of these crimes are actual individuals.

Our research report sought to raise awareness of this emerging crime-related societal phenomenon among officials and the public. We stressed the need for extensive study and knowledge by underscoring the risks and losses of electronic crime. We also acknowledged the significant obstacles countries confront in this area. This research covered rising organized cybercrime, although other areas need more study. Research could focus on the following:

- **Legislative Framework:** Study international collaboration and effective legislative frameworks to combat organized cybercrime
- Analyze the issues policymakers and the legal community have in reacting to cybercrime's rapid evolution
- **Technological Solutions:** Discover new ways to identify, prevent and mitigate cyber-attacks. Explore how A.I., ML and big data can improve cybersecurity.
- **Global Collaboration:** Examine multinational collaborations and alliances to fight organized cybercrime. Evaluate transnational cyber threat mitigation strategies, including information-sharing networks and coordinated operations
- **Social Media and Cyber Extortion:** Study how social media platforms influence organized criminality, especially cyber extortion. Analyze cybercriminals' social media exploits and recommend mitigation techniques
- **Cybersecurity Awareness and Education:** Assess the success of cybercrime awareness efforts and instructional programs. Explore new ways to educate individuals, companies and policymakers on cyber threat risks and prevention

By examining these topics, policymakers, law enforcement and cybersecurity professionals can develop more effective tactics to prevent organized cybercrime.

REFERENCES

[1] Sdiri, K. "The crime of organized crime." *Al-Hikma Journal of Social Studies*, vol. 3, 7 Nov. 2015, pp. 251–267.

[2] Al-Nabhani, M.F. *Combating Crime in the Arab World*. Arab Mirror Publishing House for Security Studies, 1989.

[3] Mendel, P. "Human trafficking and online networks: Policy, analysis and ignorance." *Antipode*, Wiley Online Library, 2016.

[4] Khalil, S. "Cross-border organized crime." *National Criminal Journal*, vol. 44, nos. 1–2, Cairo, pp. 8–9.

[5] "Brief about Organized Crime." *Iraqi Forum 2014*. https://iraqi-forum2014.com.

[6] Dakhil, R.A. "Organized Crime and Corruption in Iraq." *Al-Adab Journal*, vol. 2, no. 89, 2009, pp. 491–514.

[7] Dreckley, F. and A. Hikmat. "Organized Crime and its Methods of Combating." *University of Iraq*, 2015, pp. 465–504.

[8] Zhou, Y. *et al*. "Analyzing and detecting money-laundering accounts in online social networks." *IEEE Network*, vol. 32, no. 3, May 2018, pp. 115–121.

[9] Medjahdi, K.M. *Mechanisms of International Cooperation in Combating Organized Crime*. PhD Thesis, University of Tizi Ouzou-Mouloud Mammeri.

[10] Salimah, Z. and B. Butraha. "Electronic crime: Foundations and concepts." *Journal of Social Science Development*, vol. 13, no. 1, 9 Nov. 2020, pp. 07–20.

[11] McGuire, M. and S. Dowling. *Cyber Crime: A Review of the Evidence*. Home Office Research Report, Home Office, London, 2013.

[12] Al-Obady, D.H.S.A. "The crime of electronic blackmail for women (A comparative study)." *Al-Anbar University Journal of Law and Political Science*, vol. 10, no. 2, 2020.

[13] Ashour, A.J. "Abstract: Criminal responsibility for the crimes of electronic blackmail on social media (A comparative study)." *Journal of Misan Research*, vol. 16, no. 31, 2020.

[14] Didier, E. *et al*. "Exploring legal accountability of global technology and social media companies for the cyber exploitation and online human trafficking of Yezidis and other minorities by ISIS." *Journal of Human Trafficking, Enslavement, Conflict-Related Sex and Violence*, vol. 3, no. 1, July 2022, pp. 4–44.

[15] Sarkar, S. "Online drug trade: A threat to the pharmaceutical industry." *International Journal of Advanced Research in Computer Science and Management*, vol. 10, May 2022, pp. 15–20.

[16] Al-Anzi, M.N.N. "The effectiveness of public relations in combating electronic blackmail." *Journal of Arts, Literature, Humanities and Social Sciences*, no. 55, Aug. 2020.

[17] Kareem, A. *et al*. "The spread of electronic blackmail phenomenon in Iraqi society: Survey of the Iraqi community's opinions on dealing with it." *Proceedings of Humanities and Natural Sciences Conferences*, no. 0, Apr. 2019. Accessed 11 Sept. 2022. http://proceedings.sriweb.org/akn/index.php/art/article/view/197.

[18] Reza, I. *et al*. "Effects of electronic blackmail as a punishment between Imami Jurisprudence and Iraqi Law." *Misan Journal of Academic Studies*, vol. 20, no. 41 AR, 2021. Accessed 11 Sept. 2022. https://www.iasj.net/iasj/article/229453.

[19] Nehme, T. *Impasse of Cyber Laws: Iraqi Case*. ABD, Rutgers University, 2020.

[20] Stanila, L. "New species of criminal phenomena: Organized cybercrime." *Journal of Eastern-European Criminal Law*, 2020, p. 17.

[21] European Commission. "Survey on Scams and Fraud Experienced by Consumers: Final Report." Jan. 2020.

[22] European Informatics. "Data Exchange Framework for Courts and Evidence: Overview of Existing Legal Framework in the E.U. Member States." 2015, http://s.evidenceproject.eu/p/e/v/evidence-ga-608185-d3-1-411.pdf. Accessed 26 Dec. 2020.

[23] Dashora, K. "Cyber Crime in the Society: Problems and Preventions." *Journal of Alternative Perspectives in the Social Sciences*, vol. 3, no. 1, 2011, pp. 240–259.

[24] Salman, Saba Abdulbaqi, *et al*. "Security attacks on e-voting system using blockchain." *Iraqi Journal for Computer Science and Mathematics*, vol. 4, no. 2, May 2023, pp. 179–188.

[25] Al-Tai, M. Haqi, B. M. Nema and A. Al-Sherbaz. "Deep Learning for Fake News Detection: Literature Review." *Al-Mustansiriyah Journal of Science*, vol. 34, no. 2, June 2023, pp. 70–81.

[26] Abdulhameed, A.A. *et al*. "Modeling web security analysis attacks with CySeMoL tool." *Al-Mustansiriyah Journal of Science*, vol. 31, no. 3, Aug. 2020, pp. 101–109.

[27] Wadhwa, A. and N. Arora. "A review on Cyber Crime: Major threats and solutions." *International Journal of Advanced Research in Computer Science*, vol. 8, no. 5, 2017.

[28] United Nations. *Ninth Congress on the Prevention of Crime and the Treatment of Offenders*. Cairo, Arab Republic of Egypt, 1995. Document No. 2/88CONF/E.1.

[29] Broadhurst, R. *et al*. "An analysis of the nature of groups engaged in Cyber Crime." *International Journal of Cyber Criminology*, vol. 8, no. 1, 2014, pp. 1–20.

[30] Lusthaus, J. "How Organised Is Organised Cybercrime?" *Global Crime*, vol. 14, no. 1, 2013, pp. 52–60.

[31] Leukfeldt, E.R. *et al*. "Organised cybercrime or cybercrime that is organised? An assessment of the conceptualisation of financial cybercrime as organised crime." *European Journal on Criminal Policy and Research*, vol. 23, 2017, pp. 287–300.