LEX LOCALIS-JOURNAL OF LOCAL SELF-GOVERNMENT
ISSN:1581-5374 E-ISSN:1855-363X
VOL. 23, NO. S5(2025)

CYBER EXTORTION: A LEGAL AND SECURITY PERSPECTIVE ON CONTEMPORARY CHALLENGES AND COPING STRATEGIES

D.Fathi Tawfiq Abed Alrahman Alfaouri [1]
Mohammad AbdAllah Alshawabkeh[2]

[1]University of Petra, Faculty of Law
Criminal Law
[2]Dhofar University

falfaouri@uop.edu.jo[1]
malshawabkeh@du.edu.om[2]

Research Abstract
This research addresses the crime of cyber extortion as one of the most serious crimes emerging in the digital space, seeking to examine it in light of the legal and security frameworks, with a focus on contemporary challenges and ways to address them. The research began by defining the conceptual framework of the crime, defining cyber extortion and distinguishing it from other similar crimes, then reviewing its most prominent forms and methods, which range from financial, emotional, and political extortion, based on evidence from practical experience.
The research also focused on the challenges facing legislators and security officials, from the inadequacy of legal texts and the difficulty of adaptation, to the dilemma of technical tracking, anonymity, and the complexity of cross-border crimes. It then moved on to explore ways of addressing these challenges through legal mechanisms, such as enacting advanced legislation, imposing harsher penalties, and strengthening international cooperation, as well as security and technical mechanisms based on monitoring, tracking, and developing digital protection tools.
The research concluded with a number of findings, most notably that cyber extortion is a multidimensional challenge—legal, security, social, and psychological—and that addressing it requires integration between legislation, security, technology, and community awareness. It also recommended updating national legislation to keep pace with technological developments, strengthening specialized security capabilities, intensifying awareness campaigns, and establishing psychological and legal support centers for victims.
The research thus seeks to present a comprehensive vision that makes cyber extortion a shared issue between the state and society, and pushes towards the formulation of more effective strategies to reduce its risks and preserve human dignity and security in the digital space.

Abstract
This research addresses the crime of cyber extortion as one of the most dangerous emerging crimes in the digital space. It provides a legal and security-oriented reading that highlights contemporary challenges and explores possible strategies for response. The study begins by defining cyber extortion and distinguishing it from similar offenses, then examines its most prevalent forms and methods, ranging from financial and emotional extortion to political blackmail, supported by real-life examples.
The research also explores the challenges faced by legislators and security agencies, including legislative gaps, difficulties in legal classification, challenges of digital tracing, identity concealment, and the complexity of cross-border crimes. It then discusses mechanisms of confrontation, focusing on legal measures such as enacting updated legislation, imposing stricter penalties, and fostering international cooperation, alongside security and technical measures including monitoring, tracking, and the development of digital protection tools.
The findings reveal that cyber extortion constitutes a multidimensional threat—legal, security, social, and psychological—and that addressing it requires integration between legislation, security, technology, and societal awareness. The study recommends updating national laws in line with technological developments, strengthening specialized security capabilities, intensifying awareness campaigns, and establishing psychological and legal support centers for victims.
In sum, this research seeks to present a comprehensive vision that frames cyber extortion as a shared responsibility between the state and society, and calls for more effective strategies to mitigate its risks while safeguarding human dignity and security in the digital sphere.

Introduction: In an age where cyberspace has become a natural extension of human existence, cyber extortion has emerged as a dark side of technological civilization, transforming technology from a tool for knowledge and communication into a means of domination and aggression against

human dignity. It is not a passing act, but rather the embodiment of the breakdown of values in the face of the savagery of modern media, and a weapon that threatens both individual and collective security. This type of crime is based on subjugating the human will through hidden threats and psychological pressure exerted from behind screens, turning security into anxiety, freedom into restriction, and privacy into a bargaining chip. Therefore, studying this issue is not an academic luxury, but a necessity dictated by the need to protect society from a danger that goes beyond individuals to affect the stability of the state. The problem lies in the inadequacy of traditional texts to prosecute cross-border crimes and the inability of security agencies to confront perpetrators who hide behind the mask of technology. Therefore, a comprehensive approach is required that combines strict laws, prudent security, and advanced technology to protect rights and deter criminals.

This research, therefore, does not stop at description, but delves into the essence of the phenomenon, analyzing its forms and dimensions, revealing its challenges, and proposing ways to address them, thereby contributing to legal and security thinking and raising a conscious cry against a crime that threatens the essence of human dignity in an era where cybersecurity has become synonymous with survival itself.

Research problem: The problem addressed in this research is the deep tension between the acceleration of the digital revolution and the unlimited virtual spaces it has created, on the one hand, and the inability of legislative and security systems to prosecute new crimes, foremost among which is cyber extortion, on the other. The danger of this crime stems from its unique characteristics, as it is practiced in an invisible world and relies on complex technical tools that make it difficult to track, allowing criminals to hide behind fake identities and cross-border networks.

The essence of the problem stems from the following central question: How can the legal and security system balance the protection of individual rights and the guarantee of community security in the face of cybercrime, which is growing and evolving at a rate that exceeds the capacity of traditional texts and regulations to accommodate?

Key questions:

- What is cyber extortion? How can it be distinguished from other forms of cybercrime?
- What are the most prominent means and forms of cyber extortion in today's world?
- What are the legislative shortcomings that hinder the effective legal response to this crime?
- How do technical and security considerations hinder tracking and monitoring efforts?
- What are the optimal legal and security measures to ensure effective protection for individuals and society in the face of this threat?

Importance of the study: The importance of this study stems from the fact that it addresses the crime of cyber blackmail, which is no longer just isolated individual behavior, but has become a cross-border phenomenon that threatens moral values, undermines the stability of individuals, and affects the security of societies and states alike. This crime derives its danger from its ability to exploit technological developments to subjugate people under the sword of threat and scandal, upsetting the balance of their lives and turning modern communication tools into channels of psychological terror and social pressure.

The importance of this research is highlighted by two complementary dimensions:

Scientific importance: This research contributes to enriching legal and security thinking by providing a contemporary treatment of a new crime, through deconstructing the concept of cyber extortion, explaining its characteristics, analyzing its various forms, and highlighting the challenges faced by legislation and security agencies in combating it. It thus contributes to filling a knowledge gap in Arab legal and security studies and provides a qualitative addition to the specialized scientific library.

Practical significance: The results of this study serve as a guide for legislators, decision-makers, and law enforcement agencies, revealing legislative shortcomings and providing them with a

comprehensive overview of legal, technical, and security response mechanisms, thereby ensuring enhanced individual protection and the maintenance of community security.

Therefore, the importance of this research goes beyond purely academic treatment, becoming an intellectual and legal cry against a crime that violates privacy and sows terror in people's hearts, making it a scientific and practical duty to address it, and a civilizational mission aimed at preserving human dignity in an era where freedom is intertwined with danger in a digital space that knows no boundaries.

Reasons for choosing the topic: The importance of choosing the topic "Cyber extortion: a legal and security perspective on contemporary challenges and ways to address them" stems from the fact that it touches on one of the most serious issues raised by the contemporary digital reality. The world has witnessed a radical shift in crime patterns, with crimes no longer confined to the streets and traditional locations, but moving into cyberspace, which is not limited by geography or time.

Cyber blackmail is the most prominent form of these crimes, as it poses a direct threat to individuals' freedom and privacy and raises social, political, and security concerns. Therefore, studying this phenomenon is both a scientific and practical necessity, as it reveals the conceptual and legal framework of the crime, highlights shortcomings in legislation, sheds light on security and technical challenges, and proposes practical solutions that contribute to enhancing individual protection and maintaining community security.

Thus, the choice of this topic was not accidental, but rather came in response to an urgent scientific and practical need imposed by the challenges faced by both legislators and security officials in addressing crimes that are hidden behind screens but have a profound impact on social, psychological, and political reality.

Motives for choosing the topic

1. Scientific dimension: This stems from the researcher's interest in emerging legal issues and his desire to contribute to the enrichment of the Arab legal library with a contemporary study that combines in-depth theoretical analysis with a realistic treatment of the phenomenon.

2. Practical dimension: The researcher's awareness of the urgent practical need for specialized studies on cybercrime, especially with the increase in cyber extortion cases in courts and the legal and security issues they raise, which require innovative and effective solutions.

3. Ethical dimension: The researcher's sense of intellectual and moral responsibility in confronting a crime that threatens what is most precious to human beings: their dignity, freedom, and peace of mind. This makes addressing this crime a duty that transcends the boundaries of academic research and becomes a moral and humanitarian mission.

4. Personal dimension: The researcher's direct connection to issues of cyber extortion in society and its negative effects on victims reinforced his conviction of the need to shed light on this phenomenon and present a comprehensive vision for addressing it.

Therefore, the choice of this topic combines scientific justifications, practical considerations, and personal motivations to create a research project that aims to contribute to building an intellectual, legal, and security foundation that will help shape a rational response to growing cyber challenges.

Research objectives: This research seeks to achieve a set of objectives that are divided between the scientific and theoretical aspects on the one hand, and the practical and applied aspects on the other. These objectives can be summarized as follows:

1) **Establishing a precise conceptual framework for the crime of** cyber **extortion** by defining it, describing its characteristics, and distinguishing it from other cybercrimes that are similar in form and content.
2) **Monitoring and analyzing contemporary forms and methods of cyber extortion**, revealing the diversity of its tools and methods and clarifying the extent of the danger it poses to individuals and societies.

3) **Identify shortcomings in national legislation that hinder effective legal action against this crime,** and highlight the need to develop texts or draft specific legislation that takes into account the changing nature of cyberspace.
4) **Propose integrated legal and security mechanisms to combat this crime**, based on strengthening national legislation, enforcing deterrent penalties, and developing international cooperation in the fight against cybercrime.
5) **Providing practical technical solutions that contribute to improving the ability** of **security agencies** to monitor, track, and protect, thereby strengthening society's immunity against this type of threat.
6) **Contribute to raising legal and social awareness of the dangers of cyber extortion**, considering that cultural prevention is no less important than security and legal measures.

These objectives collectively reflect the aspiration of the research to serve as a bridge between legal and security thinking and practical application, with a view to building an integrated vision for combating cyber extortion, protecting human beings and preserving their dignity, and consolidating community security in a world where challenges are accelerating and risks are growing.

Research methodology: This research adopted a multidimensional scientific methodology in addressing the topic of cyber extortion: a legal and security reading of contemporary challenges and ways to confront them. It is based on a descriptive-analytical approach to clarify the concept of crime, its characteristics and forms, and a comparative approach through a review of relevant Arab and international legislation and a comparison of their strengths and weaknesses. and an inductive approach based on details found in legal texts, security reports, and technical studies to arrive at overall conclusions that reveal the features of the phenomenon, as well as a critical approach to evaluate the effectiveness of legal rules and security measures and propose ways to develop them. **The researcher relied** on a set of scientific tools, including national laws and international agreements, academic studies specializing in criminal law and information security, security reports and statistics, as well as technical research that explains the mechanisms of cyberspace and the means of monitoring and protection. The methodology was thus comprehensive, combining description and analysis, comparison and induction, criticism and evaluation, to ensure a sound scientific and practical view of this emerging crime.

Previous studies

The first study, "Sahar Sharif Fakir Saber (2021) "The Crime of Cyber Extortion and **Ways to Combat** It" – This study focused on the conceptual foundation of cyber extortion, defining it and identifying its causes and pillars, while discussing relevant national and international legislation. The researcher followed a descriptive analytical approach, using partial comparisons between some legislations. The results showed that cyber extortion is complex due to the multiplicity of its tools and its cross-border nature, and that current legislation is insufficient to fully address it. The study recommended the need to develop an integrated legislative system at the national and international levels, with a focus on mechanisms for cross-border judicial cooperation.

Second study: Amani Hashim Latif (2020) Cyber extortion and its implications for the political and social reality in Iraq:

This study examined the social and political dimensions of cyber blackmail in Iraq, focusing on how it affects social trust and political stability. The researcher relied on a descriptive field approach and legal analysis of Iraqi texts. The results showed that cyber extortion has become a tool for political and social pressure in Iraqi society, and that the absence of precise legislation exacerbates the phenomenon. The researcher recommended raising community awareness, updating laws, and activating cooperation between security and social institutions to curb this crime.

Third study: Wafa Saqr (2019) Study of the crime of electronic blackmail (comparative study)

This study focused on clarifying the differences between traditional cybercrimes and cyber extortion from a comparative legal perspective. The researcher adopted a comparative approach,

analyzing the texts of legislation in some Arab and foreign countries. The results showed that criminal texts in most Arab countries remain general and vague, which makes effective deterrence difficult, unlike some foreign legislations that have established precise texts. The study recommended the need to draft more specific Arab laws, drawing on comparative experiences in Europe and America.

Fourth study: Marwa Saad Gad Al-Husseini (2023) Cyber blackmail of Egyptian women: An applied study of a sample of Facebook and Instagram users.

This study focused on the phenomenon of cyber blackmail directed at Egyptian women via social media. The researcher used an analytical field approach by studying a sample of Facebook and Instagram users and linked the social and psychological factors that increase women's vulnerability to blackmail. The results showed that girls and young women are the most vulnerable, and that legal and regulatory weaknesses exacerbate the phenomenon. The researcher recommended the development of specialized awareness programs and the strengthening of legislation to protect women from digital crimes.

Fifth study: Two researchers from Minya and Assiut Universities (2022) Study of social awareness of cyber blackmail among young people: An analytical study of the Egyptian environment

This study measured Egyptian youth's awareness of the dangers of cyber blackmail through a survey and analysis. The researchers used a descriptive field approach, employing questionnaires for youth samples. The results showed that young people's awareness remains limited and that the vast majority are unaware of the legal measures available to combat this crime. The study recommended the inclusion of digital security concepts in educational curricula and the launch of awareness campaigns targeting the groups most vulnerable to blackmail.

Chapter One

Conceptual Framework of Cyber Extortion

Introduction

Any serious scientific research can only be built on clearly defined concepts that establish the theoretical framework for the phenomenon under study, define its boundaries, and distinguish it from other phenomena. Therefore, delving into the subject of cyber extortion requires first defining its nature as a contemporary legal and security concept by reviewing its various definitions in criminal jurisprudence and national and international laws, and comparing it with similar digital crimes such as electronic fraud or traditional crimes of intimidation. Concepts are the gateway to understanding, and through them, the picture that enables the researcher to penetrate the depth of the phenomenon becomes clear.

This conceptual framework is important because cyber extortion is a relatively new crime linked to the development of digital technology and the opening up of cyberspace, which gives it a special character that differs from traditional crimes. It is a hybrid crime, in which legal, security, and social dimensions intersect, and which is carried out through various methods, starting with threats to publish personal images or information, and ending with demands for money or the exploitation of the victim for illicit gains.

Because the concept alone is not sufficient to understand the phenomenon, this chapter will also address the multiple forms of contemporary cyber extortion, highlighting the technical tools used by criminals and the psychological tactics they employ to trap their victims. This chapter thus forms the knowledge base on which the subsequent chapters are built, setting the general framework and revealing the initial features of the crime before addressing the challenges of combating it and ways to confront it.

Section One

Definition of cyber extortion and its distinction from similar crimes.

Requirement 1: Definition of cyber extortion

First: Definition of extortion: In linguistic terms, **extortion is** linked to the unlawful taking of money or benefits, whereby the perpetrator forces others to concede or submit under threat or pressure. Extortion is the coercion of another person's will and forcing them to give up something they do not willingly consent to, whether it be money, a right, or a benefit (1) Dictionaries state that extortion carries the meaning of deprivation, coercion, and compulsion, as in the saying, "So-and-so extorted money from another if he took it by force." The perpetrator is called " " (**the extortionist**), and the money taken is called "**المبتزّ**" (the extorted).()2)This term is also associated with other meanings such as plundering, dispossession, and taking something by force.3. Therefore, extortion is essentially an illegal act based on depriving others of their rights or forcing them to do something they do not want to do.4.

Second: Definition of **electronic blackmail:** The term "**electronic**" is an Arabicization of the foreign word "electronic," which originally refers to anything related to modern digital technologies. It is a term that has been adopted into the Arabic language, It did not appear in old dictionaries, although it is used today to refer to everything related to digital technical media. The meaning is derived from "**technology"** and what is associated with it in terms of mastery and precision in the means used (5).Accordingly, cyber extortion can be defined as "the use of modern technical media to threaten or extort individuals financially or morally, with the intention of obtaining illegal gains.

Third: Electronic blackmail in Islamic jurisprudence: Islamic jurisprudence has not addressed the term "electronic blackmail" per se, due to the novelty of the phenomenon, but it has addressed a related concept, namely coercion. Coercion in jurisprudence is synonymous with blackmail in terms of corrupting consent and eliminating freedom of choice**. The Hanafi school of jurisprudence defines** it as an act practiced on a person that nullifies their consent or corrupts their choice, so that they no longer have free will or are incapable of acting on their own behalf.6 **The Maliki school of jurisprudence** defines coercion as forcing another person to do something they do not want to do under threat, thereby corrupting their consent and making the act devoid of choice**.** This jurisprudential concept is consistent with the essence of electronic extortion, which is based on psychological or physical coercion to achieve the extortionist's interests**. The Shafi'i school of jurisprudence** define coercion as forcing a person to do something they do not want to do under threat of serious physical or psychological harm, thereby depriving them of their freedom of choice and causing them fear and distress (7).

1) Dictionary of Jurists' Language, Muhammad Rawas Qalaji, Hamid Sadiq Qunibi, Dar al-Nafais for Printing, Publishing, and Distribution, Beirut, Lebanon, second edition, 1408 AH-1988 AD, p. 38.

2) Al-Sahah Taj al-Lugha wa Sahah al-Arabia, Abu Nasr al-Farabi, edited by Ahmad Abd al-Ghafur Attar, Dar al-Ilm lil-Milayin, Beirut, Lebanon, 1407 AH-1987 AD, 3/865; Lisan al-Arab, Ibn Manzur, Jamal al-Din Muhammad ibn Makram, Dar Sadir for Printing, Publishing, and Distribution, Beirut, Lebanon, first edition, 1410 AH-1990 AD, p. 312.

3) Contemporary Arabic Language Dictionary, Dr. Ahmad Mukhtar Abdul Hamid Omar, Dar Al-Alam Al-Kotob, Riyadh, Saudi Arabia, 1st edition, 2008, vol. 1, p. 200.

4) Taj al-Arous min Jawhar al-Qamus, Mahbub al-Din Abi Fayyad al-Zubaydi, Dar al-Fikr, Beirut, Lebanon, 2005, 2/13.

5) The Crime of Electronic Extortion, Judge Ali Al-Zaydi, Comparative Law Library, Baghdad, Iraq, 2019, p. 7.

6 Al-Mabsut, Muhammad ibn Ahmad ibn Abi Sa'd Shams al-A'imma al-Sarkhsi (d. 483 AH), Dar al-Ma'rifah, Beirut, n.p., 1414 AH-1993 AD, vol. 24, p. 38.

7 Ahkam al-Qur'an, Abu Bakr Muhammad ibn Abdullah ibn al-Arabi, edited by Ali Muhammad al-Bajawi, Isa al-Babi al-Halabi Press, Cairo, 1387 AH - 1967 AD, 2nd edition, vol. 2, p. 1165.

As for the Hanbalis, they defined it as forcing someone to do something they dislike, whether by using force or threatening them with harm to themselves or their property, or something similar [(8).] Thus, it appears that coercion in the jurisprudential conception is considered the legal equivalent of what is known today as extortion, as it is based on psychological or physical pressure to corrupt the consent of the coerced person and force them to do what they do not want to do.

Second: Electronic blackmail in law

Researchers have provided several definitions of electronic extortion, which can be summarized as follows:

- **Cyber blackmail as a personal threat:** It is sometimes defined as an attempt to obtain financial, sexual, or moral gains from the victim, often women, by threatening to publish photos or personal secrets that could disgrace them or damage their social reputation [(9)] This definition focuses on the social dimension of cyber blackmail, but it does not negate the possibility that men may also be victims of this crime.
- **Cyber extortion as a technical crime:** It is considered to be the exploitation of modern means of communication and information technology to threaten or intimidate individuals into giving money or doing things they do not want to do· This definition is more comprehensive than the previous one, as it combines legal and technological aspects, indicating that the danger lies in the misuse of digital media [().10]
- **Blackmail through the exploitation of technical skills or social relationships:** Some studies suggest that perpetrators may rely on their technical expertise to hack into devices and steal data, or exploit their social proximity to victims to obtain sensitive information that they can later use to make threats. However, this definition focuses primarily on the technical aspect of the crime and overlooks the profound psychological and social impact that blackmail can have on the victim. [11()] .
- **Blackmail as a general threat:** Some legal trends broaden its definition, considering electronic extortion to be any act that threatens human freedom or instills fear in a person by threatening harm to them, their money, or their loved ones. The threat may be direct, through written, visual, or audio media, or indirect, through hints that confuse the victim and instill fear in them ([12]).

These definitions show that the lack of legislative harmonization between countries leads to differences in the characterization of the crime, making it urgent to establish a unified international legal framework capable of addressing cyber extortion as a cross-border crime.

Finally, we see that cyber blackmail, as one of the new crimes brought about by the digital revolution and rapid technological development, and is based on the use of the Internet or modern technology to pressure the victim and coerce them into doing or refraining from doing something, under threat of publishing personal information, images, or secrets obtained by legal or illegal means. This definition distinguishes between traditional blackmail, which is carried out in the physical world, and electronic blackmail, which uses the digital space as a medium for its commission, making it more dangerous due to the ease of access to victims and the multitude of means of dissemination and defamation. Some Arab and international legislation adopts similar

8 Al-Mughni, Abu Muhammad Abdullah bin Ahmad bin Muhammad, Dar al-Kitab al-Arabi, Beirut, Lebanon, 1402 AH - 1983 AD, vol. 7, p. 383.

9) The Crime of Electronic Extortion, Judge Ali Al-Zaydi, Comparative Law Library, Baghdad, Iraq, 2019, p. 11.

10) The Crime of Electronic Extortion (A Comparative Study), Kazim Abdul Jassim Al-Zaydi, Comparative Law Library, Baghdad, Iraq, First Edition, 2019, p. 8.

11) Dr. Sahar Sharif Fakir, "The Crime of Electronic Extortion and Ways to Combat It," Um Durman Islamic University Journal, pp. 167-195.

12) Explanation of the clarification of the text of the revision in the principles of jurisprudence, Saad al-Din al-Taftazani, Dar al-Kutub al-Ilmiya, vol. 1, p. 196.

definitions, agreeing that the essential element of the crime is "the threat to use modern technology to achieve an unlawful benefit at the expense of the victim's freedom."

Second requirement: The legal nature of cyber extortion

From a legal perspective, cyber extortion is a compound crime, combining threats and psychological pressure on the one hand, and the use of technical means on the other. Therefore, legal jurisprudence treats it as a specific form of the crime of threats, but its specificity lies in the means by which it is committed, namely electronic means, which give it a transnational character. This raises the question of whether traditional legal rules are sufficient to prosecute this type of crime, which has prompted many countries to enact specific legislation on cybercrime, including explicit provisions criminalizing electronic blackmail and imposing severe penalties for it. [13]

Third requirement: Distinguishing cyber extortion from similar crimes

Although cyber extortion is similar to some other cybercrimes, it is necessary to distinguish between them from a theoretical and practical standpoint. There are several types of cyberattacks that may be confused with cyber extortion, but each has its own characteristics that distinguish it from cyber extortion. The most prominent of these are:

First: Unauthorized access to electronic systems

It refers to deliberately and without legal justification accessing another person's information system or database, either in whole or in part,[14] and is often done by breaching security measures or using illegal means. The 2001 Budapest Convention [15] this act a crime in itself because it poses a threat to data confidentiality and integrity. This act differs from cyber extortion in that it may be merely a preliminary stage resorted to by the perpetrator to obtain the victim's data for the purpose of threatening them later, and it may constitute a crime in itself if it is not followed by extortion.[16].

Second: Unlawful interception of data

This refers to the interception of correspondence or data in transit between electronic systems by technical means without authorization, including telephone, fax, and email communications. Article 3 of the Budapest Convention criminalizes this behavior[17], in order to protect the privacy of correspondence as a fundamental human right. As with illegal access, interception may be a preliminary step in the context of electronic extortion, or it may remain an independent act punishable by law. [18].

---

[13]) Tariq Namik Muhammad Rida, (2021), Criminal Liability for Electronic Blackmail via Social Media, Master's Thesis, Faculty of Law and Political Science, University of Kirkuk, Iraq

[14]) Barhal Amal, The Crime of Blackmail via Electronic Means, Master's Thesis, Faculty of Law and Political Science, Department of Law, Arab University of Tebessa, Tebessa, 2020.

[15] Article 2 of the Budapest Convention (2001) stipulates that unauthorized access to computer systems or any part thereof, whether by breaking security measures or exploiting technical loopholes, with the intent to obtain, use, or manipulate data, shall be criminalized. This article lays the international foundation for combating "unlawful access," which is considered one of the most serious forms of infringement on the confidentiality and integrity of information systems and a stage that may pave the way for other crimes such as cyber espionage, extortion, or computer fraud.

[16] **Mohamed Mamdouh Shehata Khalil**, Electronic Extortion between Islamic Law and Egyptian Law: A Comparative Study, Journal of the Faculty of Arts, New Valley, Issue No. 14.

[17] Article 3 of the Budapest Convention (2001) addresses the crime of unlawful interception of data by criminalizing any interception or interception using technical means for the purpose of capturing or recording communications or data transmitted via computer systems or communication networks, if done intentionally and without right. The scope of this article extends to all forms of electronic data transmission, whether by telephone, email, fax, or other means, in order to protect the privacy of correspondence and ensure the confidentiality of information. This article is particularly important because interception is often a preliminary step to subsequent crimes such as extortion or information exploitation.

[18]) Dr. Tarek Ibrahim Al-Desouki Attia, Information Security – The Legal System for Information Protection (Previous reference) p. 222.

Third: Fraud via electronic media: This type of crime occurs when data is entered, modified, or deleted in an information system with the intent to deceive in order to obtain unlawful financial gain or harm the rights of others.[19] Article 8 of the Budapest Convention has a special provision criminalizing this act, noting its increasing risks with the expansion of electronic transactions and payment cards.[20] For this crime to be committed, criminal intent must be present in two forms: general intent, which is manipulating a computer in a way that causes harm to others, and specific intent, which is the perpetrator's intention to achieve economic benefit for themselves or others. The text covers all forms of acts that may affect computer functions, whether they involve input, damage, deletion, or obliteration, as they represent a direct attack on the integrity of the information system and its performance of its various functions.[21]

Damage here refers to the deletion or corruption of data or programs in a manner that renders them unusable, thereby disrupting the information system and impairing its functions, whether through physical or non-physical components [22][23]Some jurists believe that Article (8) also implicitly covers online fraud, since access to the network is via electronic devices, and because information manipulation, if intended to obtain unlawful economic benefit, falls within the scope of criminalization.

Article 9 of the Convention criminalizes acts related to pornographic content, particularly the exploitation of children, by making it a crime to produce, distribute, possess, or display such material via computer systems. The Convention defines a "minor" as any person under the age of 18, with the authority to reduce this age limit to 16 granted to the States Parties. This article aims to strengthen the protection of children from sexual exploitation through information media, in response to growing international concern expressed at European summits and in children's rights protocols [24].

Despite the importance of this article, the convention is criticized for limiting criminal protection to minors only, unlike some Arab legislation that extends protection to all individuals regardless of age, thereby providing broader protection against the misuse of information systems to disseminate immoral content [25].

Fifth: Distinguishing between electronic extortion and influence peddling: In Article 106 bis of the Penal Code, Egyptian lawmakers criminalized the exploitation or peddling of influence. and the Court of Cassation has ruled that this crime is committed as soon as the perpetrator requests, accepts, or takes a promise or gift to use his influence—whether real or alleged—for the purpose of obtaining an advantage from a public authority. In this case, he is treated as a bribe-taker and punished with the prescribed penalty. Influence is defined as any possibility that enables its holder

19 The Herdo Center for Digital Expression Support report (2018, p. 24) indicates that the Budapest Convention established a coherent legal framework for combating cybercrime. but at the same time it has sparked widespread debate about its impact on digital rights and freedoms, particularly with regard to freedom of expression and the right to privacy, with some researchers arguing that tightening legal controls could become a tool for restricting cyberspace rather than protecting it

20 (Budapest Convention, 2001, Art. 8, op. cit.

21 Paragraphs 86 to 90 of the Explanatory Report to the Budapest Convention, p. 14; Halalawi Abboud Al-Wahid Ahmad, The Budapest Convention on Cybercrime with Commentary, op. cit., p. 101; Omar Taha Khalil and Afaf Badi Jamil, The Jurisprudential and Legal Adaptation of Cybercrimes, Journal of the Faculty of Heritage, Issue (17), 2015, p. 174.

22 Lucas (A.), Le droit de l'informatique, P.U.F. 1987, p. 221; Tariq Ibrahim Al-Desouki Attia, Information Security – The Legal System for Information Protection, op. cit., p. 221.

23) Aboud Al-Fatooh Bayoumi Hijazi, Combating Computer and Internet Crimes in Model Arab Law, p. 67; Huda Hamid Qashouqa, Computer Crimes in Comparative Legislation, Dar Al-Nahda Al-Arabiya, Cairo, 1992, p. 43.

24 Paragraphs (1–4) of Article (9) of the Budapest Convention, 2001; Suhair Al-Attar, New Crimes Against Children Through Information Systems, p. 299; Abdelfattah Bayoumi Hijazi, op. cit., p. 39.

25) Malak Atwi, Cybercrime, Annals of the University of Algiers, Issue (21), June 2012, p. 18; Amr Taha Khalil and Afaf Badi Jamil, op. cit., p. 177.

to influence public authorities, whether that influence arises from a professional, political, or social position. Despite the apparent similarity between electronic extortion and trading in influence in terms of requesting an unlawful benefit, there are fundamental differences between them. trafficking in influence requires the presence of three parties: the person with influence, the person in need, and the public official, and does not necessarily involve the element of threat. Cyber extortion, on the other hand, involves only two parties: the perpetrator and the victim. It is based on threats that force the victim to submit, and it does not require the involvement of a public official, unlike influence peddling, which is predominantly carried out by persons connected with public office.

Sixth: Distinguishing between cyber blackmail and exploiting a minor's weakness: In Article 338 of the Penal Code, Egyptian lawmakers criminalized the act of exploiting a minor's need or weakness or desire to obtain material or moral benefit, considering it a crime against personal freedom and imposing a penalty of up to seven years' imprisonment if the perpetrator is the minor's guardian or custodian.

Some may think that there is a similarity between this crime and cyber blackmail, given that many victims of blackmail are minors. However, the fundamental difference between the two lies in the method used. In cyber blackmail, the threat is the fundamental element, without which consent is invalid, while in the exploitation of minors, the perpetrator relies on exploiting the victim's weakness or psychological inclination to achieve their goal, and consent has no legal effect. Furthermore, blackmail can affect both minors and adults, unlike the exploitation of minors, which only occurs if the victim is a minor.

Fourth requirement: Elements of cyber extortion

Like other crimes, electronic extortion is based on fundamental elements that are essential to its legal construction, namely the legal element, the material element, and the moral element. It is the combination of all these elements that gives the crime its full form and determines the perpetrator's responsibility and the limits of the punishment deserved.

First – Legal basis: The legal basis is the cornerstone of criminal liability, as there is no crime or punishment except by law. Modern criminal legislation has intervened to establish clear provisions criminalizing electronic extortion as one of the most serious forms of cybercrime. Article 430 of the Iraqi Penal Code of 1969 criminalizes any threat made with the intent to blackmail the victim or damage their honor and reputation ([26]).Similarly,Article 16 of the UAE Federal Law on Combating Information Technology Crimes of 2021 criminalizes the use of information networks or information technology to blackmail or threaten others.[27] Article 18 of the Omani Law on Combating Information Technology Crimes of 2011 confirms the punishment of anyone who uses modern technology to threaten or blackmail others to achieve an unlawful interest((([28]) These texts clearly reveal the legal basis for criminalization and punishment in this crime.

Second – Material element: The material element is embodied in the external acts committed by the perpetrator and is based on three basic elements: the act of threatening, the means used, and the criminal result. The material element of the crime of electronic extortion consists of interrelated elements that reflect the external structure of the criminal act and include the act, the means, the exploitation, and the result.

- **Criminal act**: The criminal act consists of threatening the victim via digital means, such as email, text messages, or social media platforms [(29)].This act includes words, writing, symbols, or images

[26]) Article 430 of the Iraqi Penal Code of 1969.

[27]) Article 16 of the UAE Federal Law on Combating Information Technology Crimes of 2021.

[28] Article 18 of the Omani Law on Combating Information Technology Crimes of 2011.

[29]) The crime of electronic threats and extortion, Mariam Araab, Journal of Comparative Legal Studies, Faculty of Law and Political Science, University of Oran , Volume 7, Issue 1, 2021, p. 12

used to frighten the victim or force them to comply with unlawful demands. In this case, it is sufficient to simply cause fear or psychological pressure in the victim, without the need to actually carry out the threat, making the criminal act complete as soon as the psychological or physical effect on the victim occurs.[30]

– The act of threatening: Threatening constitutes the essence of the material element and manifests itself in the perpetrator directing the victim away or warning them of harm, whether related to damaging their reputation or private life or divulging their secrets (31).The Iraqi legislature has recognized in Article 430 of the Penal Code of 1969 that the mere threat of harming a person's reputation or honor is a criminal offense, regardless of whether it is carried out.[32]

– Electronic means: The crime acquires its distinctive character from the use of modern digital media such as email, social media platforms, or chat applications. Arab legislation has criminalized extortion via modern technology , as in Article (16) of the UAE Federal Law on Combating Information Technology Crimes of 2021 and Article (18) of the Sultanate of Oman Law on Combating Information Technology Crimes of 2011(33)

Third – Exploitation and coercion: The material element is also evident in the perpetrator's exploitation of the information or images in his possession to coerce the victim and force her to comply with his unlawful demands or face the risk of scandal, reflecting the coercive nature of the crime and the victim's lack of freedom.(34)

Fourth – Criminal outcome and causal relationship: The material element is completed by the occurrence of a direct criminal outcome, such as instilling fear in the victim, forcing them to pay money, or committing unlawful or immoral behavior. A causal relationship between the act of threatening and the outcome is required for the crime to be legally complete. (35)

Thus, the material aspect of cyber extortion appears as a complex structure comprising the act (36) , the technical means(37) , coercive exploitation(38) , and the resulting consequence(39),giving it a special character that goes beyond individual harm to threaten the stability of society and the protection of its fundamental values. ((40).

Third – Moral element: For a crime to be committed, it is not sufficient for the legal and material elements to be present; the moral element, represented by criminal intent,must also be present (41).When a blackmailer threatens a victim via electronic means, they are aware of the seriousness of their actions and intend to achieve an unlawful purpose, whether it be to obtain financial gain, to

30) A Brief Guide to General Criminal Law, Nasour Rahmani, Dar Al-Ouloum Publishing and Distribution, Annaba, Algeria, 2006, p. 94

31) Explanation of the Penal Code: Special Section, Mohamed Amin Douidar, Al-Nahda Al-Masriya Library, Cairo, Egypt, second edition, 1979, p. 314

32) Captain, Amani Yahya Abdel Moneim. The Crime of Electronic Blackmail Against Women. Dar Al-Fikr Al-Arabi, Alexandria, 2023, p. 112.

33) Article 18 of the UAE Federal Law on Combating Information Technology Crimes of 2021.

34) Fathallah, Mahmoud Rajab. Cyber Extortion Crimes. Dar Al-Jami'ah Al-Jadidah, Egypt, 2021, p. 80.

35) Abdul Razzaq, Mamoun Muhammad. Penal Code – General Section. Part III, 2018, p. 18.

36) Al-Boushi, Ahmed Mohammed. Cyber Extortion: A New Concept in Cyber Threat Crimes. Dar Al-Nahda Al-Arabiya, Cairo, 2022, p. 65.

37) Youssef, Amir Faraj. Criminal Liability for the Crime of Electronic Extortion. Dar al-Maktabat al-Jadida, Egypt, 2023, p. 103.

38) Explanation of the Algerian Penal Code, Abdullah Salimani, Diwan al-Maktabat al-Jami'iyya, Algeria, 1995, p. 149

39) The Crime of Electronic Extortion and Mechanisms to Combat It in the Republic of Iraq, Rami Ahmad Galbi, article published in Thaqafatna al-Amniya magazine, second edition, Iraqi Ministry of Interior, Directorate of Relations and Media, Dar al-Kutub wa al-Wathaiq, Baghdad, Iraq, 2019, p. 47.

40) The Crime of Electronic Extortion: A Comparative Study, Muhammad bin Abdulmohsen bin Shalhoub, supplementary research for a master's degree in Sharia law, Higher Institute of Justice, Sharia Law Department, Regulations Division, Imam Muhammad bin Saud Islamic University, Riyadh, Saudi Arabia, 2019, p. 9

41) Criminal Law: Introduction and Principles of Theory, Ali Rashid, Dar Al-Nahda Al-Arabiya, Beirut, Lebanon, 1974, p. 353

push the victim into unlawful behavior, or simply to damage their reputation and dignity. Criminal intent is present here in both its elements: knowledge and will. The perpetrator knows that his behavior is unlawful and knows the consequences it will have on the victim, yet his free will leads him to commit the act and proceed with it to achieve his goal. Therefore, electronic blackmail is primarily an intentional crime [42]., based on bad faith and criminal intent that leaves no room for error or negligence, but rather is based on a direct intention to harm and exploit others. Thus, the combination of these three elements – legal, material, and moral – is what gives the crime of electronic extortion its complete legal structure and makes it a model of a complex crime in which psychological and social dimensions are intertwined with legal texts, requiring legislators and the judiciary to be more precise in regulating it and assessing its effects.

Section II: Forms and methods of contemporary cyber extortion.

Cyber extortion is one of the most serious forms of cybercrime, directly threatening individuals' lives and privacy. It undermines their dignity and robs them of their right to feel safe, making them prisoners to the perpetrator's demands and subject to their power. This crime is characterized by its complex psychological and social dimensions, as the victim becomes a prisoner of fear and anxiety of scandal or defamation, which doubles its danger to the entire social structure ([43] . The crime of electronic blackmail is characterized by being a dynamic and multidimensional crime, whose forms and methods change with the evolution of technology and the social and political environment. It can be broadly classified into two main categories that summarize its characteristics: the essential forms of the crime and the technical and psychological methods used to commit it.

First requirement: Forms of cyber extortion

In today's world, cyber extortion takes various forms, differing in terms of the intended purpose and the nature of the relationship between the perpetrator and the victim:

Sextortion: This is the most prominent form **of extortion** worldwide, in which the extortionist threatens the victim with publishing images or videos of a private nature in order to obtain illegal gains, which may be financial, sexual, or behavioral. Sextortion is the most common and dangerous form of cyber extortion, where the perpetrator hacks into the victim's electronic devices, such as smartphones or computers, to obtain images or videos of a private or sensitive nature, and then threatens to publish this material publicly if the victim does not comply with their demands. which are often acts that affect dignity and honor or involve immoral practices. This type of crime constitutes a complete offense in terms of threat, data exploitation, and psychological and moral coercion [(44)]Victims often give in under the weight of fear of scandal, which reveals the severity and psychological depth of this type of crime. The danger of this type of crime lies in its reliance on the element of "social stigma," which puts victims—especially women—in a position of extreme vulnerability, sometimes pushing them to respond or even consider ending their lives.

Financial blackmail: Financial blackmail is another equally serious form of blackmail, whereby the blackmailer threatens to publish personal photos, information, or secrets in exchange for money. In this type of blackmail, the perpetrator exploits the victim's concern for their reputation and fear of defamation to force them into a position of financial compromise. This type of extortion often targets young people and girls alike, demanding varying sums of money in exchange for silence and not publishing the material. Financial extortion thus intersects with psychological extortion, combining psychological threats with economic exploitation, which doubles its devastating impact

[42]) The role of digital forensic evidence in proving cyber extortion crimes, Akram Deeb, Noura Ben Bouabdallah, previous reference

[43]) Dr. Sahar Sharif Fakir, The Crime of Cyber Extortion and Ways to Combat It, Um Durman Islamic University Journal, Issue (unspecified), pp. 167-195, Al-Hikma Journal for Studies and Research, Volume 04, Issue 05(19), 30/09/2024, ISSN print: 2769-1926, ISSN online: 2769-1934 Accessed on 10/9/2025

[44]) Amani Yahya Abdel Moneim Al-Naqib, (2023), The Crime of Cyber Blackmail Against Women, Dar Al-Fikr Al-Arabi, Alexandria.

on individuals and society.[45] It often involves the use of ransomware or threats to disclose sensitive data in exchange for money. This type of extortion particularly affects institutions, as it leads to the disruption of information systems and the interruption of vital services, making it sometimes necessary to respond to the extortionist.

Child blackmail: Blackmailing children and adolescents is considered one of the most dangerous forms of cyber blackmail, given that it targets an age group that is vulnerable in terms of experience and knowledge of modern means of communication. Children, especially girls between the ages of 12 and 18, are lured through social media sites or online gaming platforms. After obtaining offensive images or videos, the perpetrator threatens the victim with using them either to obtain financial gain or to force an illicit relationship. These practices often leave deep psychological and social scars that can destroy the victims' futures or push them into dangerous behaviors such as suicide or isolation from their social environment ([46]

Reputation and job-related blackmail: The criminal threatens to reveal personal or professional secrets in order to damage the victim's reputation or social standing. This is often used against public figures or employees in sensitive positions, and strikes at the heart of an individual's social standing.[47].

Political and institutional blackmail: This type takes on a strategic dimension, as it is used to spread chaos or achieve political gains, and often affects national security by targeting government institutions, parties, or organizations. It is considered one of the most dangerous forms of blackmail due to its impact on the stability of states. These forms, despite their diversity, share a common element, which is "**coercing** the victim" by threatening to use personal or professional data, but they differ in the type of illicit gain targeted (financial, sexual, social, political **([48]) .**

Second requirement: Methods of cyber extortion (technical and psychological)

Cyber blackmail does not simply involve possessing sensitive material against the victim, but requires intertwined technical and psychological methods that make the crime effective:

1) **Technical methods:** Hacking and data theft: Through phishing or exploiting vulnerabilities through social media tools (Facebook) [(49)], which is the most common method of obtaining blackmail material.
2) **Ransomware**: Not content with simply controlling data, ransomware has evolved into what is known as “double extortion,” where data is both encrypted and stolen.
3) **Digital espionage**: Through screen recording software or remote camera operation, which provides highly sensitive content.
4) Deepfakes: A modern technology that enables perpetrators to fabricate images or videos that put victims in compromising situations, even if they do not provide original material, a trend that makes legal action even more difficult.
5) **Denial-of-service** (DDoS) **attacks**: Used as a tool to pressure organizations into stopping attacks in exchange for money.

Psychological tactics and social engineering:

[45] Mahmoud Ragab Fathallah, (2021), Crimes of Electronic Extortion, Dar Al-Jami'ah Al-Jadidah, Egypt.

[46]) Muhammad Ahmad Al-Razqi, (2002), Lectures on Criminal Law, General Section

[47] Kazim Abdul Jassim Al-Zaydi, (2019), The Crime of Electronic Extortion, Comparative Law Library, Baghdad, First Edition

[48]) Ahmed Muhammad Al-Boushi, (2022), Electronic Extortion: A New Concept in Cyber Threat Crimes, Dar Al-Nahda Al-Arabiya, Cairo

[49]) Latouh Hawazem's thesis (2019) examined and analyzed the criminal liability arising from the misuse of social media networks, comparing positive law and Islamic law, explaining the legal and security challenges facing legislators in controlling this type of crime, and how to balance freedom of expression with deterrent criminal controls

1) Romance scams: where the perpetrator builds a relationship that appears to be affectionate and caring, only to end up exploiting the victim emotionally or financially.
2) **Exploiting fear and shame**: This is the essence of blackmail, where the criminal relies on psychological pressure resulting from the victim's fear of scandal or loss of reputation.
3) **Impersonation of authority and impersonation**: Impersonating an official or media entity to lend credibility to the threat and increase the victim's sense of helplessness.
4) **Social engineering**: This involves studying the victim's personality and gathering detailed information about them, then constructing a carefully crafted scenario that forces them to comply.
5) The combination of these technical and psychological methods makes cyber extortion a complex crime. It is not just a passing threat, but a calculated process that exploits both the technical weaknesses and psychological fragility of the victims.

Chapter Two

Ways to Confront It

Introduction

Confronting cyber extortion is no longer a legal luxury or a security option, but rather an existential necessity to protect individuals, communities, and states from collapsing under the weight of digital crime. **In this** context, this chapter provides an analytical reading of ways to confront cyber extortion on two main levels: On the one hand, legal mechanisms highlight the need for flexible and up-to-date legislation that accommodates the characteristics of digital crime and provides the judiciary and public prosecution with effective tools for accountability and punishment, in addition to strengthening international cooperation to prosecute perpetrators across borders. On the other hand, security and technical mechanisms highlight the need to build advanced capabilities in the field of digital investigation, monitor patterns of extortion, and develop partnerships between the state and the private sector to secure the digital infrastructure.

This chapter thus marks a practical turning point, as it moves from identifying weaknesses and shortcomings in the fight against cyber extortion to exploring possible solutions, providing the reader with a roadmap that combines a strict legal vision with a renewed security reality, so that the fight against cyber extortion can be more robust and comprehensive in protecting society from its clutches.

- **Section I: Legal mechanisms (legislation, penalties, international cooperation)**

Legal mechanisms are the first line of defense against cyber extortion; they give the state the ability to control criminal behavior, define its parameters, and determine deterrent penalties for offenders. The more flexible and comprehensive the legislation, the more effective the judicial system will be in curbing this phenomenon. This discussion can be divided into three main requirements: legislation, penalties, and international cooperation.

The first requirement: legislation – the legal basis for combating cyber extortion

Although many traditional criminal laws address crimes of threat or extortion, the digital nature of crime necessitates specific provisions that take into account the particularities of the electronic environment. The absence of explicit legislation creates a legal vacuum that allows perpetrators to escape accountability, or at least to challenge the legality of criminalization.

National legislation and its variations: Most Arab countries have recognized the seriousness of cyber extortion and its psychological, social, and economic consequences, and have sought to combat it by explicitly including it in criminal law and imposing severe penalties on perpetrators. Although legal approaches vary from one country to another, the common denominator is the establishment of the principle of deterrence to protect individuals and society from this emerging threat.

In Sudan, Article 176 of the 1991 Criminal Code criminalizes extortion, stating that anyone who threatens another person with the intent of forcing them to hand over money or legal documents is guilty of a crime punishable by imprisonment for a term not exceeding seven years, in addition to a

fine [50] The 2007 Cybercrime Act reinforced this approach, with Article 10 stipulating that anyone who uses an information network or computer to threaten or blackmail others shall be punished with imprisonment and a fine depending on the nature of the act[51] .

In Saudi Arabia, Article 3 of the Anti-Cybercrime Law criminalizes anyone who eavesdrops on information or blackmails others using electronic networks, with a penalty of up to one year in prison and a fine of up to 500,000 riyals, or one of these two penalties.[52]

In Egypt, Penal Code No. 58 of 1937, amended in 2003, addresses – addressed the crime of blackmail in Article (428), stipulating a prison sentence of seven years for anyone who threatens another person with the publication of personal information, images, or secrets with the intent to harm their reputation, freedom, or property. If the threat is carried out, the penalty is increased to nine years [53].

In Iraq, Article 430 of the Penal Code issued in 1969 stipulates that anyone who threatens another person with committing a crime or exposing information about them or their family, whether the threat is made directly or via electronic media, shall be punished with up to seven years' imprisonment or simple imprisonment [54].

In the United Arab Emirates, the Federal Law on Combating Information Technology Crimes of 2021 attaches particular importance to this crime, as Article (16) stipulates that anyone who commits the crime of electronic blackmail shall be punished with imprisonment of up to ten years and a fine ranging from 250,000 to 500,000 dirhams, especially if the blackmail relates to matters of honor or reputation. [55]

In the Sultanate of Oman, Article 18 of the 2011 Information Technology Crimes Law criminalizes extortion via electronic media, specifying a penalty of imprisonment for a period of not less than three years and not more than ten years, and a fine ranging from 1,000 to 10,000 Omani rials, with the penalty being increased if the blackmail is linked to a felony or an attack on honor and reputation ([56].

These texts show that most Arab countries have established solid legislative foundations for combating cyber extortion. However, there are disparities in the nature of the penalties imposed and in the methods of legal drafting, which calls for consideration of the possibility of coordinating efforts between these legislations to unify concepts and enhance the effectiveness of the response, especially since the crime, by its nature, transcends geographical boundaries and takes advantage of the open cyberspace.

The need for continuous updating: The digital world is rapidly evolving, and if legislation does not keep pace with technologies such as concealment, encryption, cryptocurrencies, and identity masking, it will become incapable of protecting society. Therefore, there is a need to periodically update laws in line with the evolution of criminal methods.

Requirement 2: Punishment – Deterrence and protection of society

Nature of penalties imposed: Penalties often range from imprisonment to fines, and in some jurisdictions may be more severe in cases of extortion against sensitive institutions or public figures, or if it results in serious harm such as suicide or damage to national security.

Effectiveness of the penalty

- Penalties should be sufficiently dissuasive for offenders and proportionate to the seriousness of the social, psychological, and economic impact of the crime.

[50]) Article 176 of the Sudanese Criminal Code of 1991.
[51]) Article (10) of the Sudanese Cybercrime Law of 2007.
[52]) Article 3 of the Saudi Arabian Anti-Cybercrime Law.
[53]) Article 428 of the Egyptian Penal Code of 1937, amended in 2003
[54]) Article 430 of the Iraqi Penal Code of 1969:
[55] Article 16 of the Federal Law on Combating Information Technology Crimes in the United Arab Emirates of 2021
[56] Article 18 of the Law on Combating Information Technology Crimes in the Sultanate of Oman of 2011

- Weak enforcement of penalties or delays in trials undermine victims' confidence in the justice system and sometimes push them to settle with extortionists outside the law.

Supplementary penalties

- These may include confiscating the devices used, blocking websites that engage in extortion, and closing suspicious accounts.
- Some laws also require offenders to undergo rehabilitation or training programs, demonstrating a rehabilitative dimension alongside deterrence.

Third requirement: International cooperation – crossing borders to combat transnational crime

Cyber extortion often brings together perpetrators and victims in different countries, with perpetrators exploiting differences in laws or slow judicial proceedings to avoid prosecution.

First: International agreements: The Budapest Convention on Cybercrime of 2001 is considered the most prominent international reference in this field, as it established a unified framework for combating cybercrime, including cyber extortion. The convention aims to strengthen cooperation between member states by harmonizing national legislation, developing prosecution mechanisms, and exchanging information and technical expertise. The importance of this convention lies in its early recognition of the seriousness of cybercrime and its efforts to establish a cross-border legal framework that provides member states with a practical mechanism to combat transcontinental threats. (57)

Second: The role of the United Nations: Through its Office on Drugs and Crime (UNODC), the United Nations plays a pivotal role in supporting Member States in combating cybercrime, including cyber extortion. This role has been reflected in a number of initiatives, most notably:

- Developing training programs to build technical and legal capacities.
- Providing guidance for the development of national legislation in line with international standards.
- Promoting cooperation between judicial and police authorities at the international level.

The importance of these initiatives lies in the fact that they help developing countries bridge the legislative and technical gap exploited by criminal groups, thereby contributing to raising the level of national and international preparedness to counter cyber threats. (58)

Third: The role of the International Criminal Police Organization (INTERPOL)

- Interpol plays a practical role in coordinating international efforts to combat cyber extortion by:
- Establishing specialized units to combat cybercrime.
- Providing technical and technological assistance to member states to track down perpetrators.
- Developing digital information exchange systems to ensure rapid response to cyber incidents.

This role is vital given the cross-border nature of cyber extortion, as no country can tackle these threats alone without international partnerships that enable information sharing and the tracking of criminals across different jurisdictions. (59)

Fourth: General Data Protection Regulation (GDPR): The European General Data Protection Regulation (GDPR), issued in 2018, is one of the most important international legal tools that has contributed to reducing the opportunities for exploiting personal data in cyber extortion crimes. This regulation has imposed strict controls on data collection and use, granted individuals the right to take legal action against any misuse of their data, and required organizations to disclose any data security breaches within 72 hours, thereby reducing the opportunities for leaked information to be

57) Convention on Cybercrime (Budapest Convention), 2001.

58) Report of the United Nations Office on Drugs and Crime (UNODC), Countering Cybercrime, Second Edition, Vienna, 2020, p. 78.

59) Annual Cybercrime Report, International Criminal Police Organization (INTERPOL), Lyon, France, 2021, p. 45.

exploited in blackmail operations. It is clear that these regulations have contributed significantly to enhancing the protection of personal data and reducing the risks posed by cybercrime. (60)

Fifth: Malabo Convention on Cybersecurity and Personal Data Protection: In 2014, the African Union adopted the Malabo Convention, which aimed to establish a comprehensive framework for combating cybercrime on the African continent, including cyber extortion. The convention included several pillars, most notably:

- Establishing uniform definitions for cybercrimes.
- Strengthening cooperation between member states in cross-border investigations.
- Requiring member states to enact strict national legislation to combat cybercrime.

However, some African countries still face difficulties in implementing this agreement due to weak legal and technical infrastructure and a lack of sufficient resources to counter the growing threats. (61)

Sixth: The role of the International Telecommunication Union (ITU): The ITU plays a key role in combating cyber extortion by:

- Establishing international standards to enhance network and communications security.
- Preparing guidelines to help countries develop their cyber infrastructure.
- Providing advisory services to developing countries to support their efforts in combating cybercrime.

This role is essential in promoting international cooperation and building the capacities of countries, especially those with weak technical and legislative capabilities. (62)

- **Section II: Security and technical mechanisms (monitoring, tracking, protection programs)**

Security and technical mechanisms represent the first and most effective line of defense against cyber extortion crimes. They are the practical tools that translate legal texts into reality and make deterrence and protection possible. The law alone is no longer capable of combating this crime unless it is integrated with monitoring and tracking tools and advanced technologies that detect perpetrators and protect individuals and institutions from falling victim to them. These mechanisms can be addressed through three main pillars:

First: Monitoring and early prevention: Monitoring is a proactive step taken by security agencies and technical institutions to track digital activity and identify suspicious activities before they turn into full-fledged crimes. This includes developing advanced systems to detect attempts to hack accounts, steal data, or spread malicious links. It also includes the creation of specialized cybersecurity units that monitor social media platforms and email sites to detect recurring patterns of cyberattacks. Early monitoring is like having "watchful eyes" that warn the community of imminent danger, saving individuals and institutions from serious material and moral losses.

Second: Tracking and detecting perpetrators: One of the most prominent security challenges in cyber extortion crimes is the ability of perpetrators to hide behind technological barriers such as virtual private networks (VPNs), anonymous platforms, or encryption technologies. This is where tracking plays a crucial role, as security agencies rely on advanced tools such as metadata analysis, IP tracking, and artificial intelligence to detect criminals' behavioral patterns. Tracking proves its worth when the anonymous digital world is transformed into a legally accountable space, where the "mask of anonymity" is removed from the extortionist's face and they are brought to justice.

Third: Protection and cybersecurity programs

The fight cannot be won without building a robust protection system at the individual and institutional levels. These programs include antivirus tools, firewalls, intrusion detection systems,

60) General Data Protection Regulation (GDPR), European Parliament, Brussels, third edition, 2018, Articles 33-34.

61) Global Cybersecurity: Challenges and Solutions, International Telecommunication Union, Geneva, second edition, 2020, pp. 24-26.

62) Malabo Convention on Cybersecurity and Personal Data Protection, African Union, Addis Ababa, first edition, 2014, Article

and advanced encryption for sensitive data. User awareness should also be enhanced, as "digital awareness" is one of the most powerful weapons of protection. No matter how powerful the technology is, it can collapse at the click of a button when a user opens an unknown link or hands over their private data to a blackmailer through a deceptive ploy. Hence the need for specialized training programs and the building of a digital security culture that makes every member of society part of the protection system.

Conclusion

Cyber extortion is not a passing crime that can be easily forgotten; rather, it is a recurring phenomenon that changes its form as technology evolves, and its danger increases as the digital space expands into every detail of our lives. This research has revealed that cybercrime, especially blackmail, is not merely an individual act, but rather a reflection of legislative loopholes, security vulnerabilities, and weak social awareness. It is a crime that grows in the shadows, drawing its strength from the victim's fear and silence, and growing as legislators delay in prosecuting it or security forces fail to track it down.

Results

1) **Inadequate national legislation**: It has become clear that many legal texts still fail to cover all forms of cyber extortion, creating opportunities for impunity or leniency.
2) **The problem of legal adaptation**: It has been difficult to determine the precise legal description of the crime of cyber extortion, between what constitutes a threat, an invasion of privacy, and an independent technical crime.
3) **Security and technical challenges**: Practical experience has shown that tracking blackmailers in a space characterized by anonymity and multiple media is extremely difficult, especially when criminals resort to encryption techniques, identity concealment, and the use of dark networks.
4) **Social and psychological dimension**: It has become clear that victims, especially women and young people, are under psychological and social pressure that may push them into silence or submission, which increases the chances of repeat offenses.
5) **Weak international coordination**: Cross-border crimes reveal significant gaps in cooperation between countries, both in terms of information exchange and enforcement of judgments.

Recommendations

1) **Developing specific legislation:** Laws specific to cybercrime should be enacted that are flexible and adaptable to technological developments, with tougher penalties to deter criminals.
2) **Strengthening security and technical capabilities**: Invest in training security personnel and providing them with the latest tracking and monitoring software, while establishing specialized units to investigate cyber extortion cases.
3) **International cooperation**: Activating international agreements on cybercrime and building bridges for coordination between countries to speed up extradition procedures and the exchange of digital evidence.
4) **Raising community awareness**: Launch awareness programs targeting young people and women in particular, educating them about the dangers of responding to blackmailers and informing them about reporting mechanisms and how to seek help.
5) **Psychological support for victims**: Establish psychological and legal support centers for victims, because addressing the psychological effects is no less important than legal prosecution.

References

◈ **Jurisprudential references**

1) Explanation of Algerian Penal Law, Abdullah Salimani, University Publications Office, Algeria, 1995.

2) Al-Mabsut, Shams al-A'imma al-Sarkhsi (d. 483 AH). Dar al-Ma'rifa, Beirut, 1993.
3) Ahkam al-Qur'an, Ibn al-Arabi, edited by Ali al-Bajawi. Issa al-Babi al-Halabi Press, Cairo, 1967.
4) Al-Mughni, Ibn Qudamah, Dar al-Kitab al-Arabi, Beirut, 1983.
5) Ma'jam Lughat al-Fuqaha, Muhammad Rawwas Qalaji and Hamid Qunibi, Dar al-Nafais, Beirut, 2nd edition, 1988.
6) Al-Sahah, Al-Jawhari (edited by Ahmad Abd al-Ghafur Attar), Dar al-Ilm lil-Milayin, Beirut, 1987.
7) Lisan al-Arab, Ibn Manzur, Dar Sadir, Beirut, 1990.
8) Taj al-Arous, al-Zubaidi, Dar al-Fikr, Beirut, 2005.
9) Ma'jam al-Lugha al-'Arabiyya al-Mu'asirah (Dictionary of Contemporary Arabic), Ahmad Mukhtar Omar, Dar 'Alam al-Kutub, Riyadh, 2008.

Legal books and references

1) Youssef, Amir Faraj. Criminal Liability for the Crime of Electronic Extortion. Dar al-Muttaba'at al-Jadida, Egypt, 2023, p. 103.
2) Al-Naqib, Amani Yahya Abdel Moneim. The Crime of Electronic Blackmail Against Women. Dar Al-Fikr Al-Arabi, Alexandria, 2023, p. 112.
3) Al-Boushi, Ahmed Mohamed. Cyber Extortion: A New Concept in Cyber Threat Crimes. Dar Al-Nahda Al-Arabiya, Cairo, 2022, p. 65.
4) Fathallah, Mahmoud Rajab. Cyber Extortion Crimes. Dar Al-Jami'ah Al-Jadidah, Egypt, 2021, p. 80.
5) The Crime of Cyber Threats and Extortion, Mariam Araab, Journal of Comparative Legal Studies, Faculty of Law and Political Science, University of Oran, Volume 7, Issue 1, 2021, p. 12.
6) Tariq Namik Mohammed Reza. Criminal Liability for Cyber Extortion via Social Media. Master's thesis, Faculty of Law and Political Science, University of Kirkuk, Iraq, 2021.
7) Annual Cybercrime Report, International Criminal Police Organization (INTERPOL), Lyon, France, 2021, p. 45.
8) Article (16) of the Federal Law on Combating Information Technology Crimes in the United Arab Emirates, 2021.
9) Dr. Sahar Sharif Fakir. The crime of electronic extortion and ways to combat it. Omdurman Islamic University Journal, issue (unspecified), pp. 167-195; Al-Hikma Journal for Studies and Research, vol. 04, issue 05(19), 30/09/2024.
10) Barhal Amal. The Crime of Extortion through Electronic Means. Master's thesis, Faculty of Law and Political Science, Al-Arabi Al-Tebsi University, Tebessa, 2020.
11) Report of the United Nations Office on Drugs and Crime (UNODC). Countering Cybercrime. Second edition, Vienna, 2020, p. 78.
12) Global Cybersecurity: Challenges and Solutions. International Telecommunication Union, Geneva, Second Edition, 2020, pp. 24-26.
13) Hardo Center Report on Supporting Digital Expression. Legal Regulation and Cybercrime, 2018, p. 24.
14) Abdul Razzaq, Mamoun Muhammad. Penal Code – General Section. Part III, 2018, p. 18.
15) General Data Protection Regulation (GDPR), European Parliament, Brussels, third edition, 2018, Articles 33-34.
16) Kazim Abdul Jassim Al-Zaydi. The Crime of Cyber Extortion (A Comparative Study). Comparative Law Library, Baghdad, First Edition, 2019, p. 8.
17) Judge Ali Al-Zaidi. The Crime of Cyber Extortion. Comparative Law Library, Baghdad, Iraq, 2019, pp. 7-11.
18) Rami Ahmed Galbi. The Crime of Electronic Extortion and Mechanisms to Combat It in the Republic of Iraq. Our Security Culture Magazine, Iraqi Ministry of Interior, Issue No. 2, 2019, p. 47.

19) Mohammed bin Abdulmohsen bin Shalhoub. The Crime of Electronic Extortion: A Comparative Study. Supplementary research for a master's degree in Sharia law, Imam Muhammad bin Saud Islamic University, Riyadh, 2019.
20) Latouh Hawazim al-Sufdi. Criminal Liability for Misuse of Social Media: A Comparative Analytical Study in Light of Legal Systems and Islamic Law. Master's thesis, Islamic University, Gaza, Palestine, 2019.
21) Malak Atwi. Cybercrime. Annals of the University of Algiers, Issue (21), June 2012, p. 18.
22) Omar Taha Khalil and Afaf Badi Jamil. Jurisprudential and legal adaptation of cybercrimes. Journal of the Faculty of Heritage, Issue (17), 2015, p. 174.
23) Mohammed Ahmed Al-Razqi. Lectures on Criminal Law, General Section. 2002.
24) A Concise Guide to General Criminal Law, Tasawur Rahmani, Dar Al-Oloum Publishing and Distribution, Algeria, 2006.
25) Criminal Law: Introduction and Principles of Theory, Ali Rashid, Dar Al-Nahda Al-Arabiya, Beirut, 1974.
26) Explanation of Penal Law: Special Section, Muhammad Amin Dweidar, Al-Nahda Al-Masriya Library, Cairo, 1979.

International Agreements

1) Article (18) of the Law on Combating Information Technology Crimes in the Sultanate of Oman, 2011.
2) Malabo Convention on Cybersecurity and Personal Data Protection, African Union, Addis Ababa, 2014.
3) Budapest Convention on Cybercrime, 2001.
4) Article (10) of the Sudanese Cybercrime Act, 2007.
5) Article 176 of the Sudanese Criminal Code, 1991.
6) Article 428 of the Egyptian Penal Code, 1937, amended in 2003.
7) Article 430 of the Iraqi Penal Code, 1969.
8) Article 3 of the Saudi Arabian Anti-Cybercrime Law.

finally