Journal of Namibian Studies, 34(2023): 1499–1515 ISSN: 2197-5523 (online)

The legal framework to protect electronic network users (comparative study)

Daniah Majid Abdulhameed[1], Mohammed Amer Shinjar[2], Ekhlas Hameed Hamzah[3]

Abstract

The study aimed to identify the most prominent risks of using the Internet at the level of individuals and organizations, and to identify the legal and technological foundations necessary to protect Internet users. The study relied on a descriptive approach by reviewing and analysing studies and reports related to the subject of the study. The study is divided into two sections The study dealt with the dangers of using the Internet on individuals and institutions, and the legal and technological foundations for providing protection to individuals and institutions when using the Internet networks. The study concluded a set of conclusions, the most important of which are: The risks of using the Internet vary at the level of individuals and organizations. Facing the risks of using the Internet requires an integrated set of criminals, civil and other laws, as well as cooperation from institutions related to Internet services. In conclusion, the study recommended the need for international coordination to form an international organization concerned with issuing transnational laws to confront electronic crimes and risks.

Keywords: Internet Risk - Cybersecurity – Cybercrime.

1- Introduction

With the development of information technologies, networks and increased interconnection in the world, the risks associated with online communication have become increasingly urgent. Due to the global nature of such a connection without obstacles to the material borders, the network technologies challenge the international legal structure based on concepts such as the jurisdiction and sovereignty, where each judicial state is organized by the sovereignty of the communications that occur in its territory. Online connection, which goes beyond geographical and judicial restrictions, is a serious concern for national and international legal systems in its current form [1].

[1] Al-mamoon university College, Baghdad, Iraq

[2] Al-Bayan University, Baghdad, Iraq, mohammed.amer@albayan.edu.iq

[3] Baghdad University, Baghdad, Iraq

It is a partially dangerous concern due to the online communication features, such as hiding the identity of the participants in communication, as well as the lack of consistency of their efforts and the effects they can achieve. Communication with these features that work in an unlimited environment for the Internet opens the doors to a wealth of deviation, misuse and crime. Just as network technology has penetrated almost every field of life on this planet, as well as the risks associated with this technology. The crime, which, through network and computer technologies, has facilitated, electronic crimes, war, in turn - has become a cyber. Electronic crimes, electronic warfare and electronic terrorism are among the emerging phenomena that the law needs to be absorbed. Internet risks appear at different levels - national and national lessons (such as Internet crimes, cyber terrorism) and international (such as cyber war). Collectively, these concerns are described through the comprehensive concept of cybersecurity, at the national levels and the national lessons. Cyber security issues are primarily related to criminal matters. The main cases are highlighted by dividing the national criminal laws (objective and procedural) and the need to keep them. The diversity of national laws is one of the main reasons for the global weaknesses of cybercrime, because this diversity does not allow the development of a single legislative response to the global phenomenon. Many countries, especially developing countries, have criminal laws that specifically address Internet crimes, and they do not have enough ability to enforce laws [2].

At the international level, cybersecurity is concerned with the application of international law to the reality of networks and computer technologies, including the possibility of using it in modern war. Supporting behaviour - a distinction between the perpetrator between the state or the non -governmental actors - and the determination of the judicial jurisdiction of the perpetrator is great challenges, with all these challenges on hand, the effective legal regulation of the Internet assumes the creation of an application policy that can deal appropriately the essence of the problem and its technical complexity at levels Different, including legislative interventions in the form of criminalization and alignment; International cooperation; Cooperation with the private sector, vocational education and capacity building in terms of technical support and assistance, especially in developing countries [3].

2- Research problem

Although the Internet is widespread everywhere in modern society and plays a decisive role in many aspects of daily life, it was not supposed to use by many and for a large number of jobs that he

performs today. On the contrary, the internet was designed to allow a small group of scientists to share unconstructive reports, which has not been designed to secure sensitive information safely. Moreover, the Internet has not been designed to allow easy monitoring of the user's behaviour and has not been designed to protect from attacks that arise from inside the Internet itself. This inherent design continues today, unchanged significantly, while Internet uses have developed significantly. Ease and lack of disclosure of its identity that people around the world can access information systems via the Internet, as well as the defective design of the Internet, has created a security vulnerability in front of electronic attacks on an unprecedented scale [4]. E -attack targets vary, consumers, private sector and governments alike, the costs of such attacks. Electronic attacks are likely to increase and complicate, as instructions for advanced attack methods have become available on a broader scale for potential online attackers, which reduces the technical knowledge required to carry out an attack [5].

In this context, countries and the international community must work to develop legal and technological foundations to face the risks to which Internet users are exposed to individuals and nurseries. We can formulate the current search problem in the following two questions:

1. What are the most prominent risks of using the Internet at the level of individuals and organizations?

2. What are the legal and technological foundations necessary to protect Internet users?

3- Research importance

Electronic crimes and violations of Internet users are widely spread in recent times, and at the same time national and international laws stand unable to effectively legal these crimes and therefore it was important to determine the legal and technological foundations to protect Internet users, through which the necessary legislation can be developed Technology laws and solutions to counter the risks of Internet use.

3.1- Research aims

1. Determine the most important risks of using the Internet at the level of individuals and organizations.

2. Learn about the legal and technological foundations necessary to protect Internet users.

4- Research Methodology

The current research depends on the descriptive approach by reviewing and analysing studies and reports related to the subject of the study. The research will be divided into two topics:

The first topic: the risk of using the Internet on individuals and institutions.

The second topic: legal and technological foundations for providing protection for individuals and institutions when using Internet networks [6]. Then we show related conclusions and recommendations.

4.1- The risks of using the Internet on individuals and institutions

The technology space is the fourth field after the Earth, the atmosphere and the sea because of its clear impact on leading the basic tasks such as economic, commercial, health, government operations, national security and defence, and that security interests differ in the different materials and resources in it, and there is no doubt that private commercial sites differ from Government sites as well as financial sites, entertainment and social communication sites. Where the product of scientific and technological progress was largely dependent on networks and websites in most of the joints of life, but this broad use of electronic space has its risks in addition to its advantages, these risks may reach a threat to the security and safety of the country on the individual level of citizens or the national level of the state, As the practical reality has secreted many problems of incorrect use or violations of individual or government sites that appear in the form of electronic crimes, blackmail, money laundering, electronic terrorism, espionage and children's exploitation via the Internet. These threats show their danger more in the countries of the third world and Iraq, one of which is, where we often hear about honour crimes as a result of electronic blackmail that many women have been killed [7].

Cyber security threats include a wide range of illegal activities on the Internet. In general, they can be divided into two types of categories: crimes that target / harm computer networks or devices directly such as malware, viruses, service rejection attacks, crimes facilitated by networks or computers, and the primary goal of them is independent of the computer network or device such as fraud or Identity theft, fraudulent hunting, information war or electronic chase. There are different categories and types of electronic crimes. Electronic crimes can be divided mainly into three:

1 - Electronic crimes against people such as transporting children's pornography, harassment via e -mail, publishing obscene materials, or violating the privacy of citizens. These electronic crimes have a

negative impact on individuals and society as a whole, if they are not effectively confronted.

2 - Electronic crimes against all forms of property such as computer sabotage (destroying others' property), transferring malware such as the Melissa virus, and using various spyware to steal the company's secret data. These crimes have lost millions of dollars worldwide by destroying the computer and business network.

3 - Electronic crimes against the government include terrorist activities that penetrate or penetrate the government or army site [8].

Computer -based violations may be in the form of piracy, computers, unauthorized access, computer fraud, which is to obtain property through false allegations. Likewise, the theft of identity Online, strict identity theft, human trafficking devices, stolen credit cards or social security numbers, computers forgery, the fake user demonstrated as a legal user, children's pornography and online pornography are different forms of Internet crimes.

There are many common causes of electronic attacks in electronic space, more than 90% of web sites / web applications / computer systems are vulnerable to a type of web applications, so the electronic space is an open square for criminal activities for Internet criminals. From here a strong defence mechanism is required to protect cyberspace, especially since there are many reasons for weak computers and internet systems:

a. Ease of access due to the lack of homogeneity and complexity in technology, computer systems are vulnerable to unauthorized access or system penetration through a secretly planted logic bomb, key recordings that can steal access codes, advanced audio recordings; The retinal imaging devices, etc., can deceive biological standards and overcome the walls of protection from common methods to bypass the safety system [9].

B. The ability to store data in a relatively small space, the computer has a unique feature to store data in a very small space and that is why removal or derivation is either through an actual or virtual broker that makes it much easier.

C. The complexity of the code, computers operating systems consist of millions of codes that may not be 100 % safe. These security gaps are exploited by Internet criminals, benefit from these gaps and penetrate the computer system.

Dr.. Negligence: The e -criminal takes advantage of the position of weakness and human neglect while protecting the computer system, which in turn provides the cybersecurity and controlling the computer system.

E- Loss of evidence: Loss of guide is a common and clear problem as all data are routinely destroyed. Collect more data outside the regional scope, doubts about the effectiveness of the prevailing investigation technologies and participation in privacy concerns also paralyzes the investigation system of these crimes [10].

4.2- legal and technological foundations for providing protection for individuals and institutions when using Internet networks

Cyber security risks and threats must be tackled so that the use of electronic space remains as safe as possible by developing a strategy to address these attacks and violations by identifying and processing vulnerabilities and vulnerabilities in websites Technical, as well as legislation of legal texts related to information crimes and identifying the pillars of electronic crime that took a new form of the traditional concept of crime. While the applicable cybersecurity policy includes a wide range of considerations, legal procedures play a major role in preventing and combating cybercrime. This is required in all fields, including criminalization, procedural authorities, jurisdiction, international cooperation, and the responsibility and responsibility of the Internet service provider. In particular, at the national level, electronic crime laws often relate to criminalization - identifying specialized crimes for basic electronic crime actions. However, countries are increasingly aware of the need for legislation in other areas. Technological developments related to cybersecurity and cybercrime mean that - while traditional laws can be applied to some extent - legislation must also deal with new concepts and things, such as "computer data", which are not traditionally taken under law. In many countries, laws related to technical developments date back to the nineteenth century [11]. These laws, and still, are largely focused on material things - around which the daily life of the industrial community revolves around. For this reason, many traditional general laws do not take into account the peculiarities of information technology, information related to electronic crimes and crimes that generate electronic evidence. These actions are largely characterized by new, unfinished things, such as data or information, while the criminal law is often seen as the most relevant when it comes to cybercrime, the legal responses to broader concerns related to cybersecurity also include the use of other law branches, such as the law Civil and Administrative Law. Other divisions within these legal systems include objective and procedural law, as well as regulatory and constitutional laws, or law -based laws. In many legal systems, each of these systems is characterized by specific goals, institutions and guarantees. Cybercrime laws are usually found in the areas of objective and procedural criminal law. However, there are also important number of other legal fields.

4.3- Criminalization

At the national level, electronic crime laws are often related to criminalization, indicating the prevailing focus on identifying specialized crimes for basic e -crimes. On the global level, many judicial states tend to realize that the frameworks of criminal and procedural law have sufficient, although this hides major regional differences, as more countries see that laws are partially sufficient or insufficient at all. Also, while there is a high -level consensus on broad areas of criminalization, detailed provisions reveal more contrasting approaches. Consequently, crimes that involve illegal access vary to computer and data systems regarding the subject of crime (data, system or information), and with regard to criminalization of "abstract" access as an incomplete crime or a condition for more intention, such as to cause loss or damage [12].

The required intention for crime also differs in the curricula of interference with computer or data systems. Most countries require that the overlap be intentional, while others include reckless overlap. To interfere with computer data, the behaviour that ranges the overlap is from damaging or deleting data, to modifying, suppressing, entered, or transferring data. The criminalization of illegal objection varies according to whether the crime is limited to the transfer of non -public data or not, and with regard to whether the crime is limited to the objection to technical means. Not all countries are criminalized the abuse of computer tools. For those who do it, differences arise on whether the crime covers possession, publishing or using programs (such as malware) and / or computers access codes (such as the victim's passwords). From the perspective of international cooperation, these differences may have an impact on the results of double criminalization between countries.

4.4- Piracy and criminalization

Perhaps the problem in legal dealing with piracy is that criminalizing electronic activity is a very complex legal issue that involves a specific intention to enhance political goals, among other things. It may also be a challenge from the social acceptance perspective of such a crime, such as the examples of electronic attacks led by Anonymous due to the "Robin Hood" flavour of unknown intentions. Just as the mafia was once identified as organized crime, government authorities must benefit from an unknown appearance when discussing cybersecurity with the general public. This singularity with Anonymous will not be unjustified. According to a report published by Verizon in 2012, piracy activists (generally) surpassed Internet criminals as a group responsible for the largest damage caused by electronic attacks with absolute numbers in dollars. Moreover, Anonymous specifically has a high general grade due to its dependence on social media (Twitter extracts, YouTube pages and websites), brand mechanisms (Guy

Fawkes masks and label practices), political views in the context of carrying out electronic attacks on prominent personalities. There is no doubt that large sectors of the American public followed or influenced by the attacks of PayPal / Visa / MasterCard electronic, the interruption of Sony service, and the protests of the movement they occupied, on the other hand, the penetration is a comprehensive term that covers a number of works that instead of being a unique activity on This way. This is at least true for objective elements. Some of these actions have already been criminalized in various judicial states. These actions are crimes such as, for example, illegal access to computer data, interception and intervention. However, the attack may vary in its self -element, that is, the specific intention to achieve a specific goal or result [13].

4.5- Procedure and proof

The cross -border nature of cybercrime and electronic crimes in an electronic environment are the main difficulties faced by the application of law. Traditional assumptions about the observation of the perpetrator as he is preparing for, committing, or escaping from a crime, or escapes from it. The challenges of investigation in electronic crimes arise from criminal innovations by the perpetrators, difficulties in accessing electronic evidence, and internal resources, abilities and logistical restrictions. The suspects often use identity hiding techniques Opinion, new technologies quickly make their way to a wide criminal audience through online crime markets. Determining the perpetrator, investigation, and collecting evidence for crime may be difficult for various reasons. In addition to the challenges of concealing identity and obfuscation, the country that hosts the e - criminal and its activities may not determine what has been done as illegal, and therefore may not be able to prosecute him or cooperate in handing him over to trial elsewhere; The host country may not have valid agreements with the victim's state that obliges it to help collect evidence that can be used against the perpetrator; Or perhaps very volatile electronic evidence has been destroyed, or because it was routine transactions data that was not kept by the Internet service provider that the perpetrator used to commit the crime. Electronic space makes physical space unsound [14].

Therefore, at the procedural level, the main problem of implementing the national law lies in reconciling the historical truth that the police are practically and organized within the borders of the jurisdiction (associated with its nature with the sovereignty for law enforcement integrating traditional and new police technologies. While some investigative measures can be achieved with traditional forces, many procedural provisions do not translate well from a graphic and fundamental approach to an approach that includes storing electronic data and data flows in actual time.

The evidence is the means through which the relevant facts are proven by guilt or innocence during the trial. Electronic evidence is all these materials in electronic or digital form. It can be stored or transient. It can be found in the form of computer files, transmitters, records, descriptive data, or network data. Digital forensic medicine is interested in restoring - often volatile and easy to pollute - information that may have an affirmative value. Forensic technologies include creating "bit opposite" copies of stored and deleted information in order to ensure that the original information is not changed, the "fragmentation" encryption file or digital signatures that can clarify the changes in the information. This means that there are sufficient numbers of forensic medicine, the availability of forensic medicine, and accumulation by law enforcement authorities due to the huge quantities of data for analysis. The suspects use encryption, making access to this type of evidence difficult and take a long time without a ciphering key. In most countries, the task of analysing electronic evidence is the responsibility of law enforcement, the additional challenge is the use of technology by law enforcement agencies - at the present time, it seems that violators via the Internet better use the technological capabilities they possess. The presence of a related body of special knowledge and experience within the police force is the decisive element in the effective organization of cybersecurity. The plaintiffs must see and understand electronic evidence in order to build a case in the trial. Many developing countries worldwide do not have sufficient resources for public prosecutors to do so. Computer skills in the Public Prosecution are usually less than investigators' skills. The same applies to judges who deal with highly specialized cybercrime cases. Judicial training is on Electronic Crime Law, Evidence Collecting, Basic and Advanced Computing Knowledge is a special priority. While the methods differ, many countries are considered this good practice, because it guarantees fair acceptance alongside all other types of evidence. A number of countries outside Europe do not accept electronic evidence at all, making the trial of electronic crimes and any other crime that electronic information is proven useful. While countries in general do not have separate proof rules for electronic evidence, a number of countries referred to principles such as: the base of the best guide, the importance of evidence, the rule of rumours, reliability, and integrity, all of which may have a special application on electronic evidence [10].

4.6- Aligning laws

Many countries have elements of the legal enabling environment that deal with cybersecurity and cybercrime, but these national legal frameworks differ widely in terms of the way these issues are addressed. In today's globalized world, the law consists of many national, regional and international legal systems. Interactions

between these systems occur at multiple levels. As a result, the rulings sometimes conflict with each other, which leads to the conflict of the law, or failure to overlap adequately, leaving gaps in the judicial jurisdiction. These differences between national laws lead to a question about whether national legal differences in electronic crime laws can be reduced, and if so, the matter is to what extent. In other words, how important coordination of electronic crime laws is? This can be done in several ways, including through binding and non - binding international or regional initiatives. The basis of coordination may be a single national approach (with all others reviewing their laws in line), or, often, shared legal elements specific in the law of a number of countries, or are expressed in a multilateral instrument - such as the treaty or an international standard other than Bind [7].

One of the main arguments supporting the unification of laws through judicial states is to avoid safe havens and the pillars of the perpetrators. Consequently, if the harmful acts involved on the Internet are criminalized, for example, in the state “A”, but not in the state “B”, the perpetrator in the state B. B. He can be free to target the victims in the state “A” via the Internet. In such cases, State A. alone cannot provide effective protection from the effects of such national activities. Even when its criminal law allows the judicial jurisdiction to confirm the perpetrator in the state B., it will still need approval or assistance from the state "B" - either with regard to collecting evidence, or handing over the specified perpetrator. In order to protect persons subject to its jurisdiction, the state is unlikely to help the state in the event that behaviour is not criminalized in its country.

Adjustment can also allow the global evidence to be collected. The alignment of procedural law is a second and indispensable condition for effective international cooperation. In the above example, if the state "B" does not have the procedural power to urgently preserve computer data, as a way for example, the state A will not be able to request these facilities through mutual legal assistance. In other words, the state is required to provide assistance except within its territory, to the extent that it can do so in order to achieve an equivalent national [9].

4.7- The institutional arrangements for cybersecurity bureaucracy

The institutional arrangements supporting cybersecurity are varied, such as the curricula of issues. First, there is no single response that suits everyone to effective institutional design, as global institutional arrangements vary greatly. Second, not all cases of cybersecurity are yet specific institutional. The clearest is the field of electronic crimes, where practice indicates that cybercrime cases, once passed to legislation, are usually within the jurisdiction of law enforcement and the judiciary.

With regard to privacy, for example, a number of examples show the extensive practice of institutional responses:

In the European Union, in general, each country is mainly responsible for the interpretation and enforcement of data privacy violations. Usually, every independent agency data protection department has the authority to enforce against other government entities. For member states that have a criminal component of data protection legislation, national or regional prosecutors may be involved by the Department of Political Affairs in specific issues [14].

In Argentina, the National Data Protection Directorate (NDPD) is established under the Personal Data Protection Law responsible for digital data protection. NDPD is subject to the Ministry of Justice and Human Rights, in Canada, at the federal level, the PIPEDA (PIPEDA) Law is assigned its supervisory and enforcement role to the Canadian Privacy Commissioner (OPC), whose reports are submitted to Parliament, in Malaysia, the processing of personal data is organized under 2009 Personal Data Protection Law (PDPA). The Personal Data Protection Commissioner is appointed by the Ministry of Information, Culture and Communications and is responsible for implementing and enforcing personal data protection laws in Malaysia [15].

In South Africa, the Personal Information Protection Law (PPIA) requires that personal information be addressed only by an official party who has notified the information protection organizer (organizer), which provides its reports to the President of South Africa [3].

And if we look at the practical reality of cybersecurity in Iraq, we find that the Iraqi government formed the response team to cyber events, which works in cooperation with the Ministry of Interior and Communications and holds it responsibility for securing and protecting networks, national data centers and official sites that work in the Iraqi cybersecurity and the team coordinates National efforts and support for institutions in the public and private sectors to achieve sobriety and reliability of electronic systems and to enhance citizen confidence in institutions and improve the level of Iraq internationally in the field of cybersecurity to encourage and develop electronic services and support E -government project. The team has made many achievements by blocking and frustrating electronic attacks and attempts to penetrate networks and websites affiliated with sensitive governmental institutions. Where the CERT teams work to find measures and procedures to bridge the cyber security gap and address the basic weaknesses in it, as this team has formed several teams operating separately and consistently in terms of dividing and classifying the fields that must be worked on in a way that ensures the achievement of the desired goals during a specific time limit [16].

Strong government participation and institutional solutions in securing cyberspace are justified due to the strong dependence of the government on technology and electronic space for its own processes. In addition, the government has a unique advantage through which global economic, political and technological powers that can lead to electronic threats, at the international level, can monitor and understand an agreement that provides for international cooperation on cybersecurity and the implementation of global judicial jurisdiction On the actions of cybersecurity, the benefits will be tangible. One of these benefits is to provide an opportunity to create a United Nations agency that has the purpose of ensuring the safety and security of the Internet [15].

4.8- Employment of individuals and educational training

There is a pilgrim to expand efforts to appoint cybersecurity and educational training (especially law enforcement authorities, the judiciary and other authorities). For example, the United States government has established the National Institute for Cyber Security (NICE). Nice launched alongside the Ministry of Education and other strategic agencies from four axes to build a smart country via the Internet through training and awareness through educational programs after graduation and professional development of Federal Security Specialists. To achieve this goal, NICE targeted a wide range of population as potential employees: students and partners from the private sector [12].

Any legislation to reform cybersecurity should make these arrangements permanent. Government agencies must be granted power and resources to start new recruitment campaigns and expand the scope of current campaigns. The logical basis for this investment is two parts. First, in a world where communication is constantly increasing, more cybersecurity will be needed to manage this connection, so there will be a parallel increase in demand for cybersecurity. Second, by enhancing its presence in employment and education, the federal government can attract these individuals to fill the functions of cybersecurity who may have joined unknown ranks or other pirate groups. Certainly people opposed to the government or even indifferent to the government may not be persuaded by government employment efforts. But for those young people who show exceptional computer skills and seek a society that uses these skills and appreciates these skills, employment and education campaigns will definitely help governments in this task [16].

4.9- Technological solutions

There are two basic technical strategies to protect critical systems: (1) Defending the system from the dangers of the Internet while the system remains on the Internet, and (2) air gap in the system and

public networks, that is, separating these important systems from the Internet Completely by the authorities. Such proposals were recently popular with some politicians in light of developments with the National Security Agency leaks.

1 - Defence and monitoring systems

The United States government is partially protecting computers and networks with an infiltration system called "Einstein". The Einstein program is designed to conduct actual time monitoring and make decisions based on threats and provide an intrusion system for any activity in some countries. In the performance of these jobs, Einstein shares information and cooperates with the Ministry of Internal Security and the National Security Agency. Thus, within its own network, the United States government is currently in its own network, in close coordination between departments, and deleting personal identification information from joint cybersecurity data, and works on the basis of actual time response, for the private sector defence systems, or to preserve electronic health, believes many Cyber security experts that the main cyberspace security science is a simple and logical first step in cybersecurity for companies. Estimates indicate that the maintenance of good cyber security can prevent up to eighty -five percent of the online intrusion. Instead of waiting for legislative delegations to stimulate spending on cybersecurity for companies, it would be wise for companies to think if there is something that justifies some pre-emptive investments in e -health as part of their basic responsibility for companies. However, even basic e -health, not to mention complex programs such as Einstein, is expensive for some companies [4].

If the private sector is not supported in providing the private sector with high -cost defence systems, an important source element can be seen to develop technical solutions for the private sector in identifying weaknesses, security violations and potential risks. This can be achieved by communicating with the decisive results about the weaknesses of network owners and the private sector.

2 - Standardization and air networks

Standardization can be seen as a distinction and a defect. The criteria are necessary for the inter -operation of the products by many sellers. The possibility of inter -employment is very important in national communications and infrastructure, including the national energy network and medical and financial institutions. The result of tens of thousands of the criteria used is a greatly connected world. Biomedical operationalism in biomedical infrastructure assets helps prevent and obstruct cybersecurity risks through, for example, developing improved standards for the browser safety, applications security and email authentication [8].

With the increased interconnection and standard standards, the increasing weaknesses come, both for external and internal threats. The use of identical security operations on each computer network does not seem the perfect solution - at least not without balancing competing costs. The negative effect of the inter -operational capacity is to increase the weakness of the entire system, which facilitates access to the rest of the systems as soon as part of it is at risk. This includes the spread of viruses and other harmful programs, as well as piracy. He should Defending such systems should be completely inconvenient to overcome the risk, which is in themselves far, if possible at all, some commentators suggest separating the system's important networks from the Internet completely; A system such as power generation and water distribution, and the basic services that the nation relies on to remain operating. The security industry indicates this process as the creation of a "air gap" between the ultra -critical systems and the public network. The air gaps may be somewhat exhausting, but the security reward is unparalleled: the isolated air systems are completely isolated and in practice that the attacker was not actually able to reach the system [2].

5- Conclusions

1. The risks of using the Internet vary at the level of individuals and organizations, and these risks are characterized by continuous development and the emergence of new and innovative forms of them every period.

2. Facing the risks of using the Internet requires an integrated set of criminals, civil and other laws, as well as cooperation from institutions related to Internet services.

3. The fact that the risks of the internet transit to countries require international and security cooperation for the effectiveness of their confrontation.

4. There is a problem related to the budget between the protection of Internet users from risks and the freedom to use the Internet as a result of the exploitation of some countries for cybersecurity claims to restrict the freedoms of expression.

5. Current laws are historically linked to the grace of material crime, which requires the redefinition of the concepts of procedures, evidence and criminal evidence in the inappropriate internet environment.

6- Recommendations

Despite the great achievements of the CERT team referred to in Lebanon, we wish the relevant authorities in the Iraqi government to

take more steps and procedures towards enhancing the strength and protection of information systems, whether governmental and individual, and this is achieved through several directions:

The first trend is the legal trend, which can be achieved through:

1- Legislation of a law on information crimes concerned with the concept of electronic crime, its staff, controls and provisions, as the Information Crime Law in Iraq is still a draft offered for study and discussion and has not yet been approved

2- Including the study of law in universities for the concept of electronic crime and the development and investigation methods

3- Developing the skills of judges and workers in the field of forensic evidence in the concept of digital crime

4- The joint international cooperation to combat cybercrimes by entering Iraq in international treaties and agreements concerned with this field

The second trend is the technical or technological trend: which is achieved through:

1- Building and developing a national technology framework for cybersecurity, which defines the requirements for controlling cybersecurity in Iraq.

2- The creation of a team specialized in the field of cybersecurity in government institutions works to provide continuous protection for official government sites.

3- Working to raise the level of the ability and skills of workers in the field of cybersecurity to keep pace with the continuous development in this field through the establishment of continuous courses, training programs and external missions so that the practical level remains in keeping with the rest of the countries.

4- Supporting and developing private companies working in the field of technology and achieving cooperation with them so that their experiences can be used to achieve security against cyber-attacks.

The third trend is the social trend, which is achieved through:

1- Working to increase the individual awareness of the concept of cybersecurity and the risks that they may be exposed to as a result of their use of websites of all kinds.

2- Spreading the awareness and culture of reporting any penetration of personal sites or exposure to extortion and providing the necessary security protection for individuals, taking into account the preservation of the privacy of information, and this aspect is achieved through cooperation with the relevant authorities in the Ministry of Interior.

3- Women give women to work in the field of cybersecurity more by enabling them to take office and not limit or marginalize their role in government institutions or private companies.

Bibliography

1. Abu Hamama, Hassan Ali Abd (2018). The crime of spoiling the child online: a comparative legal study "France, Egypt, Jordan". Amman Arab Research Journal - Legal Research Series, Maj 1, A1, 125-156.
2. Ahmed, Mustafa Mohamed (2020). The legal framework for electronic consumer protection of e -commerce risks. Journal of the College of Law for Legal and Political Sciences, M. 9, 34, 90-135.
3. Al -Saleh, Ibtisam Musa Saeed (2018). The subject of the crime of electronic theft in Jordanian and comparative legislation. Journal of Legal and Political Sciences, Q8, A4, 93 - 128.
4. Al -Dinawi, Zainab Muhammad Jamil (2019). Legal protection for privacy on the Internet in light of international and internal efforts. The International International Forum: Privacy in the Information Society, 23-37.
5. Al -Mansouri, Salem Bakhit Treibish (2020). Electronic crimes in people. Moroccan law magazine, p. 43, 27-42.
6. Al -Naimi, Faisal Ghazi Muhammad (2022). The legal basis for the crime of electronic blackmail for children and the interest it is considered. Maysan Research Magazine, Maj 18, A 35, 367 - 394.
7. Al -Nimr, Raed Muhammad Falih (2019). Protecting the privacy of social media users in light of legislation in the Kingdom of Bahrain. The International International Forum: Privacy in the Information Society, 87-106.
8. Al -Hajri, Latifa Salem (2021). Attempting electronic crimes: reading in Qatari and Egyptian legislation. Journal of Law and Business, p. 69, 94 - 122.
9. Anjom, Omar (2018). The legal legal system to establish digital confidence. Journal of Law and Business, p. 24, 40 - 66.
10. Bin Abdullah, Zahra (2019). The criminal protection of the child from sexual exploitation crimes via the Internet. Judicial ijtihad magazine, Maj 11, p 1, 273 - 290.
11. Bin Odeh, Houria (2019). The developments of international protection for privacy. The ninth school day: guarantees of the right to private life and its reality at the international and internal levels, Maj2, 84 - 120.
12. Badan, Khaled (2021). Legislative and technical protection of the right to privacy via the Internet. Adalah magazine for legal and judicial studies, p. 15, 167-178.
13. Tijini, Amin (2020). Information crimes. Journal of Legal Studies and Research, p 6, 115-137.
14. Safar, Samer Hamid (2020). Legal protection for privacy in the virtual world. Arts, Literature, Humanities and Sociology Magazine, 48, 101-112.

15. Sheikh, Sana (2021). Criminal protection for private life online in Algerian law. Journal of Law and Business, p. 64, 66 - 80.
16. Abshat, Amina (2021). Electronic crimes between international covenants and national legislation. The Algerian Journal of Rights and Political Science, M. 6, A1, 248 - 261.