MODERN TRENDS TO COMBAT AGAINST CYBERCRIME

Dr. MUS'AB TURKI IBRAHIM NASSAR
Assistant Prof. of Criminal Law ,Ministry of Interior /Police Collage,Qatar.

Abstract: *Cybercrime is an important challenge faced by specialists in international and criminal law, because of the difficulty in determining their nature and elements, and the consequent criminal, civil, or international responsibility, as some states resort to them to have dominance over the armed conflict issue, or to pose political or military threats. The researcher indicated the difficulty to include cyber crimes in the current international legal framework due to their nature and the absence of a formal and final legal declaration agreed on. The researcher recommends the establishment of public-private sectors partnerships, at multi levels to fight cybercrime, as they are transnational crimes.*

Keywords: *Crime confrontation, Cybercrime, International law, Criminal law.*

Introduction:

Crime is considered a social phenomenon in all advanced and backward societies, and some describe it as an anti-social behavior that violates the law and the culture of society, and on this basis it is found in all societies with different features from one society to another.

International studies and reports on the development of crime in various countries of the world indicate a rise in its rates and trends towards an increase year after year.

Because of the tremendous development in the means of communication and transportation, the forms of crime and the methods of committing it have developed, and the crime has gone beyond crimes of assault on oneself and money to new crimes such as cyber crimes.

Since, in conjunction with this great development on the Internet and the increase in dependence on it, the so-called (information hackers or hackers) appeared, and they are people who have deep experience in the field of information technologies and computers, and they have the ability to access prohibited sites in computer network systems of various forms, Their activities target important websites, such as the websites of military and financial institutions, where they infiltrate those institutions' websites with the intent of obtaining secrets or documents, publishing political protest messages, or even collecting money.**(1)**

In recent years, the material and moral damage caused by cyber-attacks, to which countries, organizations and individuals have contributed, have increased, and these attacks have become of concern to countries and governments in the international community due to the multiplicity of parties that carry out these attacks and the difficulty of tracing their sources or determining the place of their launch.

On this basis, the Internet has become a battlefield and conflicts via espionage and control of databases that affect the national and vital security of some countries, and these were called "cyber attacks", which became one of the most effective and inexpensive means, As a result, the world and the international community are faced with a new type of arms race, which is the arms race with computer technology through the creation or development of electronic programs intended for military or security purposes known as "cyber", where these programs can, at the click of a button, hack and commit technical actions harmful to others. across the virtual world, Where the fate and future of countries depend on their ability in confronting and dealing with cyber attacks, and the world is witnessing new dimensions in the way of fighting and the method of building the capabilities of the armed forces of countries **(2)** .

Cyber crimes have become one of the most important challenges faced by specialists in international and criminal law, due to the difficulty of determining their nature and elements, and the consequences of these attacks on international criminal or civil responsibility, especially since these attacks may be resorted to by some countries in order to achieve gains such as hegemony On the reality of the armed conflict or directing political or military threats to other countries, In addition to the negative consequences of criminal and terrorist threats that these attacks may produce if non-international groups resort to performing them in order to obtain political or economic advantages (3).

Accordingly, it is necessary to address the growing wave of this type of crime, by working to combat it and limit its penetration in safe societies, and this can only be achieved by working to prevent crime and enacting legislation that punishes and prevents such crimes.

Therefore, through this research paper, the researcher worked to shed light on an international phenomenon that has become present and the international community is experiencing it and working to confront its negative effects, namely “cyber crimes”, whose legal adaptation has become the biggest challenge for specialists in international and criminal law, and to indicate whether they are prohibited or restricted. In accordance with the provisions of international law, through the following two topics:

The first topic: the nature of cybercrime

The second topic: International trends in combating cybercrime

Study problem:

The cyber attacks that emerged at the end of the twentieth century constituted the most important challenges faced by legal professionals; This is because of the ambiguity surrounding this term, as cyber-attacks or crimes against websites are one of the most dangerous types of attacks, as it is a war taking place in a virtual world that no one feels, the risks in this field lie in the difficulty of identifying the entity that carried out the cyber attacks in many cases, as well as the absence of international legislation that places countries or institutions that carry out such activities under the law, which means the inability to prosecute them legally, hence the problem This current study in that it attempts to answer the main question it revolves around (modern trends in combating cybercrime?).

Study questions: The current study attempts to answer the following questions:

- What is the concept of cyber?
- What is cyber crime?
- What are the types of cyber crimes and their sources?
- What are the aspects of international cooperation in combating cybercrime?
- What are the national efforts in combating cybercrime?
- What are the obstacles to international and national cooperation in combating cybercrime?

Study objectives:

The study aims to achieve the following objectives:

- Clarify the concept of cyber.
- Identify the elements and sources of cybercrime.
- Clarifying recent trends to confront cybercrime.
- Identifying the obstacles facing international and national cooperation in combating cybercrime?

The importance of the study:

The importance of this study emerged from the importance of the topic it deals with, as information crimes have spread dangerously in all countries of the world, which have become vulnerable to falling under the threat of these crimes by using viruses, spyware, and others.

Consequently, cyber crimes and hacking of sensitive Internet sites have attracted the attention of researchers and scholars in the field of international and criminal law alike.

Study Methodology:

The nature of the topic covered by the study requires the researcher to take a specific approach, as the researcher will adopt an integrated and complex methodology to find a comprehensive framework for analysis, and the most prominent of these approaches are:

1. The descriptive approach: This approach means studying the phenomenon as it exists in reality, describing it accurately and stating its characteristics, and giving it a numerical description through numbers and tables that show the amount of this phenomenon, its size, or the degree of its connection with other phenomena.

2. The Analytical Approach: This approach is concerned with defining and evaluating the parts that make up the whole for any issue, and it is a means of obtaining rich and new knowledge.

It is known that the analytical method takes analysis in different forms and levels depending on the nature of the research topic, and the multiplicity of analysis processes is a condition to provide a more general and comprehensive understanding of the issue under study, as it works on analyzing the topic into simple elements or dividing the thing into its components and units, as well as through analysis He explained the opinions of scholars and researchers on the subject of the research.

3. The comparative approach through a comparison between Jordanian and Qatari law and international agreements.

The first topic

The nature of cyber-crime

The world has recently witnessed rapid developments in the fields of computing and information technology, which have brought about far-reaching changes in all areas of life, especially in the military and security fields, which have witnessed many changes related to the way of fighting and the way to build the strength of armies.

The cyber used in electronic warfare affected the patterns of this war, and accordingly, the country that owns the technology has gained superiority on the battlefield through qualitative and comprehensive intelligence and an accurate offensive ability **(4)** .

Many researchers point out that the term cyber is one of the terms that talk about a hypothetical concept whose interactions revolve in the Internet space, but this perception is wrong perception to a large extent, as the Internet and computer networks, in general, are one of the fields of electronic warfare that exceeded their weapons in destructive power, The capability of conventional and high-powered weapons.

Cyber-war is the actions taken to achieve an information advantage by influencing the enemy's information and systems and defending private information and systems.

Military operations in cyberspace are one of the emerging aspects of warfare, as operations such as network defense, intelligence gathering, and morale targeting (5).

And the attacks that are carried out in the (cyber) space all represent the field of the electronic battle of the future, through which the attacks will be launched by penetrating supply chains, electronic intelligence, implanting malware and other operations that are used in those attacks.(6).

Digital technologies and their development have increased the effectiveness of cyber wars. The first announcement of digital technologies entering the battlefields in the Balkan war at the end of the last century was at the hands of NATO against the Serbs in what were called “dark bombs.” This cyber attack led to the computer network being suspended. The main thing, which completely paralyzed the computer systems of the Yugoslav Ministry of Defense, Today’s reality is full of many variables that push us to shed light on this new military method, which has imposed itself forcefully on the reality of armed and unarmed conflicts in our world today, and this phenomenon will be highlighted as follows:

The first demand: Definition of cybercrime

The second demand: forms of cybercrime

The third demand: the sources of cybercrime

The first demand

Defining cyber crimes

Many terms and concepts have been given to cyber-attacks. The term virtual warfare, electronic warfare, or cyber-war has been applied to cyber-attacks in which hackers attack files and websites that belong to others, such as attacking websites of important facilities or attacking Computers belonging to military units or economic units of countries with the intent of destroying and controlling them and harming that country **(7)** .

Cyber-attacks is a modern term that appeared in recent decades as a result of the information technology revolution, and cyber-attacks were not known until recently, which constitutes one of the most important current challenges faced by specialists in public international law, with regard to determining their nature, definition and elements, especially They target all computers, the information within them, systems, programs, and networks that are open for use by the general public, or those networks that are designed for the use of a specific class of users and are separate from the public Internet **(8)** .

Cyber-attacks are shrouded in great ambiguity, which resulted in difficulties faced by specialists in public international and humanitarian law in particular in determining a specific and agreed-upon definition of cyber-attacks.

The cyberspace in which cyber attacks take place can be described as a virtual world with our physical world, in which it is intricately affected and affected by where cyber attacks depending on computer systems, Internet networks, and the huge stock of information and data, where the connection to the Internet is done through computers, phones, and other devices without being restricted by geographical borders.

Therefore, cyber-attacks in this direction can be described as a realistic behavior that takes place in a virtual world based on the use of digital data and electronic means of communication, and then the development of this concept, as it became broad based on the achievement of concrete and direct military or security objectives, as a result of Hacking sensitive websites, usually performing functions classified as the priority, such as the protection systems of nuclear or electrical power plants, airports and other means of transportation **(9)** .

Cyber-attacks are defined as combative means by using them to infiltrate electronic systems designed to protect or regulate the workflow of vital facilities, such as nuclear power plants, dams, or transportation means such as airports, with the aim of controlling them to self-destruct by feeding them incorrect information to the control devices. and electronic protection, But this trend was criticized, because there is a trend that saw the classification of cyber attacks as a combative means may not be correct, because cyber-attacks lack kinetic energy, which is the most important characteristic of conventional weapons, so it is not possible to feel the cyber attack in a way, In addition, the means of cyber-attacks do not contain explosive materials, and therefore cannot be considered as a means of combat **(10)** .

And some of them defined cyber attacks as the fourth arm of modern armies next to the air, land and sea forces, especially since the Internet era witnessed the beginning of talking about real battles taking place in this virtual world, and there are those who believe that cyber-attacks represent the fifth dimension of war. In this direction, cyber-attacks were defined as: “a set of measures taken by the state to attack ordinary information systems with the aim of affecting and damaging them, while at the same time defending the information systems of the attacking country” **(11)**.

The second demand

Forms of cybercrime

There are many forms and types of cyber crimes through which electronic weapons are used, and the most prominent forms of these crimes will be addressed, as cyber crimes are divided into three levels, which are as follows:

Level one: electronic espionage

Electronic espionage (Cyber espionage) is hacking a network or an electronic device with the aim of stealing the information on it, which is usually of great importance, whether it is military, economic, industrial, commercial, or other information, which has consequences an outrageous strategy on the target party **(12)** .

This level describes against individual electronic privacy, which constitutes an attack on the personal rights of the individual and a violation of private life, including the theft of financial data and its dissemination via the electronic information network (the Internet), or a person creating a file through a computer that contains information belonging to another person without His knowledge, permission, or tampering with digital records and changing their stored entries in databases **(13)** .

And because these crimes can cause great losses in a limited time, a number of countries have resorted to them, either during times of political conflicts and political tension with other countries or during wars in conjunction with traditional military operations, Among the most prominent examples of cyber-espionage carried out by countries against others is what was mentioned in the report of the investigation committee formed by the European Parliament in (2001 AD), which accused the United States of using an electronic espionage network under the name (Echelon network) established during the Cold War To spy and steal industrial information of European industries **(14)**. It should be noted that countries are not the only target for such attacks, but also companies, whether commercial or advertising, and non-governmental organizations, which are also exposed to many electronic or cyber-espionage operations.

The second level: is the information warfare between companies and institutions

This level revolves within the framework of competition between companies and institutions based on anticipating everything to disrupt the competitor and threaten its markets, so that a certain company penetrates the information system of its competition, stealing the results and details of its research, destroying its data and replacing it with other incorrect data **(15)**.

Level Three: Global information warfare (Cyber Warfare).

Electronic warfare or cyber warfare refers to a war that is conducted in the field of cyberspace in which the main actors are states, and in which electronic mechanisms and weapons are used in the attack so that this attack is directed primarily at the computers or electronic networks of the enemy or The electronic systems that run the state and the information they contain with the aim of obstructing the opponent from using these systems, devices, and networks or destroying them completely **(16)**.

This level represents the wars that take place between some countries or that global economic powers may wage against specific countries in order to steal the secrets of opponents or enemies and direct that information against their interests, as the country that owns this technology enjoys superiority in the battlefield through intelligence A qualitative and comprehensive, accurate and blitz attack ability, and the ability to defend its vital infrastructure, in addition to high capabilities for command-and-control and what follows, However, the development in the field of information technology, in particular computers, means of communication and electronic networks, made it possible to target the opponent, an individual, a country or an institution, in new ways that suit the nature of that development **(17)**.

In general, three main levels of cyber warfare or cyber attacks can be identified as follows:

First: This is represented in those operations accompanying conventional wars to achieve knowledge superiority, such as attacking the air defense system, which leads to large-scale strategic losses as a result of the importance of air defense for countries.

Second: It is represented in limited electronic warfare, in which infrastructure and civilian targets are exposed to cyber attacks.

Third: It is represented in unlimited electronic warfare, through which the attacker seeks to maximize the destructive effects of the infrastructure, as it negatively affects the social structure of the state, such as attacking the capital markets, emergency services, electronic systems for power generators, and other goals that entail Large-scale destructive effects, and the purpose of this type of war is to extend the range of material losses as much as possible **(18)** .

Accordingly, cyber attacks target specific information or information systems at the party to be attacked, in order to increase the value of that information or systems for the attacker or reduce its value for the defender, or both, because the value of the information and its systems is the measure of the amount of possession of the attacker or defender. With information and organized it that the goal that the attacker seeks in his war to achieve may be financial goals, such as stealing and selling records of bank accounts, and that war may be for political or military purposes or even just for excitement and to show capabilities as in the case of information hackers **(19)** .

The third demand

Cybercrime sources

It is clear from the above, that cybercrime is no longer limited to hackers who work individually or collectively, or organized criminal groups that aim to achieve material gains, but the circle of perpetrators and sources of these attacks is also expanding to include all countries which may resort to electronic attacks, As an instrument of foreign policy, states may also cooperate with other sources by providing financial and technical support to complete a cyber-attack against a specific target in accordance with their interests **(20)** .

In general, the sources of cybercrime and those who have the ability to launch cyber attacks can be divided into three main categories, which are countries, organizations, and individuals, and each of them will be explained according to the following detail:

First: the countries

Countries represent the biggest danger and the most powerful actor in the field of cyber and electronic space. At the end of (2008 AD), about 180 countries were able to possess an arsenal of electronic weapons, which may push countries and others to compete in the coming years in order to achieve electronic supremacy, as a result of Because cyberspace provides opportunities for countries to achieve their interests, and the electronic capabilities of countries are generally divided into defensive and offensive capabilities, the capabilities of the state increase in the electronic field as its offensive and defensive capabilities increase, and its dependence is relatively less on cyberspace compared to other countries **(21)** .

The more a country relies on cyberspace, the less vulnerable it is to cyber attacks, because of the consequences of that reliance on the state's vulnerability to cyber-attacks and the increase and severity of the damage that may be inflicted upon it in the event of such an attack **(22)** .

An example of this is what happens between countries through spy wars in order to obtain strategic and military information about other countries, such as the spy wars between the United States of America and the Soviet Union during the Cold War and what some countries are seeking at the present time by using communication and information networks to achieve The same goals are spying, hacking, and then destroying websites, whether those conflicts are motivated by political or competitive motives, or they revolve around obtaining information, influencing ideas, waging psychological and media warfare, and leaking information **(23)** .

In general, despite the widening range of sources and means capable of making an impact in cyberspace, states are still the most important factor in this field, capable of launching the most complex cyber-attacks and the most threatening to the peace and security of the international community.

The technical, military and financial capabilities of states cannot be compared to any other party. Therefore, states are the most dangerous source of cyber-attacks on the international scene **(24)** .

Second: non-governmental organizations (NGOs)

The role played by non-state sources in the field of cyberspace outweighs their role in any other field; whether in terms of their ability to interact or influence the security of states, and these organizations play a prominent role in the field of cyberspace and a source of cyber threats.

Some of these organizations are small organizations that seek to make a quick profit before they are discovered by governments and the enforcement of the law on them. Others operate at the global level and may be protected by some governments. Perhaps the most dangerous types of these organizations are criminal organizations, which are divided into two types: Traditional criminal organizations use cyberspace to carry out their traditional attacks, and the second type is represented by cybercriminal groups, given that cyberspace is the only area of their work **(25)**.

Third: Individuals: There are four categories of individuals who are able to launch cyber attacks, which we will explain in the following detail:

1. Newbies: The main objective of these attacks by newbies is to achieve adventure and excitement and to be accepted in the hacker community **(26)**.

2. Hackers: This source represents what is known as hackers, and these work through software penetration of computers. This category is considered an amateur hacker category, in addition to the category represented by professional hackers, or what is known as (Crackers), They have the ability to control computer programs and ways of managing and hacking them and knowing their content illegally and unauthorized, either directly by obtaining the password or indirectly by capturing the electromagnetic waves emitted by the computer during its operation and translated **(27)** .

3. Political hacking: It is what combines the term electronic hacking with political activity, and the motives behind political hackers carrying out cyber attacks are primarily political and not aimed at achieving personal interests **(28)** .

4. Electronic terrorist groups: Electronic terrorist groups are similar to political hackers in the type of attacks they carry out, as their attacks are often motivated by political purposes, but the scope of the attacks they carry out is different from hackers, the main goal that seeks The aim of cyber-terrorists is to harm goals that are of great importance to the state and society, whether they are economic, political, or commercial, while the goal of political hackers may be only political pressure without necessarily causing severe damage **(29)** .

Through the above, the researcher believes that the twenty-first century has witnessed a great development in the spread of cyber crimes, as these crimes in this century have become the second unconventional Cold War, which began in (2000 AD) to the present day, The reason for this, as we have indicated, is the increased reliance on the Internet by countries and public and private institutions, which increased the chances of launching these crimes and cyber attacks on those sites, and by reviewing the countries that have been subjected to cyber attacks, we find that they are among the major and technologically advanced countries such as the United States of America, Israel and China, this indicates that despite the tremendous development that countries seek to fortify their institutions and confidential information in their sensitive facilities, these cyber attacks are capable of penetrating those systems and causing sabotage and destruction in them.

The second topic

International trends in the fight against cybercrime

Cybercrime is one of the cross-border information crimes that have emerged recently with the technological spread of its connection to the computer, and the tool of cybercrime is the Internet. It is characterized by the nature of resourcefulness and cunning on the part of its perpetrators through the use of highly efficient information technologies, which leads to the penetration of networks and computers connected to the Internet, where the security system of the network is penetrated and access to the device to reveal its contents or destroy it and manipulate the information stored in it **(30)** .

Because of the seriousness of this crime and the difficulty of detecting it and the absence of physical evidence that condemns its perpetrator, it has become a significant and noticeable growth on the crime scene as a result of the absence of an effective strategy to combat it at the international level in light of the lack of international agreements and the difficulty of international cooperation to reduce it, which prompts this situation to put forward Several questions, the most important of which are:

- What are the international efforts to combat cybercrime?
- What is the nature of the international policy followed in combating and countering such crimes?
- What are the national and international measures that can be taken regarding these repeated crimes?

Through this study, these questions will be answered, as follows:

The first demand: aspects of international cooperation in combating cybercrime

The second demand: national efforts to combat cybercrime

The third demand: Obstacles to international and national cooperation in combating cybercrime.

The first demand

International cooperation in combating cybercrime

As we mentioned earlier, the emergence of the computer and the Internet is one of the most important achievements of modern science in this era and the greatest benefit to man, as these achievements (computers and the Internet) provided services to humanity in most aspects of economic, educational, medical life and many other fields.

However, these achievements were accompanied by the emergence of new experts with expertise and craftsmanship in adapting this technology to carry out criminal acts, which led to the emergence of modern technical crimes in addition to traditional crime, Rather, it transformed crime from its normal character and limited dimensions to new dimensions that depend on technology in the implementation of the act. Innovative methods and new methods that were not known before, these criminals have benefited from the development of modern informational means, increasing the speed of spreading their crimes until they threaten the information system. Rather, they can cause complete paralysis of civil and military systems, land and space, disable electronic equipment, penetrate banking systems, disrupt air traffic and paralyze power stations. And others by means of information bombs sent by a computer keyboard from distances exceeding tens of thousands of miles, making cybercrime an international cross-border crime **(31)** .

These criminal acts drew the attention of countries and international bodies that realized their danger, ease of perpetration, and direct impact, making combating them one of the first priorities of the international community and governments to put in place legal protection mechanisms to confront these criminal acts, as many countries of the world were busy issuing legislation and regulations to combat this crime, Therefore, international legislation, regulations, and treaties began to spread to combat this crime in the countries of the world, but these laws were marred by shortcomings and impotence in the pursuit of cybercrime because it is a crime that originates in a country has its effect in another country, and its evidence is spread across other countries, the difficulty appears in any law governing in Cybercrime **(32)**.

These crimes led to the emergence of new challenges to the legal system at the international level, especially after cybercrime cast a shadow over the entire world. Therefore, international efforts joined forces to combat this phenomenon effectively and efficiently, the first of which was the efforts made at the level of international bodies that played a remarkable role. In this field, especially the United Nations has made great efforts in combating cybercrime and urging international cooperation to curb the spread of this type of crime **(33)**.

These efforts were translated through international conferences for the prevention of crime and the treatment of criminals, starting from the Seventh Conference in 1985 AD until the Twelfth Conference in (2012 AD), in addition to the fifteenth Conference of the International Association of Penal Law under the supervision of the United Nations in 1994 AD. Which resulted in several recommendations and decisions related to cyber crimes and information crimes, as these recommendations and decisions included two aspects, the first is a substantive aspect that deals with the actions that fall under the penalty of information crime, and a second procedural aspect includes the procedures to be followed to apply the objective rules to information crimes **(34)**.

The resolution issued by the Eighth United Nations Congress on the Prevention of Crime and the Treatment of Offenders (Havana_1990) regarding computer-related crimes is one of the efforts made by the United Nations, as this Congress was held in Havana. This resolution on computer-related crimes urged Member States to intensify their efforts To combat the misuse of this device and to criminalize such acts, It also urged Member States to redouble their activities at the international level to combat computer-related crime, including their entry as parties to treaties on extradition and mutual assistance in special matters related to this crime, This resolution urged Member States to ensure that their legislation related to extradition and mutual assistance in criminal matters should be fully applicable to new forms of crime such as cybercrime, and to take specific steps towards achieving this goal **(35)** .

It was also agreed between states to issue the (UNCITRAL Model Law) in the conviction of states of the need to prevent and combat these crimes, especially since this requires a dynamic response in light of the international nature and the international dimensions of computer misuse and related crimes, as the UNCITRAL Model Law was drafted on Electronic commerce, and the other on electronic signatures (2001 AD) **(36)** .

In addition to the great effort made by the International Telecommunication Union within the framework of the global information security program announced by the Secretary-General of the Union in (2007 AD), which aims to achieve several goals, most notably the development of model legislation to combat information crime with a view that can be applied globally and be usable with existing legislative measures at the national and regional levels **(37)**.

At the regional level, there are great efforts by regional organizations. The European Union had an active role in this field, as its efforts resulted in the first international treaties on combating cybercrime; an agreement was signed in the European Union in (2001 AD).), in the Hungarian capital Budapest, This agreement sought to build a common criminal policy in order to combat information and cyber crimes around the world by coordinating and harmonizing national legislation with each other, strengthening judicial capabilities as well as improving international cooperation in this framework, in addition to determining penalties for cyber crimes within the framework of Local laws, and the European Union has established agencies to help combat this type of crime, including the Europol and the European Center for Combating Information Crime, which was opened in 2013 (AD) **(38)** .

On the Arab level in this field, great efforts have been made in combating cyber and electronic crimes. These efforts resulted in the establishment of an Arab agreement to combat information technology crimes, which emerged from the joint meeting of the Council of Arab Interior and Justice Ministers held at the headquarters of the General Secretariat of the League of Arab States in (2010 AD), with the aim of strengthening cooperation between Arab countries in combating information technology crimes and cyber crimes that threaten their security, interests and the safety of their societies, and to meet the need to adopt a common criminal policy aimed at protecting the Arab community against information technology crimes, This agreement came out of commitment to Arab and international treaties and covenants related to this matter **(39)** .

The second demand

National Efforts to Combat Cybercrime

National efforts are growing in the Hashemite Kingdom of Jordan and the State of Qatar in seeking to combat cybercrime in order to create a safe cyberspace and protect it from such crimes.

Also, in light of the development of cybersecurity challenges worldwide, protecting ICT systems and infrastructure comes at the top of the priorities of the concerned authorities in Jordan and Qatar. The great benefits that cyberspace offers us are fraught with a number of challenges that may threaten the infrastructure that enhances the ability to safely use the Internet.

In pursuit of these countries to meet these challenges, the Kingdom of Jordan and the State of Qatar continue to make more efforts to enhance cyber security, as well as cooperate with their counterparts around the world to create open and secure cyberspace. For their part, Jordan and Qatar have set a vision for building and maintaining A secure cyberspace to protect national interests and preserve the fundamental rights and values of Qatari society, To achieve this vision, both Jordan and Qatar seek to achieve specific goals of protecting critical information infrastructure, dealing with and recovering from cyber-attacks through information exchange, cooperation and timely action, and establishing a legal and regulatory framework aimed at enhancing security and efficiency cyber space.

The objectives also include promoting a culture of cyber security that is based on the safe and appropriate use of cyberspace, and the development of national cyber security capabilities. In order to make progress in achieving these goals, both Jordan and Qatar have developed and implemented national laws, regulations, and policies necessary to address cyber security and cybercrime issues, and working to increase the capabilities and capabilities that contribute to combating cybercrime, and building and permanently strengthening strong international relations with the aim of setting cyber security standards, In addition to encouraging investment in research fields in order to develop and market innovative electronic security technologies and solutions, permanently monitor the security status of critical information infrastructure, and work to continuously enhance response capabilities to electronic incidents.

To this end, the State of Qatar, represented by the Ministry of Transport and Communications (formerly the Ministry of Communications and Information Technology), established the "Qatar Computer Emergency Response Team", known as "Q-CERT", in 2005 in cooperation with Carnegie Mellon University work in the cyber security sector Through the administrations of "Q-CERT" and "Vital Information Infrastructure Protection" with government agencies, public and private sector bodies, and with Qatari citizens to educate them on how to contain the risks and threats they face on the Internet.

The industry also works to protect vital information on the Internet and ensure its security, and since information security issues transcend the geographical borders of a single country, the cyber security sector is a member of the global Forum of Incident Response and Security Teams” known as, (FIRST), which supports This forum is the international relations linking insurance teams to each other and partners around the world in order to exchange the latest information on threats and risks to vital websites. The sector is also a member of the international Meridian organization concerned with matters of protecting critical infrastructure.

The Qatari government also issued Law No. 14 of 2014 called the Cybercrime Law, to curb cybercrime in an attempt to increase the tools for combating cybercrime.

The law defines electronic crimes through Article 1 of it as: “Any act that involves the use of an information technology means, an information system, or the information network in an illegal manner in violation of the provisions of the law.”

Qatari law also provides for severe penalties of up to 10 years in prison for illegally entering websites and government information systems, or forging and using an electronic editor, and punishes with imprisonment for a term not exceeding three years, and a fine of no more than 500,000 riyals, whoever manages through The information network or any of the information technology means, unjustly, from entering a website or information system for one of the state’s agencies, institutions, bodies, entities or affiliated companies, The penalty is doubled if the entry results in obtaining electronic data or information, or obtaining data or information that affects the internal or external security of the state, its national economy, or any government data that is secret by nature or pursuant to instructions issued to that effect, or cancels or destroys such electronic data and information, or destroy, disseminate, harm beneficiaries or users, or obtain undue money, services or benefits.

In Jordan, efforts have been made and are still being made to combat this type of crime. At the level of internal organizations and institutions, the Public Security Directorate took the initiative in 2008 to form the Attribution and Technical Investigation Department (which is affiliated with the Criminal Investigation Department) to investigate this type of new crime , Through a group of officers who were rehabilitated and prepared for that, and later this section was expanded and supported to become at the level of a unit affiliated with the Criminal Investigation Department, and it was called the “Anti-Cyber Crimes Unit ”, and it was entrusted with the task of receiving all complaints related to Cyber-Crimes.

At the international level, any complaint from any country or any international body outside Jordan is also received and submitted through the Arab and International Police Department (Interpol). After receiving the complaint, the investigation and information-gathering process begins to identify and apprehend the perpetrator **(40)**.

It is indicated here that there is close cooperation and coordination between the Anti-Cyber Crimes Unit and some relevant authorities that provide them with the necessary information to investigate this type of crime at the international and local levels. At the international level, there is coordination, for example, with the management of social networking sites such as Facebook, Twitter and others regarding child sexual abuse via the Internet.

Where these sites provide the Anti-Cyber Crimes Unit with all the technical information it requests, related to any account that is used to commit this crime, such as e-mail, the digital Internet Protocol address (IP Address), and the phone number used for the person exploiting the account holder, and at the level, There is also close cooperation with local telecommunications companies and Internet service providers to provide the unit with all the technical information it needs, which is for the exploiter, such as the IP address, as well as the personal information registered to them, such as his full name and address, which is information that is useful Including determining the identity of the account holder used in the commission of the crime and to determine his location **(41)** .

Jordanian legislation has been developed in line with official efforts to combat this type of crime, as we find that the new Jordanian Cybercrime Law No. 27 of 2015, which sets severe penalties for perpetrators of this type of crime, where Articles (3+ 4-6) of the law stipulates severe penalties in the event of access to the information network or information system by any means or permission.

Likewise, whoever obtains intentionally through the information network or information system related to credit cards, data or information that is used in the implementation of electronic financial or banking transactions shall be punished.

The latest Jordanian efforts in combating cybercrime were in the preparation of the draft cyber security law for the year 2019, and the draft law comes to protect the Kingdom from the threats of cyber security incidents and to Build national cyber security capabilities to confront threats to information systems and infrastructure, raising the level of general and comprehensive national security for institutions and individuals, and developing deterrence, monitoring, warning, and response capabilities to cyber security incidents.

The draft law also aims at creating a safe and attractive environment for investment and stimulating the national economy and finding a reference body that implements public policies that stem from the national strategy for cyber security and works to coordinate national efforts and be a national point of contact with regional and international cyber security centers.

The third demand

Obstacles to international and national cooperation in combating cybercrime

Despite the various services provided by the international information network in various fields such as tourism, cultural, economic, security and military affairs, this was accompanied by many cases of attacks on the privacy of confidential information with the intention of theft, espionage, piracy and sabotage, as these attacks became a concern for all countries of the world Because of the widespread exchange of encrypted information related to political, military or industrial espionage or any criminal activities, this reality imposed the need for international cooperation in combating and stopping these attacks and the need to establish special units to combat information crime **(42)** .

However, these tireless efforts to find effective mechanisms between countries to combat cybercrime faced many difficulties and obstacles that stand in the way of that cooperation, despite the existence of previously mentioned agreements and treaties urging this cooperation, and the most important obstacles it faces can be summarized International cooperation in combating cybercrime as follows:

First: The shortcomings of legal legislation and international treaties on combating cybercrime

The shortcomings and differences of legal systems in the countries of the world have led to the lack of agreement on a specific model and image, which includes the so-called misuse of information systems to be followed, and there is no specific definition of cyber activity that must be an international agreement to criminalize, and the reason for this is due to Legislation shortcomings in all countries of the world and not keeping pace with the speed of scientific and technological progress **(43)** .

Therefore, we find that the different legal systems' lack of agreement on a unified picture of criminal behavior in information crime tempts computer hackers to organize themselves and commit their crimes without being bound by geographical borders, which confirms the inevitability of international cooperation to combat this crime, and the many attempts made by Before the United Nations, as well as some European and Arab countries, in combating these crimes by signing relevant agreements, it was not enough, These agreements are still tainted by deficiencies, as the lack of bilateral or collective treaties between states has limited fruitful international cooperation in combating this type of crime and the inability to establish international responsibility for these crimes.

Even if they exist, these treaties remain insufficient to achieve the required protection in light of the rapid progress of computer systems and programs and the Internet, and the development of cybercrime at the same speed has led to confusion among the legislature and state security authorities **(44)** .

It is also noted that most of the criminal legislation currently applied in most countries of the world is based on the regional character with regard to the application of the rules of the criminal procedure through non-national authorities, so it is inevitable to conclude bilateral and collective agreements between countries to facilitate the investigation of cyber crimes because, Despite the conclusion of some agreements, they did not fulfill the purpose of solving the problems of jurisdiction, the exchange of criminal evidence and the extradition of criminals , Therefore, there remains an urgent need for more flexible criminal legislation and international treaties to keep pace with the speed of technological progress and the information age **(45)** .

Second: Weak international coordination regarding criminal procedures to combat cybercrime

The lack of coordination with regard to the criminal procedures followed in relation to cybercrime between different countries, especially with regard to investigation and obtaining evidence, hinders the spread of cyber crimes, and that obtaining evidence in such crimes is outside the borders of the state through seizure or inspection in a particular information system is very difficult besides it is difficult to get the evidence itself **(46)** .

There is also the problem of jurisdiction in cyber crimes, because it is one of the problems that hinder obtaining evidence in it, especially since it is one of the most crimes that raise the issue of jurisdiction at the local and international levels due to the overlap and interdependence between information networks, because cyber crime may occur in a specific place. And its effects are produced elsewhere **(47)**.

The lack of international coordination with regard to criminal procedures and forms of jurisdiction in cyber crimes is one of the most important obstacles in the field of international cooperation to combat these crimes, because the investigation in the information technology environment, according to European Council Recommendation No. (95/13) requires rapid intervention to extend Procedures to computer systems that may be located outside the country, So that this matter does not represent an attack on the sovereignty of a particular country or on the provisions of international law, an explicit legal rule must be established that allows this procedure. Therefore, there is an urgent need for the existence of international agreements regulating how to take these measures, and there must be quick and appropriate procedures and communication systems that allow the investigative bodies may contact foreign bodies to collect certain evidence, which requires the development of international cooperation agreements **(48)** .

Third: Difficulties related to international legal aid

We know that the origin of requests for international letters rogatory, which is one of the most important forms of international judicial assistance in the criminal field, is that it is delivered through diplomatic means, and this of course makes it characterized by slow and complexity, which contradicts the nature of the Internet and its speed, which is reflected in the crimes related to the Internet.

One of the great difficulties in the field of mutual international judicial assistance is the delay in responding, as the country receiving the request is often slow in responding to the request, whether it is due to a lack of trained personnel or as a result of language difficulties or differences in procedures that complicate the response and other reasons, Therefore, there is an urgent need to find a fast way or method through which delegation requests are delivered, such as appointing a central authority, for example, or allowing direct communication between the competent authorities in considering such requests in order to eliminate the problem of slowness and complexity in the delivery of rogatory requests.

This is indeed what was recommended by the Eleventh United Nations Congress on Crime Prevention and Criminal Justice, which was held in Bangkok during the period (18-25/4/2005 AD), where it stressed the need to enhance the effectiveness of the relevant central authorities involved in the work of mutual legal assistance. Establish direct channels of communication with each other in order to ensure timely implementation of requests **(49)**.

We also find this in the second item of Article (27) of the European Agreement on Information Crime, And Article (35) of the same European Agreement, which requires the states party to it to specify a POC that operates for (24) hours a day, seven days a week in order to provide direct assistance to investigations related to data and network crimes or to receive evidence in electronic form about crimes, The same article also required the parties to the need for the contact point to be able to quickly connect to the other party's contact point, and for each party to have trained personnel capable of facilitating the work of the network.

Conclusion, results and recommendations

In the conclusion of this research, the researcher has clarified an international phenomenon that has become present in the international community and is working to confront its negative effects, which are cyber crimes, by explaining its concept, development, types and sources.

In some detail, this research clarified the extent of international and national efforts in the field of combating cybercrime, by addressing the aspects of international cooperation in the field of combating cybercrime and the obstacles that prevent the achievement of such cooperation, and through the foregoing, the researcher reached a set of results and recommendations We will mention them as follows:

1. The term cyber-attacks is a newly emerging term in recent decades as a result of the information technology revolution. Therefore, definitions have varied in the light of jurisprudence and international practical practices.
2. Cyber crimes are of great danger and have a significant impact on aggravating corruption, undermining the rule of law, and being a source of threat to the security of societies and countries.
3. Most countries lack cyber legislation, and if there are laws, there will be major legal loopholes in this field.
4. Placing cyber attacks within the existing international legal framework is very difficult because of their special nature, in addition to the absence of an official and final legal statement agreed on this phenomenon.
5. There is a cyber and electronic arms race between countries due to the increasing desire of countries to strengthen their defenses against the threat of cyber attacks.
6. There are international and regional efforts, knowing that these efforts are not sufficient to combat this phenomenon through international conferences and conventions to prevent cybercrime and treat cybercriminals.
7. There are difficulties and obstacles that stand in the way of international endeavors and efforts to find effective mechanisms between states to combat cybercrime.
8. Cyber crimes are global crimes that cross borders, so combating them can only be achieved through international cooperation at the criminal procedural level.

Second: Recommendations

1. Work to achieve cyber security and preserve the rights resulting from the legitimate use of computers and information networks
2. Filling the legislative vacuum in the field of combating cybercrime, and the necessity of enacting legislation that covers this vacuum in order to reach safe cyberspace.
3. Develop the national criminal legislative structure in line with international efforts in combating cybercrime.

4. Activating international cooperation, the role of international treaties and agreements, and the principle of mutual legal, judicial, and security assistance in the fight against cybercrime.
5. The researcher recommends establishing partnerships between the public and private sectors at the national, regional and international levels to combat cybercrime, exchange experiences and improve ways to combat it as transnational crimes.
6. The necessity of establishing an international court for cyber crimes that are carried out from outside the borders of the state, as it is not possible to inflict punishment on the perpetrator of cybercrime in another country, except with the cooperation of the state agencies in whose territory the attack was carried out.

Margin:-

(1) **Al-Badayna, Diab Musa (2014) Cybercrime: Concept and Causes, Amman, a working paper presented to the scientific forum "New crimes in light of regional and international changes and transformations during the period 2-4/9/2014 AD",** p. 5 .
(2) **Walid, Khaled (2013), Cyber attacks: the new arena of electronic conflict**, p. 3. ?
(3) **(Al-Fatlawi, Ahmed Obais Nehme (2016 AD), Cyber Attacks: Their Concept and the Emerging International Responsibility in the Light of Contemporary International Organization, Al-Mohaqiq Al-Hilli Magazine**, p. 6.
(4) **John Bassett and others (2014 AD), Future wars in the twenty-first century**, p. 53.
(5) **Al-Fatlawi, Ahmed Obais Nehme (2016 AD), Cyber Attacks: Their Concept and Emerging International Responsibility in the Light of Contemporary International Organization, Al-Mohaqiq Al-Hilli Magazine**, p. 3.
(6) **John Bassett and others (2014 AD), Future wars in the twenty-first century**, p. 54.
(7) **Al-Hamdani, Bushra Hussein (2014 AD), Electronic piracy:** weapons of modern war, p. 5.
(8) **Kakhya, Ibrahim (2010 AD), Electronic Warfare**, p. 41.
(9) **The Consultative Center for Studies and Documentation (2014 AD), "Transformations in the American Military Doctrine: The Seven Pillars of Weakness", strategic papers**, p. 17.
(10) **Atlam, Sharif, and Muhammad Maher Abd al-Wahed (2007 AD), "Encyclopedia of International Humanitarian Law Conventions, Official Texts of Conventions and Ratifying Countries**", p. 4.
(11) **Mohareb, Mahmoud (2011 AD), reading in a book: War in Cyberspace: Trends and Effects on Israel**, pg. 7.
(12) **Shafiq, Nouran (2016 AD), The Impact of Cyber Threats on International Relations:** A Study in the Dimensions of Cyber Security, p. 30.
(13) **Abu Bakr, Muhammad Abdullah (2006 AD), Computer and Internet Crimes**, p. 103.
(14) **Clay Wilson, Cyber Crime. In Franklin D. Kramer et al (eds), Cyber Power and National Security**, Potomac Book,(2009).
(15) **Abu Bakr, Muhammad Abdullah (2006 AD), Computer and Internet Crimes**, p. 103.
(16) **Shafiq, Nouran (2016 AD), The Impact of Cyber Threats on International Relations: A Study in the Dimensions of Cyber Security**, p. 30.
(17) **Abu Bakr, Muhammad Abdullah (2006 AD), Computer and Internet Crimes**, p. 104.
(18) **Kenneth Greers,(2011) Straedic Cyber Security**, p 26.
(19) Giancarlo A. Barletta (2011) Cyber Conflict and Geo-Cyber Stability, p. 50.
(20) **Shafiq, Nouran (2016 AD), The Impact of Cyber Threats on International Relations:** A Study in the Dimensions of Cyber Security, pg. 40.
(21) **Mahmoud, Khaled Walid (2013), Cyber attacks**: the new arena of electronic conflict, p. 7.
(22) **Richard A. Clark & Robert K. Knake (2010), Cyber War:** The Next Threat to National Security and What to Do About It. P147.
(23) **Shafiq, Noran (2013 AD), The Use of Electronic Power in International Interactions**, available online at http://www.siyassa.org.eg.
(24) **Shafiq, Nouran (2016 AD), The Impact of Cyber Threats on International Relations:** A Study in the Dimensions of Cyber Security, pp. 42-43.

(25) **Paul Cornish (2014) Cyberspace and the National Security of the United Kingdom:** Threats and Responses, P 7-11.
(26) **Shafiq, Nouran (2015 AD), The Impact of Cyber Threats on International Relations:** A Study in the Dimensions of Cyber Security, p. 45.
(27) **Mahmoud, Khaled Walid (2013 AD), Cyber Attacks**: The New Electronic Conflict Arena, p. 9.
(28) **Shafiq, Nouran (2015 AD), The Impact of Cyber Threats on International Relations:** A Study in the Dimensions of Cyber Security, pg. 46.
(29) **Shafiq, Nouran (2015 AD), The Impact of Cyber Threats on International Relations: A Study in the Dimensions of Cyber Security**, p. 47.
(30) **Malati, Hisham, (2014 AD) The specificity of procedural rules for information crimes - an attempt to approach the compatibility of national law with international standards**, p. 101.
(31) **Ababneh, Mahmoud, and Al-Raziqi (2005 AD), Muhammad Muammar, Computer Crimes and its International Dimensions**, p. 31.
(32) **Hegazy, Abdel Fattah Bayoumi (2007 AD), Criminal Evidence in Computer and Internet Crimes**, p. 15.
(33) **Al-Muwasher, Turki Abdul-Rahman (2009), Building a security model for combating information crimes and measuring its effectiveness,** PhD thesis in security sciences, p. 48.
(34) **Ababneh, Mahmoud, and Al-Raziqi (2005 AD), Muhammad Muammar, Computer Crimes and Its International Dimensions**, p. 38
(35) **Al-Radaydah, Abdul Karim (2010 AD), New Crimes and the Strategy for Confronting them**, p. 236.
(36) **Ghannam, Sherif Muhammad (2007 AD), Protection of trademarks over the Internet in relation to the electronic address**, p. 149.
(37) **Sharabsha, Linda (2012 AD), International and Regional Policy in Combating Cybercrime**, p. 12.
(38) **Sukar, Abdul Samad (2010 AD), International Security Cooperation in Combating Contemporary Crimes**, p. 45
(39) **The Arab Convention to Combat Information Technology Crimes, (2010) Preamble, General Secretariat of the League of Arab States**, Legal Affairs Department.
(40) **Al-Radaydah, Abdul Karim (2010 AD),** New Crimes and the Strategy for Confronting them,
(41) **Al-Radaydah, Abdul Karim (2010 AD), New Crimes and the Strategy for Confronting them**, p. 26.
(42) **Sukar, Abdul Samad (2010 AD), International Security Cooperation in Combating Contemporary Crimes**, p. 55
(43) **Sharabsha, Linda (2012), International and Regional Policy in the Field of Combating Cybercrime**, p. 15.
(44) **Al-Badayna, Diab (2003 AD), Security and Information Warfare**, p. 45.
(45) **Saleh, Mahmoud, (2006 AD) Information Crimes**, p. 4.
(46) **Al-Bishri, Muhammad Al-Amin (2004 AD), Investigation of New Crimes**, p. 124
(47) **Al-Badayna, Diab (2003 AD), Security and Information Warfare**, p. 78
(48) **Saleh, Mahmoud, (2006 AD) Information Crimes**, p. 6.
(49) **Saleh, Mahmoud, (2006 AD) Information Crimes**, p. 78.

Reference list:

[1] Abu Bakr, Muhammad Abdullah (2006 AD), Computer and Internet Crimes, Knowledge Foundation, Alexandria

[2] Al-Badayna, Diab (2003 AD), Security and Information Warfare, Jordan: Dar Al-Shorouk for Publishing and Distribution

[3] Giancarlo A. Barletta (2011) Cyber Conflict and Geo-Cyber Stability, International Telecommunication Union, Cairo.

[4] John Bassett and others (2014 AD), Future wars in the twenty-first century, Emirates Center for Strategic Studies and Research, Abu Dhabi.

[5] *Hegazy, Abdel Fattah Bayoumi (2007 AD), Criminal Evidence in Computer and Internet Crimes, Alexandria, House of Legal Books.*

[6] *Al-Hamdani, Bushra Hussein (2014 AD), Electronic Piracy: Weapons of Modern War, Amman, Dar Osama for Publishing and Distribution.*

[7] *Al-Radaydah, Abdul Karim (2010 AD), emerging crimes and the strategy to confront them, Amman, Al-Hamid House and Library for Publishing and Distribution.*

[8] *Suker, Abdel Samad (2010 AD), International Security Cooperation in Combating Contemporary Crimes, Cairo, Police College Press*

[9] *Sharabsha, Linda (2012), International and Regional Politics in the Field of Combating Cybercrime, Rabat, University Center.*

[10] *Shafiq, Nouran (2015 AD), The Impact of Electronic Threats on International Relations: A Study in the Dimensions of cyber Security, Cairo, Arab Knowledge Office.*

[11] *Ababneh, Mahmoud, and Al-Raziqi (2005 AD), Muhammad Muammar, Computer Crimes and its International Dimensions, Amman, House of Culture for Distribution and Publishing.*

[12] *Atlam, Sherif, and Mohamed Maher Abdel Wahed (2007 AD), "Encyclopedia of International Humanitarian Law Agreements, Official Texts of Conventions and Countries Ratifying Them", issued by the International Committee of the Red Cross in Cairo.*

Second: University theses

[13] *Al-Muwasher, Turki Abdul Rahman (2009), Building a security model to combat information crimes and measure its effectiveness, PhD thesis in security sciences, Riyadh: Naif Arab University for Security Sciences.*

Third: magazines, newspapers and research

[14] *Al-Bishri, Muhammad Al-Amin (2004 AD), Investigation of Newer Crimes, Riyadh, Prince Nayef University for Security Sciences, Studies and Research Center Series, No. (339).*

[15] *Shafiq, Noran (2013 AD), The Use of Electronic Power in International Interactions, available online at http://www.siyassa.org.eg.*

[16] *Al-Fatlawi, Ahmed Obeis Nehme (2016 AD), Cyber attacks: their concept and the international responsibility arising from them in the light of contemporary international organization, Al-Mohaqiq Al-Hilli Journal, Babylon University.*

[17] *Kakhia, Ibrahim (2010 AD), Electronic Warfare, The Arab Defense Magazine, Beirut*

[18] *Muharib, Mahmoud (2011), reading in a book: War in Cyberspace: Trends and Effects on Israel, The Arab Center for Research and Policy Studies, Doha.*

[19] *Mahmoud, Khaled Walid (2013), Cyber Attacks: The New Cyber Conflict Arena, Doha, Arab Center for Research and Policy Studies.*

[20] *The Consultative Center for Studies and Documentation (2014 AD), "Transformations in the American Military Doctrine: The Seven Pillars of Weakness", Strategic Papers, Irregular Series on Strategic Affairs, Issue: 2, September (2014), Beirut.*

[21] *Walid, Khaled (2013), Cyber attacks: the new arena of electronic conflict, Abu Dhabi, the Arab Center for Policy Research and Studies.*

Fifth: Proceedings of conferences and seminars

[22] *Al-Badayna, Diab Mousa, Cybercrime: Concept and Causes, Amman, a working paper presented to the scientific forum "Created crimes in light of regional and international changes and transformations during the period 2-4/9/2014 AD", Amman, Jordan, (2014 AD). .*

[23] *Saleh, Mahmoud, (2006 AD) Information Crimes, Muscat: A working paper presented to the regional workshop on developing legislation in the field of combating virtual crimes, Sultanate of Oman April 2-4.*

[24] *Malati, Hisham, The specificity of the procedural rules for information crimes - an attempt to approach the compatibility of national law with international standards, Rabat Court of Appeals Seminar Series, Issue Seven, (2014).*

Agreements

[25] *The Arab agreement to Combat Information Technology Crimes, (2010 AD), Preamble, General Secretariat of the League of Arab States, Legal Affairs Department.*

[26] *Foreign references:*

[27] Clay Wilson (2009), "Cyber Crime," in Cyberpower and Cyber deterrence, ed. Franklin D. Kramer et al.Dulles, VA: Potomac Books.

[28] Kenneth Greers)2011) (Strategic Cyber Security, NATO Cooperative Cyber Defence Center of Excellence,(2011).

[29] Paul Cornish, (2014) Cyberspace and the National Security of the United Kingdom: Threats and Responses.

[30] Richard A. Clark & Robert K. Knake(2010), Cyber War: The Next Threat to National Security and What to Do About It. Harper Collins Publisher.