The Seybold REPORT

ISSN 1533-9211

CYBER FORCE, CYBER CRIME, CYBER TERRORISM IN (CYBERSPACE)

Dr. HAZIM JERRI MNEKHIR

Ministry of Higher Education and Scientific Research (Department of Scholarships and Cultural Relations).
Email: hazim.jerri@scrdiraq.gov.iq

Abstract

Today, the world is witnessing a massive shift towards digital technology, as dependence on the Internet and smart devices is growing rapidly. With this radical transformation, cyberspace comes as a vital field that connects societies and individuals around the world. Cyberspace is a complex and dynamic environment that offers enormous opportunities for interaction and exchange, but at the same time presents great challenges. In this context, the concept of cyber power plays a vital role in defining interactions and relationships in cyberspace. Cyber power can be defined as the ability to use cyber technology effectively and intelligently to enhance national capacity and achieve strategic interests. The development of cyber power gives states and institutions a greater ability to protect their interests and benefits in cyberspace, including protection from cyber threats, cybercrimes, and cyber terrorism. However, we must recognize that increasing the cyber power of states and institutions comes with its own challenges. Rapid technological advancement means that security vulnerabilities and threats are constantly surfacing.

Keywords: Cyber Force, Cybercrime, Cyber terrorism, Cyberspace.

SUMMARY

In this paper, we will explore cyber power, cybercrime, and cyber terrorism in cyberspace. We will discuss cyber power as a powerful tool for states and institutions to enhance their ability to protect their interests and achieve their goals in the digital world. However, we will also focus on cybercrime and how criminals can exploit vulnerabilities in cyberspace to carry out their evil actions and attack institutions and individuals. We will also address cyber terrorism and how extremists use cyber tools to terrorize and influence people and countries.

The first axis: definition of power and its types:

First: The Definition of Power

1- The nature of power: Machiavelli believes that power: is "the means and the final end that the state seeks to reach in the field of international relations." (1)

Morkenth or knows it: "It is human control over the minds and actions of others" (2).

And Ernes Haas defined it: “It is a function of several factors, some of which are tangible, such as primary resources and industrial production, and some are intangible, such as technology and ethics.

Stephen Rosen defines it as: "The ability of an international player to use tangible and intangible resources and assets by influencing the outcomes of events in the international system in the direction of improving his convictions in the system" (3).

Through the foregoing, power can be defined: It is (a group of material and moral factors that a person, institution, or country possesses, and its ability to influence the behavior of others, using certain means).

2- The comprehensive power of the state is: the sum total of the power of the state = its natural resources + its economic capabilities + its cultural structure + its political and administrative system + its military effectiveness + its international relations (4).

Thus, power is linked to the end, as nations do not live for the sake of power, but their struggles over power were for the sake of ends rooted in values and interests, and that power is linked to means; because it is the method by which the goals are achieved (5).

Defining force: Force is defined as the ability of an international actor to act and change the behavior of another international actor, and that depends on coercion and coercion to change his behavior, and this is in the interest of the party that exercised force, and this trend has grown the owners of the realistic school, which depends on international conflicts hard power; between international actors.

Force: It is the ability to obtain final outputs. Military force, for example, cannot be considered a force in the event that it does not achieve the required results in achieving the objectives of the state. Joseph says: Power means owning the resources, and stopping at that is incorrect, those sources must be able to reach the required outputs; To become a real and effective force on the ground, and Joseph gave an example of that, although the United States of America has the greatest power and the most resources, because it was unable to achieve the required outputs; Therefore, Joseph considers it necessary to differentiate between power as a source and power as a behavior that has outputs. Talking about the Chinese rise is a natural result of China's possession of economic resources, a large population and other resources, but it cannot be viewed as a real power unless China is able to convert its resources into power. Actual (6).

3- The national strength of the state

There is no fundamental or significant disagreement in defining power or defining what is meant by it. Most definitions state that power is the ability to influence the behavior of others or control their behavior towards a specific issue. Given this definition, its scope has been limited to the process of influence. Those interested in international relations and its affairs, they provided clearer definitions in view of the connection of force with the relations of states, which is the basis for the applications of force and its practical effects, and in a symbolic way / that force is the ability (A) to push (B) to do (X) or not to do (Y) in the sense that it allows (Any relationship) with a government forcing the government of a country to follow a certain behavior that it did not choose of its own free will, such as making it take actions that it does not want to do, or preventing it from doing actions that it wants to do.

Second- Types of Power:

1- Hard Power: HARD POWER

Hard power consists of physical military power and economic power, and distinguishes talking about this form of power in the thought of the realistic school, while Joseph does not see that the concept of hard power is limited to military power only, but rather he sees the ability to use carrots through economic tools that can be It affects the behavior of others, so we can distinguish between two components of hard power, the first: represented in military force, which is the traditional force used mostly, and the second: represented in the diplomacy of coercion, which expresses the use of simple force, while military force is considered more use of force (7).

2- Soft Power SOFT POWER:

After the end of the Cold War, the concept of soft power witnessed an ascent, despite the existence of the term before the Cold War, which means the use of tools of enticement and persuasion and leaving pressure and coercion in managing international relations. Rather, soft power is used such as tools of popular diplomacy, and the employment of cultural factors such as economic aid and grants. studies, in the management of foreign state relations, and thinking began early in the seventies, with the participation of Joseph Nye and Robert Cohen, in their published book "Strength and Mutual Dependence". During which the employment of multiple and diverse tools of force, to achieve certain goals,

the writer Cohen presented ideas later, in "Political Economy", but Joseph Nye was interested in media, education in general, and how to build a cultural model for the state; To influence others, and push them to adopt policies that serve their interests (8).

Joseph Nye defined power in general: as the ability to influence the desired goals, and to try to change the behavior of others for a specific action, and he defined soft power: it is the ability to persuade and not coerce what you want to obtain, and he does not believe in economic, political and military sanctions, and he believes that the essence of power Soft lies in the ability of a particular nation to influence other nations, and this is through the attractiveness of its social, political and cultural system, and through the value system and institutions that it carries that work on enticement and do not work on coercion and threat. This attraction can be spread through: private and public diplomacy, culture popular, international organizations, institutions and commercial companies (9).

Joseph tried by talking about addressing the narrow analysis of power, which was adopted by the “realistic school.” The concept of power in the realistic school focused on military power. The second mode: is persuasion, and is used to influence the beliefs and reactions of others, without the threat of force. The third mode: setting the agenda or what is called Agenda Setting, i.e. defining the priorities of the state and matching them with the priorities of other countries.

3- Cyber Power:

The most important person who talked about cyber power, as a new form of power, was Joseph Nye, and linked this power to possessing technological knowledge and the ability to use it well, meaning that he can obtain the outputs of this power, through the interconnection of electronic information in cyberspace, which also means the use of Cyberspace, to create a cyber-force that influences events, through electronic environments, through power tools and its various forms, whether military, economic, diplomatic or informational.

With 'networks', the relative structural positions of capital and labor are preserved, albeit in grid form. Structural strength appears in these networks as much as it was during the industrial age.

4- productive cyber power:

Cyberspace, as an ideal informational environment, is ideally suited to the performance and transmission of productive electronic power. This is the constitution of social subjects through the discourse mediated by cyberspace, which thus defines the “fields of possibility” that constrain and facilitate social action (10).

Cyberspace reproduces and enhances existing discourses, as well as constructs and disseminates new ones. In many ways, productive computing power is the basis for other forms of cyber power. Without built social objects, there are no social relationships through which power can be projected. Produced cyber power also connects the military and political realms of war and aims to stir the discourse in favor of the strategic actor. This is particularly evident in the use of "soft" power to win hearts and minds, either during conflict, or before. "Upper" is the principal space in which political struggles are evident. In the age of "strategic communication" and "public diplomacy," productive cyber power is perhaps the most important form of cyber power. One of the most obvious examples of how states demonstrate productive cyber power is the heuristic construction of threat actors in cyberspace. By identifying certain actors as a threat to national security, states can pursue policies and strategies aimed at treating them as legitimate targets of other forms of state power. The term "hacker" For example, hackers have changed dramatically since their roots in the 1950s and 1960s. Now, hackers are more likely to be portrayed as "antisocial, potentially dangerous individuals," wreaking havoc on computer systems, rather than responsible "heroes" as the enemy. The new information age is largely about the innovations driving the Internet and the World Wide Web, in fact, in many cases, they are seen as "the new enemy of the information age... bad actors in the new social reality of cyberspace, although some hackers are hostile and destructive to society, yet many of them simply go against the designs and ethics of the state system and are criminalized. In the late 2010s, a lot of Julian Assange's personal background and WikiLeaks persona was made as a hacker. An article published in an international journal describes Assange's past as "crusader, hacker, petty madness, blackmail and little skepticism about his perceived moral status". In many countries hackers have been described as "naughty little boys" and the moral divide has been catered for. More emphatically on the terms "black hat" and "white hat" respectively, "moral" and "immoral" and some scholars put forward a new way to deal with them. So cyberspace is a powerful means of productive power that is expressed through the protection of the national security of the state (11). ime), into Arabic (the Convention on Electronic Crime).

- American Military Terms Dictionary: The American Dictionary of Terms mentioned the term (cyber), but it did not define it as it is in its original sources, but rather defined it in its actual scope, i.e. military, as a verb used in electronic networks and their tools with the aim of controlling or disabling other electronic programs (12).

- The dictionary of information security terms has defined: The term cyber is an attack through cyberspace, aimed at destroying and disabling websites and infrastructure and harming or controlling them ().

A. Cyber: It is a prefix used to describe a person, thing, or idea as part of the computer and information age. Derived from kybernetes, Greek for "steersman" or "ruler", it was first used in cybernetics which is the science or study of control or regulation mechanisms in human and automated systems, including computers. , a word coined by Norbert Wiener and colleagues. Common uses include internet culture, cyberpunk, and cyberspace.

B. Cyber: It is a field characterized by the use of electromagnetic electronics to store, modify and exchange data through networked systems and infrastructure.

C. Derived from “cybernetic”, which comes from the Greek word υβερνητικός meaning skill in leadership or judgment. It is mainly used in terms of cyberspace, cyberbullying, cybercrime, cyberwarfare, cyberterrorism, among others. Although it is most commonly used to describe policies and policies related to computer systems and networks as in the above cases, it is also widely used in many IT industries. Cyber is now a modern term in the internet age.

D. We can say that cyberspace, as previously mentioned, is control or remote control. When it comes with another word, it means control or management, as in cybersecurity, and it means control of cybersecurity or cybercrime, and it means how to control and control cybercrime. As for cyberspace, which means controlling everything that works electronically or within the scope of the Internet, whether it is military, economic or social, the steering wheel is control in this modern field.

So we can say that the definition of cyber: it is the ability to remotely control, control and protect the electronic system in terms of security, economic, social and military.

2- The concept of cyber:

The origin of the word “cybernetic” goes back to the Greek language, especially to the word “Kbernetike”, and this word carries a meaning that combines what is meant by “steering” and what is meant by “governance”. Both guidance and governance have a broad framework of influence. Guidance is usually within a broad framework that includes different dimensions and options. Governance is also related to regulations and procedures that can be applied in many areas.

The description of cyber is nowadays associated with computer networks and the Internet; And when cyberspace is said, the intended meaning is: everything related to computer networks and the Internet, the applications they implement, and the services they provide, in various fields of life, at the level of the entire world. It is noted that this meaning is characterized by a wide scope, multiple systems, different applications, and services that reach everyone. On this basis, cyber security is to provide the necessary protection for cyberspace.

Cybersecurity may stem from the trend towards protecting cyberspace, which includes the contents of this space on the one hand, and includes various other moral factors on the other hand. These contents may include information related to the various parties, institutions and individuals, within the cyberspace; It also includes technology that stores, processes and transmits this information over networks; It also includes business procedures that carry out tasks that perform various services; Here, too, are the individuals responsible for all of this. Moral factors include the reputation of the parties to cyberspace, especially the various institutions and countries (13).

The protection of balances is linked to conditions and performance indicators, the most famous of which are three elements: protection of work and availability of services without interruption “Availability”; protect the integrity of information from any sabotage, distortion or modification; Protecting the user's privacy "Confidentiality", whether it is an individual, an institution or a country. Then there is also the protection of assets from emergency natural disasters, or intended sabotage disasters, and perhaps one of the most important means of protection in this field is the existence of computer centers and duplicate means of communication that act as an alternative when needed, within the framework of cyberspace (14).

The protection required for cyberspace assets may come as a result of risks threatening these assets and challenging their availability, integrity and privacy of information. These risks may come as a result of unintended accidents, such as technical faults, power outages, improper practices, negligence, unexpected environmental events, and so on. Risks may be generated by malicious, hostile sources that seek to disable devices in various ways, such as infecting them with computer viruses and other malicious programs, tampering with information, revealing confidentiality, distorting or deleting them, or performing other malicious actions targeting various assets. Such intrusions may be indirect, as they come programmed according to a schedule, or remain stored waiting for

activation signals, leading to their launch towards the hidden actions designed for them. Given the extent of cyberspace extending to the entire world, the sources of risks enjoy the same extension, because every unit or element connected to this space can be a source of risks. Accordingly, protecting the cyber security of an institution, institutions, or a country within cyberspace requires studying the risks throughout this space, identifying their sources, requirements, and the possibilities of their occurrence, in addition to determining the extent of their impact on the various balances, especially the main important balances (15).

Here we come to the requirements of risk protection, usually through “Controls” that can lead to their disposal or reduce their impact on the balances. Such controls include: technical systems that protect them from viruses and malware; And administrative means that define sound practices and limit negligence, in addition to physical guarding to protect important computer centers, and specialized international organizations have been keen to set standards for defining such controls, and recommend governmental and non-governmental institutions to abide by them and put them into practice.

These organizations include the International Telecommunications Union "ITU", the International Standards Organization, "ISO", the British Standards Institute, "BSI" and the American National Institute of Standards and Technology "NIST". “All institutions and individuals alike need protection from cyber risks, but these risks differ in their extent of occurrence and level of severity, between individuals and institutions, in addition to the difference in the level of protection required, between one individual and another, and one institution and another, depending on its work, and the risks that You can be exposed to it, and just as there are costs that can be caused by risks when they occur, there are also costs to protect against risks when implementing them, if a balance is required between them, and this balance depends on the needs of the individual and the institution concerned, and we often find that large institutions that deal commercially or administratively With other institutions, it requires the latter to use specific controls, so that transactions between them, through cyberspace, enjoy the desired protection (16).

In the twenty-first century, cyberspace is a large part of the lives of individuals and official and unofficial institutions around the world. Therefore, all these parties, whether they are individuals, governments, or organizations, can bring risks to any of them and from any other party, in this cyberspace, so there must be controls that lead to protecting users from risks, and there are important proposals from countries in this regard; Therefore, it must be taken into account, according to the needs of each individual and each institution (17).

3- Cyberspace

Cyberspace is much more than an environment for the Internet, or a large-scale operating environment And comprehensive, rather, cyberspace is a field that has become influential in all the details of our lives as human beings, and influential in countries, and even in the global security system, and its influence has extended in all economic, military, political and infrastructure fields of countries, and has become a field of control, competition, conflict and war, and even a field of deterrence, and in In all areas, and the balance of power has changed, so the influential countries in the global system no longer possess only a nuclear or military arsenal, but rather a small country that does not have a large military force can influence major countries and threaten their security, by having power in cyberspace, but rather It is possible for an individual to affect and harm the national security of major countries, and for more clarification, we have given the following definitions: Cyberspace: It is "an operational field framed by the use of electronics, information is exploited through interconnected systems and related infrastructure, power depends on the context, and cyber power depends on the resources that characterize the field of cyberspace" (18).

□ Cyberspace: Cyberspace is a complex and dynamic environment, interconnected with the electromagnetic spectrum (□), and key to all military operations on land, sea, air and space.

□ Cyberspace: It is a field characterized by the use of electronics and the electromagnetic spectrum to store, modify and exchange data through networked systems and associated physical infrastructures.

Indeed, cyberspace can be thought of as the interconnectedness of humans through computers and communications, without regard to physical geography. William Gibson sometimes refers to the invention or popularization of the term through its use in his 1984 novel, Neuromancer.

□ Cyberpunk: It is a kind of science fiction, and it focuses on the philosophical world, for the science of advanced technology, and this name is derived from the science of cybernetics, and it was originally invented as a title for a short story by

(Bruce Bethick) and the title of the story was (Cyberbank), which was published in 1983, he presented advanced science, such as cybernetics and information technology, which was associated with a degree of collapse and radical change in the social system.

□ Is a genre of science fiction famous for its focus on the world of high technology and the underworld, the name is derived from cybernetics and evil and was originally invented by Bruce Bethick as the title of his short story Cyberpunk published in 1983 in which he presented advanced science, such as information technology and cybernetics Mechanism, associated with a degree of collapse and radical change in the social order, is the feeling or belief that some outsiders, armed with their individual personality and technological ability, can repel the tendencies of traditional institutions to use technology to control society. and that the term, which combines "cyber" and punk, may have originated in the 1980's with Bruce Bethke's short story, "Cyberpunk". Gardner Duzois, editor of Isaac Asimov's Science Fiction Magazine, is credited with associating the word with a literary movement that includes the science fiction of William Gibson and Neil Stephenson.

It is also a sub-genre of sci-fi which features advanced science and technology in the future. On the one side, you have powerful big corporations and private security forces, and on the other side you have the dark underworld of illegal trade, gangs, drugs, and vice versa, among all this politics, corruption and social unrest. (19).

4- The concept of cyberspace:

We know that we live inside this cyberspace, but we all do not have enough information about it, and this space has become an integral part of our daily lives until our identity has become our language and the way we communicate with others, but in fact we do not know much about this space and what goes on in this The cyber environment, there is a massive electronic interdependence that requires interpretation and planning for the future. We are living today in a unique phase of human history that we can call this phase “the Internet of things”, as it is a phase in which personal life devices are connected electronically, communicate with each other, and make decisions according to the indicators that it sees. That this stage is in which our personal information is distributed and stored in many databases and many devices, and then all these things have now become matters recognized by society and have become an essential factor for business, our daily life and the provision of services, and the impact of cyberspace can now be seen in every A place, and reliance on it even in the military fields, where communications, command and control, intelligence and precise offensive elements all depend on many, "cyber systems" and related communications systems, that artificial intelligence is now controlling our lives positively without doubt, but it is not without Of the risks, this electronic interdependence must have special security, as we have begun to lose control little by little, and put the leadership in the hands of those devices, which carry all our important and sensitive information. There is no doubt that these devices still provide us with a comfortable and luxurious lifestyle, but that does not mean that We ignore information security, because it has become possible to access all our information in ways that do not occur to us, and this great interdependence has led to the possibility of penetration of these systems and governments, and these penetrations are difficult to predict, prevent, manage or mitigate without having electronic power, and some countries see these dependencies times for its national security or national defense, most countries established councils or bodies for national cyber security, so cyber security has become an important comprehensive issue that requires responses from individuals, private companies, non-governmental and governmental organizations, as well as international agencies and bodies, to expose citizens to theft, children are in danger, Companies are in danger and countries are threatened, and cybercriminals are spreading their influence at the same speed as this development, in the Internet.

That cybercriminals do not see them and do not know them, we unintentionally trust them no one is immune, and thus give them their power (20).

Whether by manipulating public opinion, espionage, identity theft, terrorism, harassment, scams, financial fraud and various types of crimes, cybercrime touches them all. Internet crime has become a reality of contemporary life at the level of people, organizations and countries. Over the course of a few years, it has grown into a real plague on society (21).

So types of crimes emerged, for example, old crimes committed with new technologies, spam, computer viruses, electronic attacks, identity theft and an increase in frequency day after day. Information and communication technologies allow huge amounts of information to be stored, processed, accessed, searched, transferred, exchanged and published, regardless of Geography distance. This is amazing (22).

The third axis: cybercrime and cyber terrorism

First - Cybercrime:

1- Definition of cybercrime

A. The German jurist Tadiman defined it as: “All forms of illegal or harmful behavior to society that are committed using computers” (23).

B. The French Jurist Masse defined cybercrime as: "Illegal attacks that are committed by informatics for the purpose of making a profit" (24).

C. C - The Two French jurists defined stans and vivat: as "a group of acts related to information that can be punishable".

It can be broadly defined as any illegal conduct that damages electronically directed information and communication technology systems and the data in these systems. In 1820, the "Jacquard apparatus" was produced by Joseph Marie, a textile manufacturer in France. This machine allowed a series of steps to be repeated in weaving special fabrics. This led to Jacquard's employees fearing that their traditional occupations and livelihoods would be endangered. They committed acts of sabotage to discourage Jacquard from continuing to use the new technology. This is the first recorded cybercrime.

d- It is also an illegal behavior that takes place using electronic devices, and its purpose is mostly material or moral benefits while charging the victim with a corresponding loss. Often the goal of these crimes is hacking in order to steal or destroy information (25).

Including comprehensive definitions of information crimes:

e- The Belgian definition: it is “every action, reaction or omission that would encroach on material or intangible funds resulting, directly or indirectly, from the illegal use of information technology.” It is noted that this definition expresses the special or distinctive technical nature. It includes the most prominent forms of cybercrime and its definition includes its moral element, i.e. criminal intent. Through this definition, future developments of technology can be dealt with.

F- Definition of cybercrime: It is “those criminal acts resulting from or through the use of informatics and modern technology, represented by computers and automated data processing or transfer.”.

Second - The emergence of cyber-attacks:

The General Assembly, at its resolution 65/230, requested the Commission on Crime Prevention and Criminal Expediency to establish an open-ended intergovernmental group of experts, in order to conduct a comprehensive study of the problem of cybercrime and the measures taken by Member States, the international community and the private sector to address it, including the exchange of Information on national legislation, best practices, technical assistance and international cooperation to reduce cybercrime. Cyberattacks are directly related to two important events:

- The first: With the development of computers in the mid-fifties of the last century, accompanied by concerted efforts as a tool for processing and saving information digitally, in order to facilitate tasks, and that private and public companies culminated in the development of the central processing unit entrusted to it, and this developed radically in the subsequent decades, until it became a device Computer, mainly in the work of many private and working institutions as well as the daily life of individuals (26).
- As for the second event: it is the emergence of the World Wide Web (the Internet), which caused a dramatic revolution in the life of mankind through communication, and the transfer of information at high speed through a torrent of data sent over the air (27).

Countries have accelerated the pace of computer use; To achieve qualitative leaps in the security and military field, in the early nineties of the last century until some called it the term cold cyber war (28).

Third - The concept of cybercrime:

Cybercrime is very similar to ordinary or traditional crime in terms of the criminal, as he has the same motives to commit the crime, and the person may be natural or legal, but the tool can differ and here the real difference can be made between the two types of crime.

In cybercrime, the tool is high-tech, and also The crime scene that does not require the presence of the criminal, the crimes are committed remotely using communication lines and networks between the perpetrator and the crime scene, and in March 2000 the Los Angeles magazine indicated in issue 22, that the loss of American companies alone due to cybercrime is about ten billion dollars annually, even if 62% of most of these cybercrimes occur from outside the institution and through the Internet, while the remaining 39% of these losses are due to the employees of those institutions (29).

Cybercrime: It is “an act that causes serious harm to individuals, groups, and institutions, with the aim of blackmailing the victim and defaming her reputation in order to achieve material or service gains, and political goals using computers and modern means of communication such as the Internet” (30).

Information crimes aim to steal information and use it in order to obtain sums of money or cause psychological harm to the victim, or publish important information related to important institutions in the country or steal data of people or banks, and as we have shown that electronic crime is similar to ordinary crime in its elements in terms of the presence of the perpetrator and the victim And the act of crime, but it differs from ordinary crime by the different means used, which are modern technology and communication networks. Electronic crime mostly takes place without the need for the criminal to be present at the crime scene

We will distinguish “cybercrime” from “traditional crime” Computer crime can involve activities that are traditionally criminal in nature, such as theft, fraud, forgery, defamation and abuse, that cybercrime, in the first place, is represented in a limited number of acts that can Affects the confidentiality of data, or computer systems and their integrity, in addition to the economic and social benefits of computer technology and the Internet, as is the case with other means that enhance the capabilities of human interaction, but it can be used in criminal activities, and while computer crimes or computer-related crimes are considered a relatively stable phenomenon

However, the main factor in contemporary cybercrime is the unified global connection of the Internet, and many countries have confirmed since 2001 the recognition that computer-related acts, including damage to computer systems and stored data, unauthorized use of computer systems, and that the international community Pay attention to cybercrime and related criminal legislation, that such acts are often considered domestic crimes, and that crimes are committed using some applications, Interpol presented on international fraud, that computer crime is of an international nature, due to, the increase in communication in The Internet between countries through telecommunications, phones and satellites. The basic concept that cybercrime carries today is still limited to the possibility of using the idea that deals with the globalization of information and communication technology in committing criminal acts across borders. Therefore, cybercrime has become cross-border.

Fourth: Types of cybercrime:

Cybercrime is carried out through a computer, whether it is alone or connected to the Internet, and this is what we call cybercrime, and it is only achieved by the presence of three elements:

Three elements:

A. Existence of motive: In most cases, the desire is to obtain money or take revenge on the target, or to monopolize the largest number of customers, as is the case between competing companies.
B. Existence of a way to carry out the attack: The cyber attacker will not be able unless there is a plan for the method of attack to achieve his purposes, and this is the difference between a professional and unprofessional attacker, and in order to repel these attacks and mitigate their damage, we must plan methods and requirements for successful implementation.
C. The existence of vulnerabilities: that is, the existence of a loophole or weakness in the design of the program that is intended to be hacked, and attackers infiltrate through it to achieve the penetration you want.

With the difference in the three elements above, we have different types and classifications of cybercrime:

1- Crimes that cause harm to individuals

It is the one that targets a group of individuals or a specific individual in order to obtain important information related to his personal account, whether on his bank account or on the Internet, and this represents the following crimes:

Personal suicide: in which the criminal lures the victim, extracts information from her indirectly, and targets private information in order to benefit from it and exploit it to achieve material gain, defame people's reputation, or sabotage or spoil relations, whether social or work relations.

- Threatening individuals: Here the criminal may steal private personal information, real or false, and then send it via social media or via e-mail to many individuals, and the purpose is to discredit the victim and destroy her psychologically.
- Electronic fraud: "It is intended to be a deliberate behavior or act of an individual or many individuals that burdens or causes additional burdens on any other parties as a result of the use of unethical practices to obtain an unfair or illegal advantage" (31).

2- Crimes that cause harm to institutions:

A- Hacking systems: Cybercrime causes great losses to institutions and companies represented in material losses and losses in systems. The supporting company, to manage the companies, and this causes huge losses to the organization, and the private information of the employees of the institutions and companies can be stolen and incited or blackmailed in order to destroy the internal systems of the institutions, and then criminals often install spying devices on the systems and control them; To achieve some material and political gains, and cybercrime related to hacking into networks, accounts and systems, it is certain that it results in economic losses for the country, and it also threatens the national security of the state, especially if it developed and was not controlled, and combating hacking criminals, and the percentage of cybercrime represents 17%, which is It is increasing day by day, and this, if anything, indicates that we are all in danger, just as the hacking and control of websites by criminals and then employing them with the aim of destabilizing the security of the country, controlling the minds of young people, and inciting them to do illegal actions (32) .

B- Destruction of systems: This type of destruction uses the well-known methods, which is the use of electronic viruses, and the method of their spread in the system causing damage, chaos and destruction, and this causes great losses to institutions, and it may destroy the main server used by institutions to facilitate their work, and this is done by hacking employee accounts And then access to all accounts at the same time, and this causes a complete failure of the server, which leads to its destruction and thus causing losses to the organization.

C- Money crimes:

1- Seizing bank accounts: This is the hacking of accounts in banks or accounts belonging to the state and private institutions, just as credit cards are stolen and seized.

2- Violation of intellectual and moral property rights: it means making unoriginal copies of programs or files, and selling them through the Internet, and this (33).

3- Crimes targeting state security:

A- Spyware: Spyware has spread widely in technological circles, some of which are used for political, economic and military purposes, and theft of intellectual property. Intellectual or inventions, so they are the most serious information crimes.

B - Terrorist organizations use the method of misinformation: Terrorists depend on the use of modern means of communication and the Internet to mislead others, which may lead to destabilization in the country and cause chaos in order to implement political interests and terrorist schemes, and to mislead the minds of young people to convince them of personal interests (34).

V. Cyber terrorism (□) “electronic”

1- Definition of cyberterrorism: It is a criminal act, but in which weapons are used as means of communication that result in violence, destruction, or spreading fear towards the target, whether it is an individual, institution, or state, and the goal is to influence governments or populations, usually representing a specific political, social, or intellectual agenda. (35).

Therefore, some jurists defined electronic terrorism as: "Breaching a law by an individual or a collective organization, with the aim of causing serious damage to public order, through the information network" (36).

While others defined it as: “the illegal, hostile and aggressive use of the Internet, with the aim of terrorizing the government and civilians, or part of them, in pursuit of political or social goals” (37).

So it is sabotage or theft of data whose goal is mostly political, and whoever carries out the terrorist operation seeks to harm the national security of the state and not obtain personal gain. It has taken a modern turn in line with technical development and electronic prosperity, and we do not exaggerate if we describe terrorism as a story composed by politicians, each in his own way to achieve goals governed by interest. It came to the point that the politicians exchanged fingers, each accusing the other of being a terrorist.

Terrorism, which has become a political commodity exported by some politicians to others, has become a legal phenomenon on the international and domestic levels. The matter was not limited to operations directed from one state to another, but rather extended within the borders of the state itself.

The methods and manifestations of terrorism have become multiple, especially in recent years. Because terrorism resorted to the use of modern technology, to reach their purposes and achieve their goals, and this was achieved after the emergence of the Internet, which in recent years has become a means of communication with distinction for terrorist groups, especially those associated with organized groups, to the extent that it has become one of their media means, and this was accompanied by the emergence of terms and vocabulary And new concepts, such as "electronic terrorism" and Internet networks provide services to terrorists to spread propaganda and promote their ideas, and they also use a means of communication to recruit new elements, collect donations, and even develop plans for expansion, in recent years, and terrorists have resorted to using modern science and its applications; To reach their purposes and achieve their goals, and with the advent of the Internet, which has become in recent years a means of communication, with distinction for the so-called terrorist groups, especially those associated with organized groups, to the extent that this medium has become one of their media, and accordingly new terms, vocabulary, and concepts have appeared. I came to the Internet like: the term "cyber-terrorism".

These groups benefit from the services provided by the Internet via electronic addresses, and the so-called chat rooms. For publicity and dissemination of its ideas, it also uses this means of communication. To recruit new agents, collect donations and sometimes to make plans. And as a continuation of the expansion of “terrorism” in its various forms, the stage of the phenomenon of network terrorism began, which targets international national security, especially in the field of technology.

It is relied upon by those who want to carry out a digital attack. It is available and widespread among the general public, and it consists of a computer and an Internet connection point. It believed that users, in general, including companies, do not appreciate the reality of the danger emanating from any chaos that may affect digital networks and computers.

Therefore, most terrorist crimes are linked to the Internet, the preferred theater for extremists. The terrorist group kills, and the extremist second group justifies, justifies, incites, and recruits.

The reason why the Internet has become a haven for terrorists is characterized by its ease of use, quick access to their audience, and cheap prices. It is also a free arena without censorship over what is written or it is seen, far from the eyes of the security censors, and the boundaries between terrorism in its old concept and electronic terrorism have disappeared, which has become a great threat everywhere.

The new Corona virus “Covid 19” and the disruption of hospital equipment after a cyber-attack According to what was reported by the British newspaper “Daily Mail”, Brno University Hospital has been conducting many tests for the virus daily since the outbreak of the disease, and its equipment has been completely disabled (38).

Terrorism can penetrate the stock market and threaten the economy with that. It can also interfere with communications systems, electricity, water, and even control transportation and aviation systems, and even threaten the infrastructure of an entire country.

This will provide wide opportunities for terrorism to control government networks and security networks and close them or control and sabotage them. (39).

2- I use cyberspace in terrorist operations through:

A- Recruiting terrorists and focusing on propaganda, advertising, and fundraising.

B- Terrorism used the Internet to communicate, plan, manage operations, gather information and manage meetings.

C- Exploiting cyberspace to learn how to make explosives.

d- Terrorist organizations can attack flight or train control systems.

e- It can disrupt banks, steal money, and cause economic damage to the state.

F- Remotely adjust the gas pressure in gas pipelines to detonate them.

g- Tampering with safety systems in chemical plants.

h- Tampering with control systems in hospitals and other service institutions

i- Controlling transportation systems, especially on highways and tunnels, and causing traffic confusion or road accidents.

j- Controlling dams control systems, which causes disasters.

K- Control over the electrical interconnection networks connected to the Internet.

l- Deprivation of essential services

M- Tampering and damage to the nuclear reactor.

We are in the midst of "cyber fear", where politicians and the media are colluding with IT security companies.

This is not the first time that social trauma has occurred and we may learn from these past cases. As author Bruce Sterling(□) notes: For the average citizen in the 1870s, the telephone was stranger, more shocking, more "high-tech" and more difficult to understand than the most exciting feats of advanced computing...in the 1990s.

In trying to understand what is happening to us today, with our bulletin board systems, direct communication to the outside, fiber optic transmissions, computer viruses, amazing hacks, the tangle of new laws and new crimes, it is important to recognize that our society has faced a similar challenge before - and that, in general, he had a pretty good run of his own.

The panic about cyberspace is perhaps best explained by communications theorist Marshall McLuhan, who observed in 1967 that "Wherever a new environment goes around an old terrorist, there is always a new one.

CONCLUSION

In conclusion of this paper, we realize the importance of cyberspace in our daily life and that it poses an important challenge to information security and public stability. We must also realize that the technological development will continue to increase, and with it the importance of dealing with cyber threats effectively and effectively. By strengthening cyber power, focusing on protecting critical infrastructure, and enhancing cyber awareness, we can address challenges related to cybercrime and cyberterrorism and keep ourselves safe in cyberspace.

Sources and Refrences

1) Muhammad Wael Al-Qaisi, American Strategic Performance After 2008, the Barack Obama Administration as a Model, Obeikan Publishing, 2016, p. 60.

2) Abdul Qadir Muhammad Fahmy, Partial and Total Theories in State Relations, Al-Manhal for Publishing, 2010, p. 16,

3) Ahmed Abdel-Jabbar Abdullah, China and the global strategic balance after 2001 and prospects for the future, Arab House for Science, Lebanon, 2015, p. 89.

4) Nabil Bakakra, Diversity and Change in the Contents of Power: Towards a New Understanding of International Relations, Journal: Daftar al-Siyasah wa al-Qanun, Issue 19, 2018, p. 156.

5) Suhad Ismail Khalil, The National Force of the State, unpublished lectures: Faculty of Political Science, Al-Nahrain University / Department of Strategy, 2017.

6) Samah Abdel-Sabour Abdel-Hay, Smart Power in Foreign Policy: A Study of Iranian Foreign Policy Tools towards Lebanon, Al-Manhal Electronic Books, 2014, p. 29.

7) Suhad Ismail Khalil, previous source.

8) Ihab Khalifa, Electronic Power: How Countries Can Manage Their Affairs in the Age of the Internet, Cairo: Al-Arabi for Publishing and Distribution, 2017, p. 28.

9) Talib Ghuloom Talib, Strategy for Developing the Potential of Soft Power, Al-Manhal E-Books, 2015, p. 21.

10) Joseph s. nye, Jr, Cyber Power, The Future of Power in The 21st Century, Public Affairs Press, 2011, pp2. file:///D:/syber/%D9%83%D8%AA%D8%A8/cyber-power%20joseph%20nye.pdf ,

11) Katie Hafner, Where Wizards Stay Up Late: The Origins of The Internet (New York: Simon & Schuster, 1998).

12) Suelette Dreyfus and Julian Assange Underground: Hacking, madness and obsession on the electronic frontier (Kew Australia: Reed Books, 1997), p. 12.

13) Hacking. Quoted in Ward, 'A Brief History of.(Effective than Bombs', InfoWorld, 19 See Robert Lemos, 'Stuxnet Attack More January 2011

14) Effective than Bombs', InfoWorld, 19See Robert Lemos, 'Stuxnet Attack More January 2011' (Quoted in Joshua Davis, 'Hackers Take Down the Most Wired Country in Europe'), Wired, 21 August 2007, http://www.wired.com/politics/security magazine/15-09/ff_estonia.

15) do About It (New York: Harper Collins, Threat to National Security and What to Richard A. Clarke, Cyberwar: The Next 2010), pp. 30.

16) Joseph S. Nye, Jr, Cyber Power, The Future of Power in the 21st Century, Public Affairs Press, 2011, pp8. file:///D:/syber/%D9%83%D8%AA%D8%A8/cyber-power%20joseph%20nye.pdf .(Joseph S. Nye, Jr, Cyber Power, Previous source, pp9.

17) Suhad Ismail Khalil, The National Force of the State, unpublished lectures at the Faculty of Political Science, Al-Nahrain University / Department of Strategy, 2017.

18) Mounir Al-Baalbaki, Al-Mawred Arabic-English Dictionary, Beirut, Dar Al-Malayoun, 2004, p. 243.

19) Hathaway, Rebecca Croff, Philip Lefties, Aaliyah Nix, Eileen Nolan, William, Perdue and Julia Spiegel, “Cyber Law – Offense,” California Law Review, 2012.p.7. https://www.researchgate.net/publication/251334352_The_Law_of_Cyber-Attack

20) Julia Creswell, “The Oxford Dictionary of Etymology: Cybernetics,” Oxford University Press Online, 2010. file:///C:/Users/discovery/Downloads/Documents/1308129610.pdf

21) William Gortney, Director of the Joint Chiefs of Staff, USN Dictionary of Military Terms, US Department of Defense, from 2010-2012. Available at the following link. file:///C:/Users/DISCOV~1/AppData/Local/Temp/jp1_02.pdf

22) U.S. Department of Defense, Dictionary of Military and Associated Terms, Publication 1-02, Nov.8, 2010, as amended through feb. 15, 2012. (Thesis Co-Advisors: Daniel Moran Dorothy Denning Integrated Cyber Defenses, December 2007, Daniel Moran: Towards Cyber Defense Doctrine

23) Ahmad Abd al-Ghani Muhammad, Cybernetics as an introduction to the transformation of the concept of photography into postmodern art for the twenty-first century, College of Art Education, 200, p. 38.

24) Ahmad Abd al-Ghani Muhammad, Cybernetics as an introduction to the transformation of the concept of photography into postmodern art for the twenty-first century, College of Art Education, 200, p. 38.

25) Khader Mosbah Ismail Titi, Fundamentals of Information and Computer Security, Al-Manhal Publishing, 2010, pg. 408. https://store.almanhal.com/1231.html

26) Khader Mosbah Ismail Taiti, previous source, pg. 409.

27) Mustafa Al-Tayeb, The difference between information security and cybersecurity, website, seen on 4/12/2019, available at the following link, https://www.oolom.com/

28) Mustafa Al-Tayeb, previous source.

29) Robert Elder, Fighting in Cyberspace Means Cyber Domain Dominance last accessed Sept 11, 2007, Print News, Feb 28, 2007. last accessed Sept 11, 2007. http://www.af.mil/news/story.asp? id=123042670 .

30) Electromagnetic: The electromagnetic spectrum consists of groups of waves that have the same characteristics, but they differ in their wavelengths and frequencies, such as infrared (radio) groups, visible spectrum waves, ultraviolet rays waves, X-ray waves, ...etc.

31) Kenneth J. Knapp Cyber Security and Global lnformation Assurance: Threat Analysis and Response Solutions Kenneth J. Knapp U.S. Air Force, Eepdf e-book site, 2019, https://epdf.pub/cyber-security-and-global-information-assurance-threat-analysis-and-response-sol59733.html.

32) Kenneth J. Knapp

33) Margaret Rouse, cyber technologies, Techtarget Network, 2005, https://whatis. techtarget.com/definition/cyber.

34) Margaret Rouse, cyber technologies, Previous source.

35) Josh Evans, What Is Cyberpunk, science fiction com, By2011, Available at the following link, https://sciencefiction.com/2011/07/27/what-is-cyberpunk/.

36) Sen S. Kostjan, Cybersecurity, a general reference approach, previous source, p. 17.

37) The Telecommunications Regulatory Authority of the Lebanese Republic, Cybersecurity, 2008, seen on 3/16/2019, http://www.tra.gov.lb/Cybersecurity-EN.

38) The Telecommunications Regulatory Authority in the Lebanese Republic, Cybersecurity, 2008, previous source. http://www.tra.gov.lb/Cybersecurity-EN.

39) Laila Al-Janabi, The Activities of National and International Laws in Combating Cybercrime, the main website of Al-Motamedon Dialogue - Issue 4634, 9/8/2017, seen on 6/3/2019 at the following link, http://www.ahewar.org.

40) Adel Youssef Abd al-Nabi al-Shukri, Information Crime, and the Crisis of Algerian Legitimacy, Journal-Iraq, University of Kufa: No. 7, 2008, p. 113.

41) Yunus Harb, Computer and Internet Crimes: Brief Concept, Pronunciation, Characteristics, Images, and Procedural Rules for Prosecution and Evidence, a working paper submitted to the National Security Conference, published research, Al-Arabi for Criminal Studies and Research 2002, 12/2/2002, p.4.

42) Amir Farag Youssef, Information Crimes on the Internet, Alexandria University Press, 2008, p. 18.

43) Naji Malaeb, Cybersecurity: Defining and Evolving Cybercrimes, Arab Security and Defense website, 5/23/2017, available at the following link, http://sdarabia.com.

44) Christopher c. joyner and Catherine Lotrionte Coercion: Elements of a legal framework, European Journal for International Law, Information Warfare as International Vol,12.no,825-56,2001.p825.

45) Ibid.p.825.

46) Peter Sommer & Ian Brown, "Reducing Systemic Cyber Security Risk", 2011, pp.13.

47) Israa Jibril Rashad Merhi, Electronic Crimes, Objectives, Causes, Crime Methods and Treatment, Arab Democracy Center for Economic and Political Strategic Studies website, 216, available at the following link: https://democraticac.de/?p=35426

48) Theyab Musa Al-Badayna, Cybercrime, Concept and Causes, College of Strategic Sciences, Amman: The Hashemite Kingdom of Jordan, unpublished research, 2014, p. 16.

49) Computer Technology World Foundation (ITPILLARS), What are electronic crimes, their types, how to implement them, and ways to confront them, published on the following link, https://www.it-pillars.com, 2018.

50) Technology World Corporation for Computers (ITPILLARS, previous source.

51) Khalid bin Suleiman Al-Ghathrah, Muhammad bin Ibrahim Al-Suwail, Information Security in Soft Language, Riyadh, 2009, pp. 24-25.

52) Nihad Kreidi, Crime and Fraud in the Electronic Environment, (Beirut, 2008), pp. 14-16.

53) Ghada Nassar, Terrorism and Cybercrime, Cairo: Al-Araby for Publishing and Distribution, 2017, p. 21.

54) Ahmed Hossam Taha Tammam, crimes arising from computer use, computer criminal protection, Ph.D. thesis, unpublished (Tanta University: Faculty of Law, 2000), pp. 210-211.

55) Muhammad Ali Al-Arian, Information Crimes, Alexandria: University Publishing House, 2004, pp. 67-68.

56) Cyberterrorism: Barry Collin, a researcher at the Washington and Intelligence Institute in California, coined the term cyber terrorism, referring to the confluence of cyberspace and terrorism, and in 1998 published the Global Organized Crime Project of the Center for Strategic Studies CSIS International in Washington, issued a report entitled “Cybercrime, Cyber terrorism and Cyberwarfar.”

57) Adel Abdel Sadiq, Electronic Terrorism, Power in International Relations, A New Pattern and Challenges, Al-Ahram Center for Political and Strategic Studies, 2019, p. 107.

58) Muhammad Abdullah Minshawi, Internet crimes from a legal and legal perspective, King Fahd University Press: Riyadh, 1423, p. 11.

59) Muhammad Al-Amin Al-Bishri, Investigation of Computer and Internet Crimes, Arab Journal for Security Studies and Training, Riyadh: Kingdom of Saudi Arabia, 1422, p. 22.

60) SKY news, A cyberattack targeting “Corona” patients, March 14, 2020. Available at the following link, https://www.skynewsarabia.com/varieties/.

61) Israa Tariq Jawad Kazem Al-Jabri, The Crime of Electronic Terrorism - A Comparative Study -, Faculty of Law, Al-Nahrain University website, 2012.

62) Ehab Khalifa, Electronic Power: How Countries Manage Their Affairs in the Age of the Internet, "The United States of America as a Model", Cairo: Al-Arabi for Publishing and Distribution, 1st edition, 2017, p. 118.

63) Bruce Sterling: The Bicycle Repairer, 1997. Available at: https://www.google.com/search?client