Economics, Law and Policy
ISSN 2576-2060 (Print) ISSN 2576-2052 (Online)
Vol. 7, No. 1, 2024
www.scholink.org/ojs/index.php/elp

Original Paper

The Cybercrime Acts and the Electronic Transaction in International Law

Walid Fahmy[1]

[1] Professor of Public International law, Pharos University in Alexandria, Egypt

Received: January 26, 2024 Accepted: February 20, 2024 Online Published: March 15, 2024

doi:10.22158/elp.v7n1p18 URL: http://dx.doi.org/10.22158/elp.v7n1p18

Abstract

Cyberthreats "Cybercrime" is a "criminal offence that may be committed on or through a computer system generally connected to a network". As a result, it is a new type of crime and delinquency that varies from previous forms in that it takes place in a virtual location known as "cyberspace". In recent years, the democratisation of computer access and the globalisation of networks have both played a role in the growth of cybercrime. In fact, not isolated and the institutions in several States are fully aware of the seriousness of this phenomenon, which goes beyond the borders of each State. If all members of Jordan's criminal justice system are unaware of sophisticated computer and electronic device technologies, cybercrime will continue to rise. Despite technological developments and the information revolution, some states limits the subject of criminal protection to cash and fails to protect information funds against fraudulent acquisition.

International law plays a significant role in combating cybercrime and establishing guidelines for cooperation among nations.

Keywords

Cyber-crime, E-payment, Law, Security, International Conventions, International Telecommunication Union

1. Introduction

New technologies, particularly information and communications technology have an important place in economic life, and the number of transactions and exchanges conducted through the Internet is increasing dramatically. While these new technologies contribute favorably to the growth of economic life, they also open new avenues for committing corporate crimes, which poses substantial risks given their increased relevance (Toffler, 1981).

The coherent link between criminal behaviour and society reaction is culturally mediated via the realm of signifier. Cultural "imaginaries" regarding the Internet and its related concerns are being formed across a wide range of representational domains, including press coverage (Jewkes & Yar, 2010).

Cybercrime are frequently worldwide in character, despite the fact that the information is data controlled by domestic law. In this context, the flow of information freely flowing through the investigating authorities is strictly bound by virtue of their national authority and the sovereignty concept. Each legislature strives to either protect or defend himself or herself in his or her own territory or to abdicate legislative competence in the face of these illegal acts, or to observe and legislate as little as possible, which is an effective solution (Gautraud, 1996).

In Jordanian legislation, the general provisions of cybercrime are not much different from what they are in conventional crime, except in a few cases in its material element, particularly with regard to the elements of time and place, the extent to which national laws apply to certain acts committed abroad and the determination of a competent judiciary within the unitary State. Moreover, the criminal conduct of such crimes is represented in the flow of information through computer systems that cannot be physically controlled.

Although there is a difference between the area of cybercrime and the field of cybercrime, the technical reality has led to the merger of the two fields of "computerization and communication" with the term cybercrime. In order to determine the legal framework for this crime, a distinction must be made between two types of cybercrime. The first type is when Information Technologies has been used as a means to commit the crime, by attacking the computer's own set of tools or the data "information and software", so that the computer and the data it carries are assaulted. The second type is when information technology and telecommunications are the object and purpose of crime. Thus, we are confronted with new criminal acts, most of which are linked involves the vulnerability of information systems' security and integrity, as well as the confidentiality of data and information included within them. This type of crime is known as cybercrime via the Internet, and is accomplished through illegal access to and exposure to sites and systems and the information contained therein, such as attacks on websites by destroying or disrupting them and others.

2. The Meaning of Cybercrime and Its Characteristics

Some scholars of criminal law have used the term "cybercrime" in reference to computer crimes, cybercrime, and other modern means of communication. There are those who use the term "cybercrime", and the truth of this difference lies in the manner in which the researcher deals with the subject of his research and the subject of the right obtained by the assault.

2.1 The Concept of Cybercrime

Because there is no legal definition of cybercrime, it remains difficult to comprehend. Because of this decision of lawmakers, the doctrine multiplied the meanings of this term, leading to the complexity of legal analyses. Indeed, the lack of a legal definition of this term is a source of confusion, both in the field of reflection and in the analysis or vocabulary chosen. This confusion has led us to develop a practical definition of what cybercrime is, in order to understand its phenomenon.

2.2 Lack of Legal Definition of Cybercrime

Today's difficulty is that all of these diverse discourses, methods, or narratives are irrational, and their assertions to knowledge are frequently inconsistent. Do activities labeled as "cybercrimes" truly pose a "clear and present danger" to our "information societies", necessitating the activation of the criminal justice system's machinery? (Završnik, 2008).

Definitions are important in cybercrime for many reasons that overlap: (1) how people define cybercrime will influence estimates of its scope; (2) how people define cybercrime will influence the consequences (or react appropriately) to specific behaviours; (3) how criminologists try to explain cybercrime will be influenced by definitions; and (4) how people define cybercrime will influence effective interventions used to focus on particular types of behaviour. Definitions are important in cybercrime for at least seven reasons that overlap: (1) how people define cybercrime will influence estimates of its scope; (2) how people define cybercrime will influence the consequences (or react appropriately) to specific behaviours; (3) how criminologists try to explain cybercrime will be influenced by definitions; and (4) how people define cybercrime will influence effective interventions used to focus on particular types of behavior (Payne, 2020).

As cybercrime is not rigorously defined, it leads to terminological drifts. Thus, Mr. Alderman and Mr. Bloch retain as a definition of computer crime, the definition of cybercrime proposed by experts of the Organization for Economic Co-operation and Development (OECD), namely "any illegal or unethical or unauthorized behavior, which concerns automatic processing of data and/or data transmissions". These scholars, incorporating the moral concept into their definition, seem to consider that criminal law alone cannot contain the whole approach to the punishment of the fraudulent use of information technology. However, this approach cannot be accepted since dispute resolution charters, such as the Internet Charter for example, have revealed their limitations as an alternative dispute resolution world. The application of the criminal law is thus a solution to the failure of these initiatives (Alterman, 1988).

As well, Cybercrime is defined as the use of digital, electronic or software capabilities to divert, hijack, destroy, or illegally exploit public or private information systems. The technical history of cybercrime

is, unsurprisingly, that of a permanent dialogue between the sword and the shield, between the attack and its counter-measure. “Counter-measures” are responses to an action or event in order to prohibit, prevent or stop their proliferation at the source. “Prohibition” counter-measures can simply put an end, hic et nunc, to a malicious operation. This is what security software does that identifies a malicious “virus” code, isolating it, placing it in quarantine, and eventually deleting it. The so-called “prevention” counter-measures will record and characterize this malicious behavior by its signature, its behavioral recognition and ensure that it is stopped as soon as it is detected. Finally, the so-called “active” or “counter-offensive” counter-measures will extend this temporary ban by actively searching for its emission source in order to neutralize it (Baumard, 2014).

The confusion by these lawyers between cybercrime and computer crime is symptomatic of a difficulty in understanding this form of delinquency. This finding legitimizes the approach of the doctrinal approach which considers that the only acceptable approach is to reserve the meaning of computer fraud to the hypotheses in which computer technology is at the heart of the incriminating act while knowing full well that it is sometimes difficult to isolate the hard core of the periphery (Lucas, 2001).

The need to clarify acts that fall under cybercrime has led the doctrine to multiply the concepts designating illegal acts in relation to computers. This has spawned a plethora of doctrinal definitions of cybercrime.

There is no legislation or regulation defining cybercrime. However, some related concepts, such as computer crime, computer crime, computer crime or computer misuse, have been defined to address the issue of assimilation or distinction between crime and cybercrime.

According to the UN, cybercrime must cover any illegal conduct involving electronic operations aimed at the security of computer systems and the data they process, and in a broader sense any illegal act committed by means of a computer system or network or in connection with a computer system (Note 1). This definition uses the term illegal behavior to refer to cybercrime. However, conduct may be considered illegal in one State and legal in the other.

These confusions have led us to question a few other definitions. For instance, In the United States, cybercrime accounts for a large proportion of the offenses examined by the police. Its concept differs from state to state, and from one police department to another. Thus, cybercrime is considered a violation of criminal law involving knowledge of information technology for its perpetration, investigation, or criminal proceedings. On its part, the California Penal Code defines a list of illegal acts that fall under the scope of cybercrime. It considers cybercrime to be the act of accessing, or intentionally allowing access to, any computer system or network in order to design or carry out any plan or device to defraud or extort money, goods or services for the purpose of defrauding; thus to alter, destroy, or damage any computer system, network, program, or data (Note 2). The Texas Criminal Code, however, goes further. He considers cybercrime to be the act of accessing a computer, a network, or a computer system without the permission of his master (Note 3).

The confusion created by these laws between cybercrime and computer crime is symptomatic of a difficulty in understanding this form of delinquency. Today, cybercrime is only an illegal act related to computers. It has no specific reference in law. Yet, despite inconsistent attempts to define it, the term regularly calls for reflex reactions from the media, policymakers, politicians, academics and the public. It's a concept that can't be easily ebranlated and dismissed since it's quickly absorbed into popular jargon; and, while it has a specific meaning, it encompasses a wide range of activities (Wall, 2001).

2.3 The Trend towards Practical Definition of Cybercrimes

The previous examples illustrate the difficulty and complexity of this phenomenon. While some of the proposed definitions are narrow and insist that the category of this crime must involve a highly consumed computer operation in circumstances where the offence could not be committed, the other examples are broad and involve many offences that are already classified as traditional offences. However, a practical definition of cybercrime is necessary in order to understand this phenomenon.

Some Scholars tend that Cyberspace is a complex space to understand. It is both natural and artificial. Natural because its source is natural: the real world (Lessig, 1999). At the same time it is an artificial space. First of all, the language used is artificial-that of mathematics, starting with fundamental coding and ending with increasingly elaborate mathematical equations. These equations are like the germ of infinity of images, most of which have no correspondence in the natural world. Cyberspace is also artificial because it results from sophisticated technology, implemented by humans.

Cyberspace acts as a transformer of the real into the imaginary, and from the real into the imaginary. A real, real, imaginary transformation is possible thanks to quantum information, for example, the substitution of substantial money by computer money is only an elementary illustration of this transformation of great generality (Shyles, 2002). In that regard, it is neither determined nor indeterminate, it allows the notion of level of reality and the logic of the third party included to be brought into play. It is potentially a transcultural, and transnational space, so it is the space of human choice (Anderson, 1991).

Compared to cyberspace, we are witnessing a real transformation of the entire international system. On the one hand, the birth of a new legal system that involves a change in transnational legal relations, and on the other hand, the development of new information and communication technologies that in turn have led to the emergence of a new type of crime known as computer crime (Allot, 2000).

The computer offender would therefore be the person who commits a computer crime. Some authors dismiss the notion of computer criminal, in favor of that of computer criminal or computer fraudster (Parker, 1985). For its part, others prefer the term "computer crime" to the term "computer fraud", because of the harmony that takes place between the literal meaning of the word offender and its legal meaning (Lucas' 1987).

Cyberspace appears as an object of the offence or as a passive instrument and the infringement results from the result that the beneficiary of the information provided by cyberspace or the presentation resulting from its operation is without right to obtain it. Therefore, it is possible to be confronted with two hypotheses. In the first, the information contained in the computers will be used unlawfully, while the second hypothesis will concern the case of the misuse of this virtual space. Cases concerning the destruction of computers, as well as the data or programs they contained.

The addition of a prefix «cyber», which tends to appear excessively with each use of a classic concept on the Internet, to « » crime, makes it possible to retain two kinds of relationships between crime and telecommunications networks. In the first instance, crime may be directly related to a telecommunication network, i.e., the law directly criminalizes an act which, if the telecommunication network did not exist, the act could not be carried out. In the present case, there is the hacking of telephone networks to make free telephone calls (Bensoussan, 1996).

Secondly, crime may be indirectly related to a telecommunication network, i.e., the telecommunication network is understood as a tool or means to commit the offense. Examples include unauthorized access to a computer system, or sending viruses over the Internet. Cybercrime in the strict sense of the term is therefore defined as all offenses committed against or by a computer system carried out through a telecommunications network. It requires the direct or indirect intervention of a telecommunications network to commit the infringement (Shinder & Cross, 2002).

Cybercrime can be defined as: any unlawful action associated with the interconnection of computer systems and telecommunications networks, where the absence of such interconnection prevents the commission of such unlawful action. Under this definition, we can identify the four roles that the computer system plays in illicit acts:

Subject: Cases involving the destruction of computer systems, as well as of data or programs contained therein, or the destruction of equipment supplying air conditioning, electricity, enabling computers to function.

Support: A computer system may be the location or medium of an offense, or a computer may be the source or raison d'être of certain forms and kinds of assets that can be manipulated without authorization.

Tool: Certain types and methods of infringement are complex to require the use of a computer system as an instrument. A computer system can be used actively as in automatic scanning of telephone codes to determine the correct combinations that can be used later to use the telephone system without authorization.

Symbol: A computer system can be used as a symbol to threaten or deceive. For example, false advertising of non-existent services, as has been done by several computerized dating clubs.

3. The Nature and the Scope of Cybercrime

Criminal behaviour is a socially influenced phenomenon. We will never be able to live in a society without cybercrime, no matter how hard we try. In reality, if we haven't yet been able to bring the crime rate down to a reasonable level in the real world, how can we expect to do so in the virtual world, which is comparably more unreal, eternal, and legally less controllable? However, the nature, extent, and meaning of crime in a particular culture varies throughout time. The concept of a crime-free society is a fiction, because crime cannot be separated from civilization. As a result, the character of a crime is determined by the nature of a community (Devi, 2019).

The complexity of a civilization determines the intricacy of the crime that develops in its environs. It is necessary and crucial to check all of the elements that affect and contribute to crime in order to comprehend crime in a community. The socioeconomic and political structures of society must comprehend crime and the measures that may be taken to reduce it. When analyzing the nature and extent of a crime, the preventative and remedial actions taken by the machinery to regulate crime and delinquent behaviour in society are also taken into account (Devi, 2019).

A few year ago, "Crime" was small-scale, straightforward, and consistent until, and it could be traced using existing methods. It is simple in the sense that it allows for countrywide generalization and a broad definition that may be encompassed within the word limit. Even a legal legislation proclaiming any conduct to be prohibited and prescribing punishment for its violation was adequate to reduce crime rates. The majority of crime and associated phenomena are personal, and while widespread, they are still on a local scale. Until recently, crime was thought to be anti-legal and anti-social behaviour performed by illiterates, impatient, mentally ill people, or conducted in response to unexpected provocation, acute emotional tension, or occasionally out of necessity, or, in extreme cases, to settle a score with victims (Chowbe, 2011).

Likewise, with the right tools, these sorts of crimes are simply traceable. Because the majority of crimes are of a personal character, and both the accuser and the victim share a common communal bond, transgressions are placed in a controllable, understandable context. In summary, crime as we have historically understood it is surrounded by a social environment in which social pressure is used to keep criminals under control, either by social knots or a socially directed sanctioned system. The social environment not only provided a buffer for residents, but also offered them the appearance of security, leading them to believe that they might avoid being victimised if they avoided particular activities or connections (Chowbe, 2011).

One element of international transactions over the internet that is difficult to identify is jurisdiction. When courts were confronted with problems of jurisdiction law, they were unable to determine the right venue to hear matters involving cybercrime since the virtual world is boundless when compared to the physical world, making it extremely difficult to monitor cybercrime. The perpetrator may have acted from nation A, using an Internet service from country B, and the victim from country C. This is a problem in terms of criminal law application, since it raises concerns regarding which nation has

jurisdiction, which country should lead the investigation, and how to settle conflicts. While this case appears to be difficult now, it is important to remember that if the offence, for example, includes cloud computing services; it would be far more difficult. There's a chance that more jurisdictions will be activated (Gercke, 2012).

The term jurisdiction is used to refer to a wide range of legal concerns. The jurisdiction of a sovereign state to control particular behaviour is described by the term "jurisdiction", which is defined by a set of public international law. As a result, it is a facet of sovereign rights. Nevertheless, in the perspective of a cybercrime investigation, refer primarily to a state's ability to enforce its internal laws. In general, law enforcement can only conduct an inquiry if the government has jurisdiction over the situation. The history of nations that have passed computer criminal laws shows that the legislator has two alternatives when it comes to dealing with the topic at hand (Gercke, 2012).

To begin, legislators may combine the foregoing criminal provisions into a single code as single Cybercrime legislation. Some of the world's most advanced industrialized countries, namely the United Kingdom and the United States, have followed this tactic by enacting the Computer Misuse Act in 1990 and the Unauthorized Access Device and Computer Fraud and Abuse Act in 1984, correspondingly. Other States, such as Malaysia, which passed the Computer Crimes Act in 1997, and the United Arab Emirates, which passed The Federal Law on the Prevention of Information Technology Crimes in 2006, have used a similar approach (Kadi, 2010).

The second alternative is to include meaningful criminal laws relating to cyber offences into the country's current penal code. Many countries throughout the world, including Germany, Denmark, France, Switzerland, and Canada, have followed this method (Kadi, 2010).

Each technique has its own set of benefits and drawbacks: incorporating new criminal provisions into existing penal legislation keeps the country's substantive criminal law in a single code and prevents the dispersion of criminal provisions over several laws. This technique is also more beneficial for courts, prosecutors, legal experts, and even regular citizens since it makes substantive criminal legislation relating to Cybercrime more understandable. The inclusion of the above- mentioned criminal laws in one separate code as a particular Cybercrime statute, on the other hand, provides at least one substantial advantages, in that it would raise public awareness of computer crime, which is widely recognized as one of the most effective means of deterring Cybercrime (Kadi, 2010).

As a result, cybercrime has become a worldwide issue, and statewide generalization of crime is no longer feasible in the current environment. Our knowledge and control of cybercrime cannot be limited to a single country, but must be global. Only by enacting new laws and preparing worldwide preventative and defensive mechanisms will we be able to safeguard our civilization from this scourge known as cybercrime.

4. Features of Cybercrimes

Cybercrime as a whole is characterized by several characteristics, whether it is generalized, induced or executed, and cybercrime is often international in nature.

4.1 Evidentiary Difficulty in Cybercrime

Cybercrime is an area of automated information processing that targets morale, not material. This crime is therefore more difficult to prove punishable because the perpetrator has used sophisticated technical and technical means, and the criminal behavior that constitutes it is very difficult to detect. It is very easy for the perpetrator to conceal any electronic material evidence, as the perpetrator does not leave any tangible material outside after him. This, of course, makes it difficult to detect the crime and identify the perpetrator, unlike the traditional crime, which usually leaves material evidence or is verified by witnesses or other evidence.

On the one hand, Computer artifacts can be easily modified, overwritten or erased and therefore pose problems because digital information sources need to be authenticated and verified. The rules of evidence vary greatly depending on the jurisdiction, and even between countries that have similar legal traditions. However, legal systems in the common law tradition generally tend to have defined rules on the admissibility of evidence. In legal systems in the civil law tradition, in which professional judges maintain a high level of control over court proceedings, the admissibility of evidence may be flexible, although the weighting of evidence including the verification of its credibility and authenticity may also be subject to a set of rules (Office des Nations Unies contre la drogue et le crime, 2010).

For instance, in several legal systems, the quality of the procedures applied to maintain the integrity of digital information from the moment of its creation to its introduction in court must be demonstrated by the proposer of the evidence. The integrity and authenticity of digital information have a direct influence on the weight of evidence, in terms of its credibility and veracity. The party seeking to present evidence must generally demonstrate the durability of the evidence or chain of custody, in order to demonstrate that the evidence has not been falsified or altered. The durability of evidence is usually a matter of fact and the chain of custody process is the mechanism applied to maintain and document the chronological history of evidence that has been moved from one place to another (Office des Nations Unies contre la drogue et le crime, 2010).

The reliability of information generated and stored on a computer has also been challenged based on security flaws in programs and operating systems that could threaten the integrity of digital information (Office des Nations Unies contre la drogue et le crime, 2010).

4.2 The Cybercriminal Has Special Characteristics

The skill required to carry out criminal activity is the most prominent characteristic of an electronic offender. The overall implementation of cybercrime requires a certain amount of skills that the offender may acquire through his or her studies in this area or through experience in information technology. However, this does not necessarily mean that the cybercriminal has a great deal of knowledge in this area. The knowledge of the cybercriminal is embodied by identifying all the circumstances surrounding

the crime to be carried out. Where an electronic criminal can be a complete picture of his crime, by returning to the way and where cybercrime is practiced by computer system, the criminal can apply his crime to systems similar to those he targets before carrying out it.

The full description of a cybercriminal can contain several elements. Age, gender, socio-economic background, nationality and motivation are among the main characteristics. Moreover, the level of the criminal represents a distinguishing feature of the element of the human association behind the criminal behavior. Understanding cybercrime as a "socio-technological" phenomenon, based on the characteristics of the people who commit these crimes, represents a broader approach to prevention than relying solely on technical cyber security concepts (Levi, 2002).

Although individual characteristics are comparatively simple to define, it is well known that the analysis of organized crime frequently presents difficulties in measuring and defining it. This study adopts the expanded definition of an organized criminal group established by the United Nations Convention against Organized Crime. In this definition, there are several approaches to typology, as well as to classify a specific criminal offense as an "organized crime". There is no reason to believe that the development of these approaches and typologies could not be applied to the involvement of organized criminal groups in cybercrime—facing new challenges and on a case-by-case basis (Office des Nations Unies contre la drogue et le crime, 2010).

4.3 Motivation for Cybercrime

There is little difference between the perpetrators of cybercrime than in traditional crime, as the desire for profit or material benefit illegally is often the motive for the commission of cybercrime. It may also be motivated by a desire to conquer the computer system and overcome its protection barriers.

The goals of digital criminals may be quite broad and include a wide range of acts. It is difficult to identify a motivation in illicit cyber actions. So, several investigations and research have yielded diverse findings on the classification of reasons. According to some scholars, six prevalent mindsets among hackers include addiction, curiosity, and the pleasure of information searches, access, peer recognition, and discovering security vulnerabilities. In addition, hacker motives were divided into three categories: the desire for a challenge, greed, and malevolent purpose or vandalism. Other scholars have summed up the motives for illicit online actions as money, amusement, ego, cause, social group membership, and prestige (Li, 2017).

Hackers may hack for intellectual reasons, such as educational experimental work, harmless fun, or as a wake-up call; for personal reasons, such as negative reactions, cyber stalking; for social reasons, such as cyber-activism; for political reasons, such as cyber terrorism, cyber-warfare; for financial reasons; and for ego reasons. Moreover, there are ten types of hackers: curious hackers thrill seekers, people who want information about computers and their flaws, power seekers, vandals, people who steal industrial information, secrets, and/or intellectual property, people who steal money, people who undertake industrial espionage, terrorists, and international spies (Li, 2017).

4.4 The Transnational Nature of Cybercrime

Cybercrime is a crime that transcends the geographical boundaries of a State, since it is carried out through the information network. The perpetrator is often in one State and the victim is in another State, and the potential harm may be in a third State. This problem is particularly evident in the area of banks, where the connection of means of communication to computers has multiplied international financial transactions by electronic means, particularly through electronic transfer of funds, giving cybercrime an international dimension, especially the crimes of information fraud and credit cards.

In other words, Cybercrime has no geographical boundaries. It can be done against a victim who is located in another city, state, or country. A perpetrator just needs access to a computer that is connected to the Internet. The culprit does not require a passport and does not pass through any checkpoints while committing his crime. Automation enables criminals to perform a large number of computer crimes in a short period of time. The restrictions that govern physical activity do not apply to perpetrators of cybercrime (Aslan, 2006).

The main impediment to efforts to internationally unify domestic computer crime legislation is the fast growth of computer networks and information technology. Differences in certain substantive values may constitute a barrier to the adoption of harmonized domestic legislation on cybercrime. Furthermore, even if countries enact laws that harmonize their criminality of specific computer activity, they may nevertheless use various criteria for conviction and apply different punishments upon conviction. This disagreement is unavoidable since computer crimes in a highly industrialized country have far-reaching consequences than in a less industrialized country (Aslan, 2006).

Another impediment to remedies that rely on international cooperation is the inability of many nations to dedicate enough resources to combating computer crime. 61 It is not enough to just pass laws; each country must have enough internal resources to implement those laws. 62 Law enforcement authorities have frequently been hesitant to devote enough resources to combating the growing threat of cybercrime (Aslan, 2006).

The international nature of cybercrime has raised an important question as to the determination of jurisdiction and location to prosecute this crime. Is it the State in which the criminal activity occurred, the State in which the information in question is located or the State in whose interests the crime was caused by such manipulation?

Given the transnational character of cybercrime and its link to organized criminal groups, the United Nations Convention on Transnational Organized Crime (Al Hait, 2014) (Note 4) can be utilized as a foundation for enacting steps to obtain jurisdiction over different computer-related offences. Article 15 of the UNTOC specifies the criteria by which the convention’s contracting countries may gain jurisdiction over the offences specified by the treaty.

It says that the convention's contracting parties may establish jurisdiction over crimes recognized by the treaty when the offence is committed inside their territory. This is a repetition of the territorial principle of criminal law, which asserts that all crimes perpetrated inside a country's territory are subject to its jurisdiction. Jurisdiction over computer-related offences can also be established if the offence is committed on board a vessel or even inside an aircraft licensed under the laws of the country. This is because watercraft and aeroplanes are seen as extensions of a sovereign territory (Al Hait, 2014).

As an example of national laws, in the United States, before any person or organized criminal group may be prosecuted, the court must have jurisdiction over the offence in question. As a general rule, the court has stated that there is a presumption that US legislation do not have extraterritorial application. This is due to the need to avoid disputes with foreign laws that may arise as a result of the passage of legislation with extraterritorial applicability (Al Hait, 2014).

In case of conflicts on Jurisdiction over Cybercrimes, taking into account the specific provisions of cybercrime laws in the United States and the United Kingdom, it needs to follow that in a hypothetical case where a British criminal commits a hacking crime against an American individual in the United States, the jurisdiction over the offence will be as follows: In the first case, because computer hacking is punished as a felony in the United States, the United States may exercise jurisdiction over the crime perpetrated within its territory under the concept of nationality. In this case, the crime did not occur in the United States since the computer hacking occurred in the United Kingdom. However, because the victim is a US citizen, the location of the offence is irrelevant. The United Kingdom, on the other hand, may not claim jurisdiction over the offence. Following the Crown Prosecution Service's decision in the Gary McKinnon case, which will be discussed further below, it can be argued that while the act of computer hacking was committed in the United Kingdom, this does not automatically guarantee jurisdiction over the crime to the courts of the United Kingdom. It should be noted that the Computer Misuse Act of 1990 requires that the crime be strongly correlated to the United Kingdom's domestic jurisdiction. However, in this case, the victim was an American who also stays in the United States. The consequences of the crime occurred outside of the United Kingdom as well. As a result, only the United States may assert jurisdiction in this matter. Nevertheless, if the victim is an American citizen residing in France, the United States will also have jurisdiction over the violation under the Nationality principle. The United Kingdom may nevertheless deny jurisdiction over the offence since it is not inextricably related to it. France's jurisdiction over the case is dubious because the crime was not intended at it. Furthermore, the crime has no bearing on France's national interests. As a result, only the United States can assert jurisdiction over the offence (Al Hait, 2014).

Pursuant to Jordanian law, just as a natural or moral person commits cybercrime, the victim may be, although it often falls on the moral person as financial institutions, super-companies and others. Although information in these crimes is the most important target interest, especially if this information is of great value and importance and the aim of the cybercriminal is to obtain compensation for this

information.

It should be noted that the victim of this crime has a negative role to play, as many victims often prefer to hide their exposure to damages resulting from cybercrime, perhaps because they want to maintain their commercial reputation and financial position, and therefore the most targeted groups are banks and international institutions, so they limit victims to not disclosing the differences on their computerized devices (Kashkoush, 2000).

5. Elements of Cybercrimes

Cybercrime is based on two main pillars: the physical and moral elements, the cybercrime must have a physical element of an offence (Corpus delicti) that represents its concrete entity and reflects the conduct of the cybercriminal in a provable manner, and there must also be a moral corner that reflects the knowledge and will of the cybercriminal.

5.1 CORPUS DELICI of the Crime

The physical element of this offense is the criminal conduct of an act or omission ordered by law, and the physical element here differs from one situation to another depending on the classification of the act, and accordingly; Cybercrime cannot be restricted to a single legal characterization. The incident committed, which is described as a cybercrime, may constitute an affront, malicious, contemptible or threatening incident, and other acts in a manner that is in full conformity with the Penal Code through certain rules, the provisions of which apply even to crimes committed through the computer system. This is not problematic, as the provisions of the Penal Code can be applied to these traditional acts, but there are certain types of behavior that require a distinction between them and their "traditional" precedent, which calls for legislative intervention such as theft and electronic fraud.

5.2 Traditional Electronic Behavior

Nulla poena sine lege can indicate a variety of things. In a narrower sense, that precise formula refers to the treatment-consequence component of penal laws: no one shall be punished except in accordance with a legislation that establishes a punishment for criminal activity. The restriction, known as nullum crimen sine lege, states that no action shall be considered criminal unless it is expressly stated in the behaviour situation element of a penal legislation. Furthermore, the concept of tudla poena sine lege has been interpreted to encompass the norm that criminal legislation must be carefully construed. The rule's last and most crucial implication is that criminal laws cannot be applied retroactively. Obviously, each of the above meanings must be kept separate (Hall, 1937).

The same is true in Jordanian law. The principle of penal legitimacy, which says: "Nullum crimen, Nulla poena sine lege", has become a well-established principle in the Penal Code, and therefore no punishment for any positive or negative conduct except on the basis of a law that provides for its criminalization at the time of its committing and no sanctions or measures that have not been regulated by law, as confirmed by article 4 of the Penal Code, and it is known that many types of conduct with which information can be obtained by computer are subject to For the provisions of the Penal Code

such as threats (Note 5), slander (Note 6), contempt, disclosure of secrets (Note 7), etc.

With regard to the applicability of traditional texts to acts committed by electronic means, such as computers, article 355 of the Jordanian Penal Code, he noted that in the crime of disclosing secrets, the legislator requested the availability of certain acts constituting the crime of disclosing state secrets. The legislator used a flexible and interpretable term in several forms when using the word “pornography”, it may be verbally disclosed secrets, it may be written and may be by another person, and this does not prevent the use of modern technical means to send secrets, e-mail So it's a way to convey State secrets (Elhusseiny, 2000).

However, there are patterns of criminal conduct found as a result of technically advanced means to which none of the provisions of the Penal Code can apply, but the application of legal texts to them is a departure from the principle of criminal legitimacy to which the court has to abide by this, and on the other hand, the broad interpretation of the texts cannot be relied upon because it would expand the cycle of criminalization, a fact that imposes legislative intervention in the absence of texts governing the facts presented. Traditional texts do not apply to these facts.

From the above, it is clear that many cybercrimes are governed by the general rules governing other crimes and others are governed by special rules, and although there is something outside the scope of these rules, this necessitates legislative intervention to deal with certain unpunished acts but in themselves they are considered wrong, or at least the increased penalty, which makes them consistent with the serious harm that may be done to financial and social institutions, the damage caused by these crimes exceeds all It is particularly conceived if it is directed against banks and other state sectors such as the stock exchange, the military sector, the air, land, sea and other sectors (Elshewa, 1998).

5.3 Non Traditional Electronic Behavior

Criminality takes different forms than in the past, where the electronic criminal has a high degree of intelligence and competence and this has made him keep up with technology, and therefore the legislator has to keep up with this, by developing his means to deter these types and images of acts that have been expanding and increasing without legal obstacles, he had to develop the means to protect him the rules of criminalization “in a way that secures the requirements of this development, and from the new crimes committed by computer, for example The use of electronic information, whose provisions are not similar to the provisions of the traditional theft offence provided for in article 499 of the Jordanian Penal Code, the difference between them is that the use of electronic information takes place without the transfer of the transfer to the possession of the perpetrator, i.e., the electronic criminal may enter into the memory of another computer and see the contents in it and withdraw a copy of it as belonging to another person”.

Other new offenses include the penetration of networks and computers belonging to third parties, whether natural or moral, as illegal intrusion, breach of confidentiality, breach of private life or illegal access to information. These offenses also include the dissemination of illegal ideas and intrigues through the information network, whether religious, political or moral, as well as the use of electronic

mail to infringe upon intellectual property rights, as well as the blocking of Internet networks and access to computer devices and their disruption by viruses that may cause the total or partial destruction of information or the diversion of data stored on State computers (Note 8).

5.4 Mental Element

The relevance of the mental component in crime should not be overlooked. For it is the mental component of an offence that separates between mistake and crime, murder and mishaps and the innocent taking of property from steal. In all of these contrasts, the conduct is the same in each section-it is the mental state that distinguishes them, and it is the mental aspect that determines when the criminal law will be applied (France, 1990).

Cybercrime, like any other traditional crime, must be committed by a person who is able to bear the responsibility for his actions as a "criminal official", and therefore those who are not recognized by the Penal Code as such and who have been under the influence of coercion or necessity under article 99 of the Penal Code, or who are unaware or of the "insane" will provided for in articles 94-94 of the Penal Code.

In general, the mental element is a relationship between the material nature of the crime and the personality of the perpetrator. This relationship is subject to the law and consists of the control of the perpetrator over his behavior and the consequences of such behavior, the essence of which is willpower and therefore of a psychological nature. It is well known that there is a division of offenses, the moral element being the basis for which the offense is either intentional or unintentional. This is what the Jordanian penal legislature has taken into account in article 11 of the Penal Code, so that the offense is intentional. If the result of the offense arises from the perpetrator's intent, if it is foreseen, it is presumed to have occurred, and the error is if the act is caused by negligence, lack of caution or failure to observe laws and regulations.

5.5 Cybercrime as Crime

Considering that the meaning of a mental element changes depending on the criminal offence, the only way to fully comprehend mens rea is to thoroughly examine the terms of specific crimes. The law on mens rea has been largely developed by debates about the required mens rea criteria in respect to certain offences. For example In English criminal law, a variety of words have been used to communicate responsibility, including purpose, intention, recklessness, wilfulness, knowledge, belief, suspicion, reasonable cause to believe, maliciousness, fraudulence, dishonesty, corruptness, and suspicion (Marchuk, 2014).

With the emergence of certain types of crimes, such as money-laundering, terrorism, organized crime and the use of modern technology in the commission of crimes, many have come to view the offender as having great intelligence. The crimes of money-laundering require a high degree of economic knowledge in the form of sale and purchase and discernment in concealing the illegitimate nature of these funds and their appearance of legitimacy. The same applies to cybercrime, which requires a share of specialized knowledge of the computer science, software and information network of the offender,

and sometimes even the use of experts to commit this crime.

Although the Jordanian legislature has not spoken of the figure of the mental element, it may require criminal intent, since the crime is intended as a public origin and the exception is unintentional. Cybercrime, according to the scenario, occurs only intentionally, preceded by the temporal and psychological elements, i.e., thinking and contemplating information and penetrating the computer and the information network in order to achieve the benefit or goal of the perpetrator. The computer may be the instrument used for counterfeiting and may be a means of unduly acquiring cash from funds or of destroying information stored on another computer, or a means of destroying a second computer's memory after transferring information in it in an attempt to remove the effects of the crime, or use viruses for destruction, destruction of the crime, the result of sexual exploitation or the will to achieve all such crimes.

5.6 Cybercrime as Unintended Crime

Under article 11 of the Penal Code, an offense is unintentional if the result of the criminal offense is due to the fault of the perpetrator, whether it is negligence, lack of caution or disregard of laws, regulations and orders. In general, the offense is unintentional if the perpetrator wants to act and his will is not affected by the crime. It is conceivable that a cybercrime could take place in this manner. It is possible that the person who relies on his skills to avoid the problems of viruses and the equipment in which he works as a result of the excessive use of the computer belonging to the department in operations on his own account.

6. The Cybercrime in International Law

There are several key international legal instruments and initiatives that are relevant to addressing cybercrime. Here are some of the most important ones:

1) United Nations General Assembly Resolutions: The United Nations has adopted several resolutions that recognize the importance of addressing cybercrime and emphasize the need for international cooperation in this area. These resolutions encourage member states to develop national legislation and cooperate with one another to combat cybercrime.

2) Council of Europe Convention on Cybercrime: Also known as the Budapest Convention, this treaty is the first international legally binding instrument that addresses both substantive criminal law and procedural law aspects of cybercrime. It sets out offenses related to computer systems and data, such as unauthorized access, computer-related fraud, and child pornography. The convention also establishes procedures for investigations, extradition, and international cooperation.

3) European Union (EU) Directives: The EU has enacted several directives to combat cybercrime and strengthen cybersecurity within its member states. These directives cover a wide range of issues, including attacks against information systems, data breaches, and the protection of critical infrastructure.

4) International Telecommunication Union (ITU): The ITU is a specialized agency of the United Nations that deals with information and communication technologies. It plays a role in promoting international

cooperation and developing guidelines and standards to enhance cybersecurity and combat cybercrime.

5) Mutual Legal Assistance Treaties (MLATs): Many countries have bilateral or multilateral agreements known as MLATs, which provide a legal framework for cooperation in criminal matters, including cybercrime. These treaties enable countries to request and provide assistance in investigations, extradition, and the gathering of evidence.

6) Interpol: The International Criminal Police Organization (Interpol) facilitates international police cooperation and assists member countries in combating cybercrime. It operates various initiatives and platforms to support information sharing, capacity building, and coordination among law enforcement agencies.

It's important to note that the legal frameworks and approaches to cybercrime may vary among countries. Some countries may have specific legislation targeting cybercrime, while others may rely on existing laws to prosecute cybercriminals. International cooperation and coordination are crucial to effectively combat cybercrime, as it often involves cross-border activities and the need to share information and evidence between jurisdictions.

6.1 Cybercrimes in International Conventions

International conventions and treaties play a significant role in addressing and combating cybercrime. These conventions provide a framework for international cooperation, harmonize legal approaches, and establish guidelines for the prosecution and prevention of cybercrimes. Here are some key international conventions that deal with cybercrime:

1) Council of Europe Convention on Cybercrime (Budapest Convention): This convention is one of the most comprehensive international instruments addressing cybercrime. It criminalizes a wide range of cyber offenses, including illegal access, data interference, system interference, computer-related fraud, child pornography, and offenses related to copyright infringement. It also establishes procedures for investigations, extradition, mutual legal assistance, and international cooperation in combating cybercrime (Maskun, Manuputty, Noor & Sumardi, 2014).

2) United Nations Convention against Transnational Organized Crime (UNTOC): While not specifically focused on cybercrime, UNTOC is a framework convention that includes provisions relating to organized criminal activities, which can include cybercrime. It encourages international cooperation and the development of domestic legislation to combat organized crime, including cybercrime, and provides a platform for countries to collaborate in addressing transnational cybercriminal activities.

3) African Union Convention on Cyber Security and Personal Data Protection (Malabo Convention): This convention was adopted by the African Union in 2014 and aims to address cybercrime and enhance cybersecurity in Africa. It criminalizes various cyber offenses, such as unauthorized access, interception of data, and cyber terrorism. The convention also promotes cooperation among African states in areas such as information sharing, capacity building, and harmonization of legislation (Bekele, D., 2017).

4) Shanghai Cooperation Organization (SCO) Convention on Combating Extremism (SCO Convention): The SCO Convention, adopted by the member states of the Shanghai Cooperation Organization, focuses on combating extremism but also includes provisions related to cybercrime. It addresses offenses such as the use of information and communication technologies for terrorist purposes and the dissemination of extremist content online. The convention promotes cooperation among member states to prevent and combat cybercrimes with an extremist dimension.

5) ASEAN Convention on Cybercrime: The Association of Southeast Asian Nations (ASEAN) adopted this convention to enhance regional cooperation in combating cybercrime. It criminalizes various cyber offenses, such as unauthorized access, illegal interception, and data-related offenses. The convention also provides mechanisms for international cooperation, including extradition, mutual legal assistance, and the establishment of a network of national contact points.

It's worth noting that while these conventions provide a framework for international cooperation, their ratification and implementation by individual countries may vary. Additionally, some countries may have their own domestic legislation specifically targeting cybercrime. International cooperation and coordination are essential in addressing cybercrime effectively, as cybercriminal activities often transcend national borders and require collaboration among countries to investigate, prosecute, and prevent cybercrimes.

6.2 The Contributions of International Telecommunication Union (ITU)

The International Telecommunication Union (ITU) plays a significant role in enhancing cybersecurity through various initiatives and activities. Here are some ways in which the ITU contributes to cybersecurity:

1) Setting Standards and Best Practices: The ITU develops international standards and best practices to promote cybersecurity. These standards cover a wide range of areas, including network security, incident response, cryptography, and secure software development. By establishing globally recognized standards, the ITU helps ensure that cybersecurity measures are consistent and interoperable across different countries and organizations (International Telecommunication Union, 2012).

2) Capacity Building and Training: The ITU provides capacity-building programs and training initiatives to help member states develop their cybersecurity capabilities. It offers workshops, seminars, and training courses on topics such as cyber threat intelligence, risk management, incident response, and cybersecurity policy development. By improving the knowledge and skills of cybersecurity professionals, the ITU helps strengthen the overall cybersecurity posture of member countries.

3) Cybersecurity Awareness: The ITU promotes cybersecurity awareness among governments, businesses, and the general public. It raises awareness about emerging cyber threats, best practices for protecting digital assets, and the importance of responsible online behavior. Through campaigns, publications, and events, the ITU aims to foster a culture of cybersecurity and encourage individuals and organizations to take proactive measures to protect themselves from cyber threats.

4) Cybersecurity Incident Response: The ITU operates the Global Cybersecurity Index (GCI) and the ITU-IMPACT (International Multilateral Partnership Against Cyber Threats) platform. These initiatives help facilitate the sharing of information and coordination of responses to cybersecurity incidents among member states. The ITU also assists countries in developing national incident response capabilities and establishing Computer Emergency Response Teams (CERTs) to effectively respond to cyber threats and incidents (International Telecommunication Union, 2012).

5) International Cooperation and Collaboration: The ITU fosters international cooperation and collaboration among member states, industry stakeholders, and other international organizations. It facilitates information sharing, coordination, and joint initiatives to address global cybersecurity challenges. The ITU also works closely with other cybersecurity-related organizations, such as the International Electrotechnical Commission (IEC) and the International Organization for Standardization (ISO), to ensure a holistic and coordinated approach to cybersecurity.

6) Policy Development and Advocacy: The ITU actively engages in policy discussions and advocacy efforts related to cybersecurity. It provides a platform for member states to exchange views, share experiences, and establish common positions on cybersecurity issues. The ITU also contributes to global policy debates and initiatives, such as the United Nations Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (UN GGE), to shape international cybersecurity norms and frameworks.

Overall, the ITU plays a crucial role in promoting cybersecurity at the international level by developing standards, building capacities, raising awareness, facilitating cooperation, and advocating for effective policies and practices (International Telecommunication Union, 2012).

6.3 The Cooperation among Countries in Investigating and Prosecuting Cybercrimes

International conventions on cybercrime provide mechanisms and guidelines to facilitate cooperation among countries in investigating and prosecuting cybercrimes. Here are some key features that promote cooperation (Verdelho, 2008):

1) Extradition: International conventions establish provisions for the extradition of individuals suspected or convicted of cybercrimes. They outline the process by which one country can request the extradition of a suspect from another country. Extradition enables the transfer of an accused person to the requesting country to face trial or serve a sentence. These provisions help ensure that cybercriminals cannot evade justice by crossing international borders.

2) Mutual Legal Assistance: International conventions also provide a framework for mutual legal assistance between countries. Mutual Legal Assistance (MLA) allows countries to request and provide assistance in various aspects of cybercrime investigations and prosecutions. This assistance can include sharing information, gathering evidence, conducting searches and seizures, and taking testimony from witnesses. The conventions establish procedures and guidelines to streamline the process of MLA, ensuring efficient cooperation between countries.

3) Law Enforcement Cooperation: International conventions encourage and facilitate cooperation among law enforcement agencies across borders. They promote the exchange of information and intelligence related to cybercrimes, allowing law enforcement agencies in different countries to collaborate in investigations. This cooperation can involve sharing data on cyber threats, coordinating joint operations, and assisting in the identification and apprehension of cybercriminals.

4) Joint Investigations and Task Forces: International conventions support the establishment of joint investigations and specialized task forces to tackle cybercrimes. These structures bring together law enforcement agencies from multiple countries to work collectively on complex cybercrime cases. By pooling resources, expertise, and information, joint investigations and task forces enhance the effectiveness of investigations and prosecutions.

5) Data Preservation and Recovery: International conventions recognize the importance of preserving electronic evidence and facilitating its recovery. They establish procedures for the preservation of data, including data stored in different jurisdictions. These provisions ensure that crucial evidence is not lost or destroyed, enabling its use in cybercrime investigations and prosecutions.

6) Information Sharing and Training: International conventions promote information sharing and capacity-building initiatives among countries. They encourage the exchange of best practices, expertise, and technical knowledge related to investigating and prosecuting cybercrimes. Training programs and workshops are organized to enhance the skills of law enforcement officials, prosecutors, and judges in dealing with cybercrime cases.

7) Harmonization of Laws: International conventions encourage countries to harmonize their domestic legislation with the provisions of the conventions. This harmonization helps establish a common legal framework for addressing cybercrimes and ensures consistency in the interpretation and application of laws across different jurisdictions. It facilitates cooperation by removing legal barriers and aligning legal approaches to cybercrime.

By providing these mechanisms and guidelines, international conventions on cybercrime create a framework for countries to cooperate effectively in investigating and prosecuting cybercrimes. They help overcome jurisdictional challenges, facilitate information sharing, enhance law enforcement capabilities, and promote a coordinated global response to cyber threats.

7. Conclusion

Following the presentation of the topic of cybercrime and its legal dimensions, the complexity and difficulty of the topic was noted, as cybercrime was a relatively recent crime requiring future studies as an attempt to establish general principles for all related crimes in technical and information development and modern means of communication. This required legislative intervention in order to establish an integrated legal mechanism and fill all the gaps in the penal laws in force in this regard.

It is imperative to recognize that the phenomenon of cybercrime, which is taking on a new form, is a serious challenge at the present time, which requires combating it both in terms of trade and punishment and in terms of prosecution, which requires; First, based on the conviction of the seriousness of this phenomenon and the attempt to reconcile respect for the principle of the national sovereignty of each State in its traditional form, and to depart, albeit to a greater extent, before the necessities and requirements of international judicial cooperation, which, as far as its success is concerned, achieves the effectiveness of all efforts and the means deployed to address and combat the phenomenon of cybercrime. Secondly, the development of the penal legislative structure with continuous and persistent legislative intelligence fills the gaps of penal regulations in such a way that they can subject these crimes to their descriptions and texts, and to keep up with the developments begged by the perpetrators of these crimes.

The point of this study is that there is no agreed definition of cybercrime, and the designation of this crime has been and continues to be the subject of doctrinal debate between its designations as information, electronic or technical crime... etc., although specialists have made efforts to thank them for reaching an appropriate definition that is appropriate to the nature of cybercrime. However, attempts to find a definition of this crime have multiplied, but not all are out of two directions; first, narrow to the concept of cybercrime, and the second has expanded its concept.

Cybercrime is a new fact and a new phenomenon in the international legal corridors. Responses to international law describe cybercrime as a new type of international crime that is not subject to international regulation. The establishment of a “needs for international law” instrument is urgent. Indeed, it is thought that the regime should generally be governed by international law. Due to the universal nature of the agreement, it will give cybercrime a legal status under international law.

References

Allot, P. (2000). The Emerging Universal Legal System. *International Law Forum, 3*(1). https://doi.org/10.1163/15718040120962653

Alterman, H., & Bloch, A. (1988). *La fraude informatique* (No. 246-247). Gazette du palais, Paris.

Anderson, B. (1991). *Imagined Communities: Reflections on the Origin and Spread of nationalism*. Verso.

Aslan, M. Y. (2006). Global, "Nature of Computer Crimes and the Convention on Cybercrime". *Ankara Law Review, 3*(2). https://doi.org/10.1501/Lawrev_0000000035

Baumard, P. (2014). La cybercriminalité comportementale: Historique et regulation. *La Revue française de criminologie et de droit penal*, (3).

Bekele, D. (2017). *The African Union Commission and Internet Society Support Internet Infrastructure Security in Africa*. Global Forum on Cyber Expertise.

Bensoussan, A. (1996). *Les Télécoms et le Droit*. Hermes.

Bologna, G. J. (1997). *An Organizational Perspective on Enhancing Computer Security*. Daniel Martin, La Criminalité Informatique. Presses Universitaires de France.

Devi, B. (2019). Cyber crimes issues and challenges in social media Awarness of Cuddalore District. In S. Saileela, & S. Kalaivani (Eds.), *Education on Digital Cultural and Social Media*. National Seminar on Digital culture and social media, Annamalai University.

Donn, B., & Parker, D. B. (1985). *Combattre la criminalité informatique Relié*. OROS.

Elhusseiny, O. E. (2000). *An overview of theft offenses in terms of their connection to automated processing systems*. UAE Information Technology Center.

Elshewa, M. S. (1998). *Information revolution and its repercussions*. Arab Renaissance Publishing House (Dar Elnahda).

Faqir, R. S. A., Sharari, S., & Salameh, S. A. (2014). Cyber Crimes and Technical Issues under the Jordanian Information System Crimes Law. *Journal of Politics and Law, 7*(2). https://doi.org/10.5539/jpl.v7n2p94

France, S. (2011). The mental element. *Vuwlr Monograph, 20*(3).

Gautraud, N. (1996). *Internet, le Législateur et le Juge*. Gazette de Palais.

Gercke, M. (2012). *Understanding cybercrime: Phenomena, challenges and legal response*. International Telecommunication Union.

Hall, J. (1937). Nulla poena sine lege. *Yale law Journal, 47*(2). https://doi.org/10.2307/791967

International Telecommunication Union. (2012). *Understanding Cybercrime: Phenomena, Challenges and Legal Response*.

Jewkes, Y., & Yar, M. (2010). *Handbook of Internet Crime*. Willan Publishin.

Kadi, R. M. (2010). The Scope and the Nature of Computer Crimes Statutes—A Critical Comparative Study. *German law Journal, 11*(6). https://doi.org/10.1017/S2071832200018757

Kashkoush, H. H. (2000). *Criminal protection of electronic commerce on the Internet*. Arab Renaissance Publishing House (Dar Elnahda).

Lessig, L. (1999). *Code and Other Laws of Cyberspace*. Basic Books, Inc. Division of Harper Collins.

Levi, M. (2002). Perspectives on "Organised Crime": An Overview. *The Howard Journal, 37*(4). https://doi.org/10.1111/1468-2311.00104

Li, X. (2017). A Review of Motivations of Illegal Cyber Activities. *Criminology & Social Integration Journal, 25*(1). https://doi.org/10.31299/ksi.25.1.4

Lucas, A. (1987). *Le droit de l'informatique*. Presses universitaires de France, Coll. Thémis Droit.

Lucas, A. (2001). *Le droit de l'informatique*. Presses universitaires de France, Coll. Thémis Droit.

Marchuk, I. (2014). *The Fundamental Concept of Crime in International Criminal Law A Comparative Law Analysis*. Springer-Verlag Berlin Heidelberg. https://doi.org/10.1007/978-3-642-28246-1

Maskun, M. A., Noor, S. M., & Sumardi, J. (2014). Legal'S Standing of Cyber Crime in International Law Contemporary. *Journal of Law, Policy and Globalization, 22*.

Office des Nations Unies contre la drogue et le crime. (2010). *Etude détaillée sur la Cybercriminalité, Rapport*.

Payne, B. K. (2020). Defining Cybercrime. In J. H. Thomas, & M. B. Adam (Eds.), *Handbook of International Cybercrime and Cyberdeviance*. He Palgrave, springer. https://doi.org/10.1007/978-3-319-78440-3_1

Pedro, V. P. (2008). *The effectiveness of international co-operation against cybercrime: Examples of good practices, 1*(4). Retrieved from https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId =09000016802fa3a2.

Shinder, D. L., & Cross, M. (2002). *Scene of the Cybercrime, Syngress*.

Shyles, L. C. (2002). *Deciphering Cyberspace: Making the Most of Digital Communication Technology* (1st ed.). Sage Publications, Inc. https://doi.org/10.4135/9781452233161

Toffler, A. (1981). *La Troisième Vague* (Casserole Ed.).

Vijaykumar Shrikrushna Chowbe. (n.d.). *The Concept of Cyber-Crime: Nature & Scope*. Sant Gadge Baba Amravati University' Sant Gadge, Baba Amravati University, Amravati.

Wall, D. S. (2001). *Cybercrimes and internet*. Routledge. https://doi.org/10.4324/9780203164501_chapter_1

Završnik, A. (2008). Cybercrime-Definitional Challenges and Criminological Particularities. *Masaryk, University Journal of Law and Technology, 2*(2).

Notes

Note 1. Tenth United Nations Congress on the Prevention of Crime and the Treatment of Offenders, A/CONF.187/10, 3 February 2000, p.5. Two subcategories of cybercrime exist:

(a) Cybercrime in a narrow sense ("computer crime"): any illegal behaviour directed by means of electronic operations that targets the security of computer systems and the data processed by them;

(b) Cybercrime in a broader sense ("computer-related crime"): any illegal behavior committed by means of, or in relation to, a computer system or network, including such crimes as illegal possession, offering or distributing information by means of a computer system or network.

Note 2. California Code, Penal Code-PEN §502.

Note 3. Texas Penal Code-PENAL §33.02.

Note 4. The United Nations Convention on Transnational Organized Crime was approved by the General Assembly on November 15, 2000. (UNTOC). It is now the primary international convention dealing with transnational organized crime administered by the United Nations. It exemplifies the United Nations' commitment to combating transnational organized crime.

Note 5. Article 420 Penal code. Article 22 of the Jordanian Telecommunications Law also states: "Anyone who, by any means of communication, sends threatening or insulting messages or messages that are inimical or that are intended to cause panic, shall be punished by imprisonment for a period of not less than one month and not more than one year or by a fine of not less than LYD 400 and not more than LYD 2,000, or both".

Note 6. Article 189/3/a Penal code.

Note 7. Article 355 Penal code.

Note 8. See, for example: Articles 4-1 of the Cybercrime Act.